Tra codici, cifratura e crittografia: il ruolo della matematica nell'arte di nascondere messaggi

Simone Zuccher
E-mail: zuccher@sci.univr.it
Web page: http://profs.sci.univr.it/∼zuccher/

Liceo Scientifico "E. Medi" e
Facoltà di Scienze Matematiche, Fisiche e Naturali – Università di Verona

Conferenze per i genitori degli studenti e non
21 Aprile 2010

Agenda

Agenda

1. Introduzione
   - Steganografia e crittografia
2. Crittografia
   - Classificazione e descrizione di alcuni metodi
3. Chiave
   - Chiave privata $\leftrightarrow$ chiave pubblica
4. Il ruolo della matematica
   - I numeri primi
5. Conclusioni
   - Domande

Agenda

Agenda

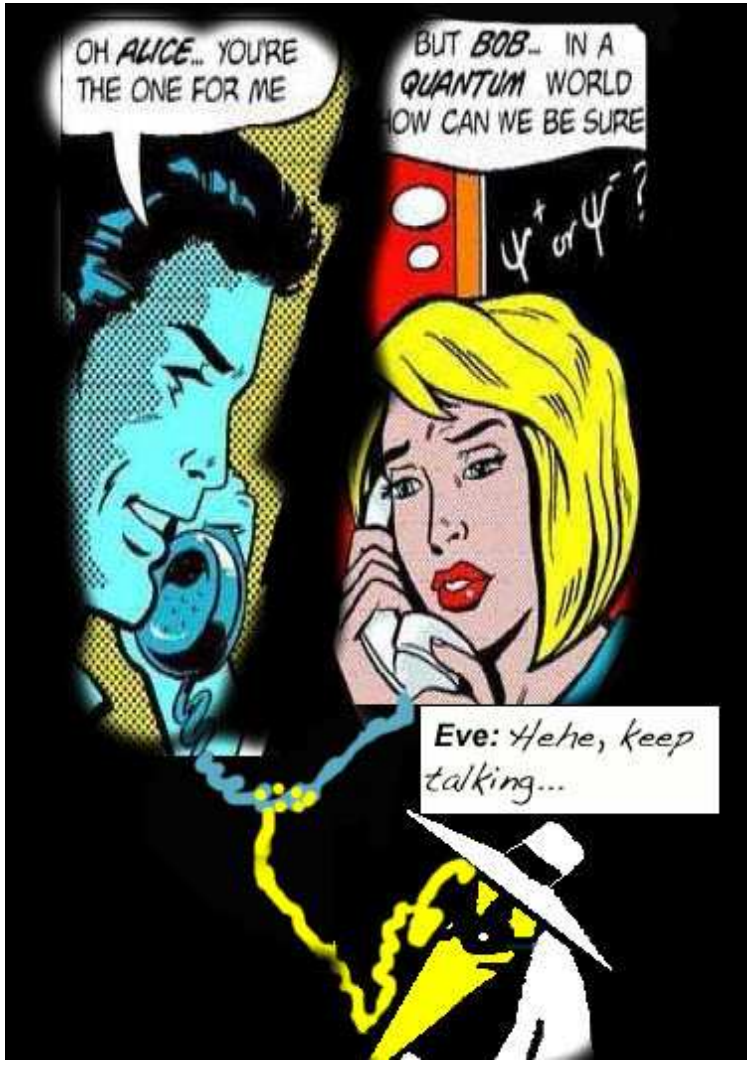
1. Introduzione
   - Steganografia e crittografia
2. Crittografia
   - Classificazione e descrizione di alcuni metodi
3. Chiave
   - Chiave privata $\leftrightarrow$ chiave pubblica
4. Il ruolo della matematica
   - I numeri primi
5. Conclusioni
   - Domande

Agenda

1. Introduzione
   - Steganografia e crittografia
2. Crittografia
   - Classificazione e descrizione di alcuni metodi
3. Chiave
   - Chiave privata $\leftrightarrow$ chiave pubblica
4. Il ruolo della matematica
   - I numeri primi
5. Conclusioni
   - Domande

Agenda

Motivazione



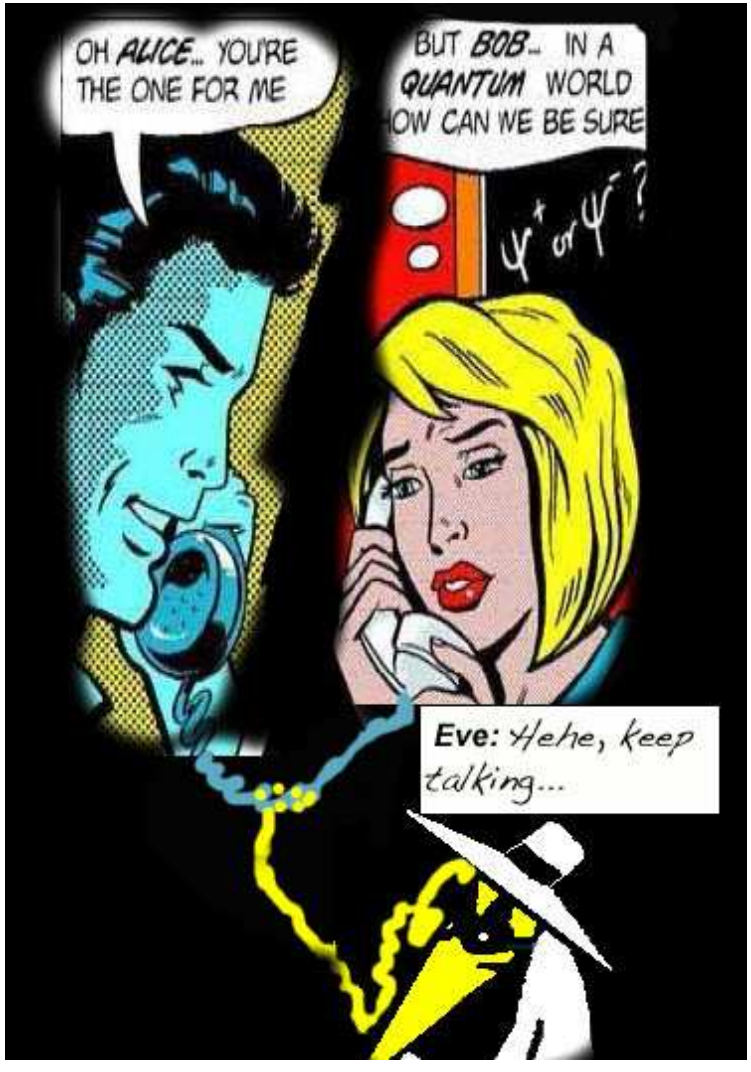
A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

Motivazione



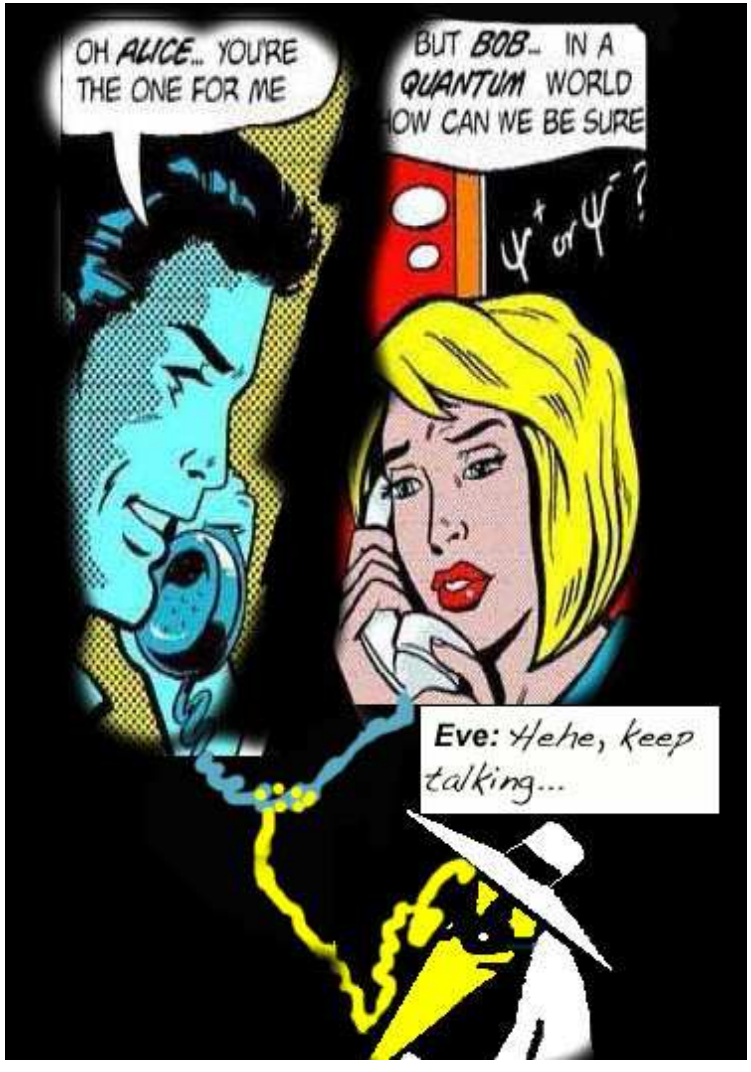
A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

Motivazione



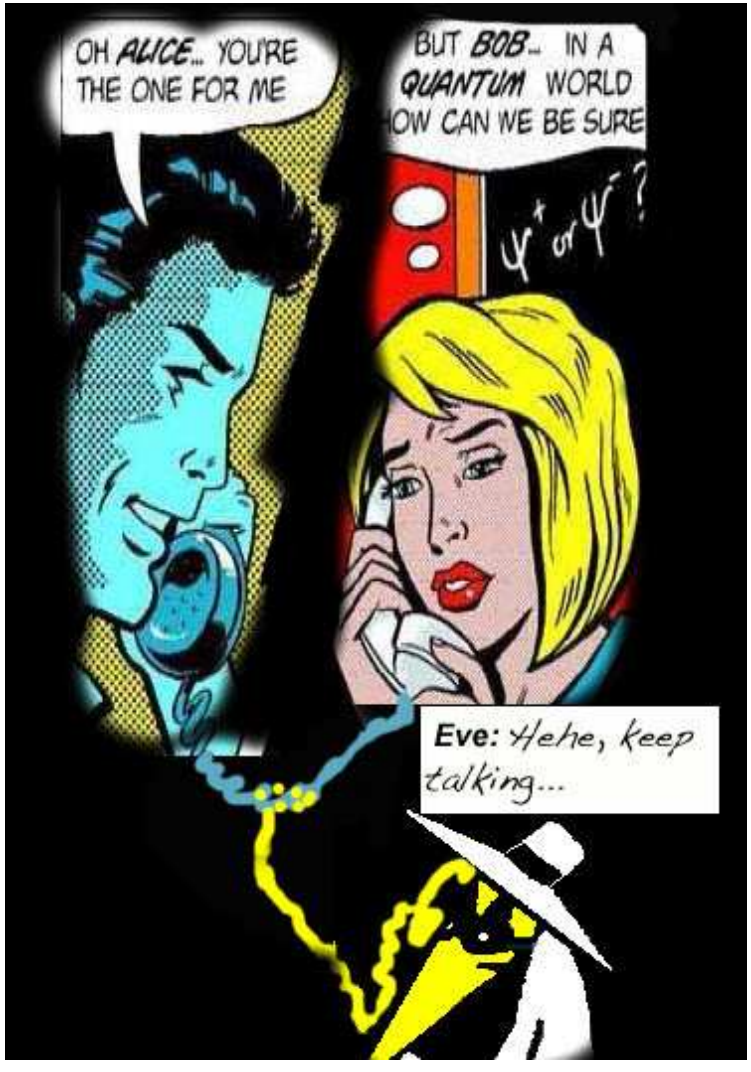
A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

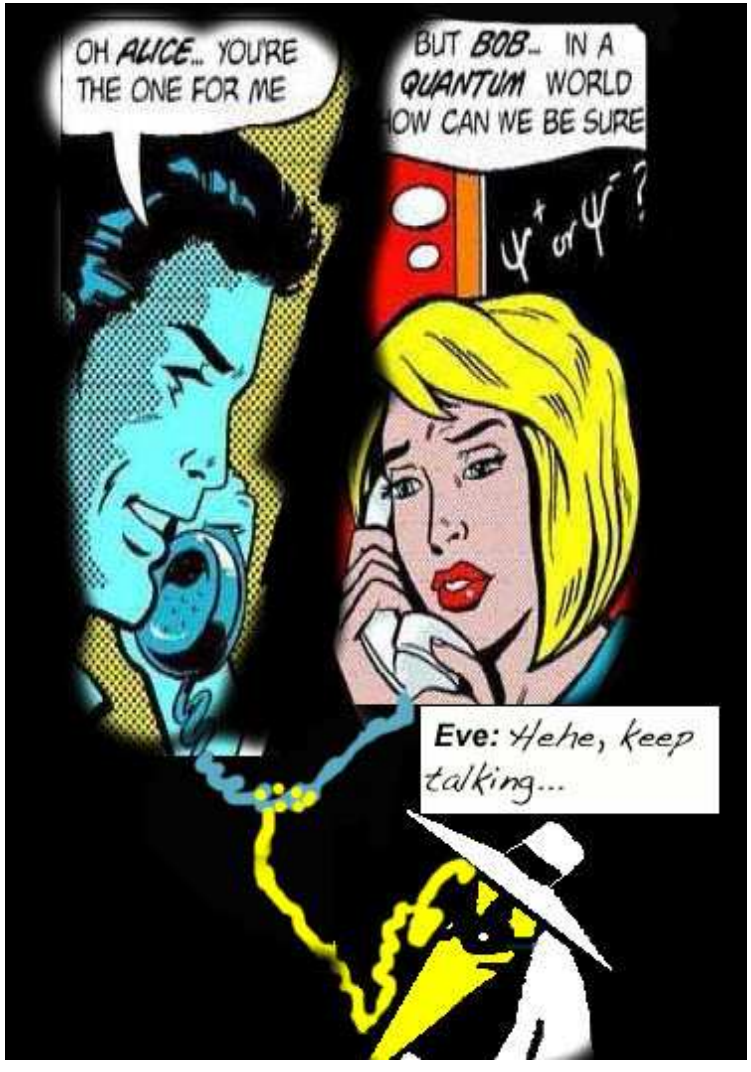
Motivazione



A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).
Domanda: come fare?
Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

Motivazione



A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Qualche definizione (etimologia)

Steganografia

Staganós + gráphein = coperto/protetto + scrivere: l'*arte di occultare un messaggio senza che attiri l'attenzione*

Crittografia

Kryptós + gráphein = nascosto + scrivere: l'*arte di scrivere messaggi segreti*

Crittanalisi

Kryptós + analýein = nascosto + scomporre: l'*arte di forzare (violare) un testo segreto*

Crittologia

Crittografia + crittanalisi

Differenza tra steganografia e crittografia

Ci troviamo di fronte a questi **due messaggi**:

1. *Squittio aumentato nell'osservare attentamente.*
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.
2. FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

Quale dei due attira di più i nostri sospetti?

Il primo sembra una cozzaglia di farneticazioni poco sensate che ci lasciano più o meno **indifferenti**;

il secondo sembra in qualche modo un codice o quantomeno qualcosa di **volutamente nascosto**

Differenza tra steganografia e crittografia

Ci troviamo di fronte a questi **due messaggi**:

1. *Squittio aumentato nell'osservare attentamente.*
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

2. FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

Quale dei due attira di più i nostri sospetti?

Il primo sembra una cozzaglia di farneticazioni poco sensate che ci lasciano più o meno **indifferenti**;

il secondo sembra in qualche modo un codice o quantomeno qualcosa di **volutamente nascosto**

Differenza tra steganografia e crittografia

Ci troviamo di fronte a questi **due messaggi**:

1. *Squittio aumentato nell'osservare attentamente.*
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

2. FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

Quale dei due attira di più i nostri sospetti?

Il primo sembra una cozzaglia di farneticazioni poco sensate che ci lasciano più o meno **indifferenti**;

il secondo sembra in qualche modo un codice o quantomeno qualcosa di **volutamente nascosto**

Differenza tra steganografia e crittografia

Ci troviamo di fronte a questi **due messaggi**:

1. *Squittio aumentato nell'osservare attentamente.*
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

2. FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

Quale dei due attira di più i nostri sospetti?

Il primo sembra una cozzaglia di farneticazioni poco sensate che ci lasciano più o meno **indifferenti**;
il secondo sembra in qualche modo un codice o quantomeno qualcosa di **volutamente nascosto**

Differenza tra steganografia e crittografia

Ci troviamo di fronte a questi **due messaggi**:

1. *Squittio aumentato nell'osservare attentamente.*
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

2. FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

Quale dei due attira di più i nostri sospetti?

Il primo sembra una cozzaglia di farneticazioni poco sensate che ci lasciano più o meno **indifferenti**;

il secondo sembra in qualche modo un codice o quantomeno qualcosa di **volutamente nascosto**

Differenza tra steganografia e crittografia

Ci troviamo di fronte a questi **due messaggi**:

1. *Squittio aumentato nell'osservare attentamente.*
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

2. FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

Quale dei due attira di più i nostri sospetti?

Il primo sembra una cozzaglia di farneticazioni poco sensate che ci lasciano più o meno **indifferenti**;

il secondo sembra in qualche modo un codice o quantomeno qualcosa di **volutamente nascosto**

Steganografia (1/3)

Primo messaggio: se evidenziamo la seconda lettera di ciascuna parola...

Squittio aumentato nell'osservare attentamente.
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

...si ottiene la sequenza

questoeunmessaggionascostotraleparole

ovvero

questo è un messaggio nascosto tra le parole

Steganografia (1/3)

Primo messaggio: se evidenziamo la seconda lettera di ciascuna parola...

Squittio aumentato nell'osservare attentamente.
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

...si ottiene la sequenza

questoeunmessaggionascostotraleparole

ovvero

questo è un messaggio nascosto tra le parole

Steganografia (1/3)

Primo messaggio: se evidenziamo la seconda lettera di ciascuna parola...

Squittio aumentato nell'osservare attentamente.
Non rendere automatico un ammortamento dell'assistenza assicurativa.
Mandare aggregati aggiungendo filato dorato.
Annichilire pacatamente asserendo, accettando sommessamente, ascoltando attentamente.
Comprare: attaccapanni, armadietto, paletta, glucosio, bevande, appendini.
Tartassare creativamente colleghi, alunni, genitori.

...si ottiene la sequenza

questoeunmessaggionascostotraleparole

ovvero

questo è un messaggio nascosto tra le parole

Steganografia (1/3)

Primo messaggio: se evidenziamo la seconda lettera di ciascuna parola...

*S**q**uittio a**u**mentato n**e**ll'o**s**servare a**t**tentamente.*
*N**o**n r**e**ndere a**u**tomatico u**n** a**m**mortamento d**e**ll'a**s**sistenza a**s**sicurativa.*
*M**a**ndare a**g**gregati a**g**giungendo f**i**lato d**o**rato.*
*A**n**nichilire p**a**catamente a**s**serendo, a**c**cettando s**o**mmessamente, a**s**coltando a**t**tentamente.*
*C**o**mprare: a**t**taccapanni, a**r**madietto, p**a**letta, g**l**ucosio, b**e**vande, a**p**pendini.*
*T**a**rtassare c**r**eativamente c**o**lleghi, a**l**unni, g**e**nitori.*

...si ottiene la sequenza

questoeunmessaggionascostotraleparole

ovvero

questo è un messaggio nascosto tra le parole

Steganografia (2/3)

- **Obiettivo**: non attrarre né attenzione né sospetti (usata da terroristi o nei paesi in cui la crittografia non è ammessa).
- **Debolezza**: se si intercetta il messaggero, basta un'attenta perquisizione per scovare il messaggio.
- Il **messaggio** è **nascosto** all'interno di: immagini (francobolli), lettere (corrispondenza), liste della spesa, puntini (sulle "i" e nei segni di punteggiatura), scritto con inchiostro invisibile sotto un messaggio insignificante, ecc.
- **Steganografia digitale**: in un file innoquo (immagine, file audio/video) si può trasmettere, ogni N byte un carattere alfabetico (come esempio precedente)... l'immagine o il file audio/video sembra inalterato!
- 440 a.C.: **Erodoto** racconta di un nobile persiano che fece tagliare a zero i capelli del suo schiavo più fidato, tatuò un messaggio sul suo cranio, una volta riscresciuti i capelli lo inviò con l'ordine di tagliarseli solo raggiunto il destinatario.

Steganografia (2/3)

- **Obiettivo**: non attrarre né attenzione né sospetti (usata da terroristi o nei paesi in cui la crittografia non è ammessa).
- **Debolezza**: se si intercetta il messaggero, basta un'attenta perquisizione per scovare il messaggio.
- Il **messaggio** è **nascosto** all'interno di: immagini (francobolli), lettere (corrispondenza), liste della spesa, puntini (sulle "i" e nei segni di punteggiatura), scritto con inchiostro invisibile sotto un messaggio insignificante, ecc.
- **Steganografia digitale**: in un file innoquo (immagine, file audio/video) si può trasmettere, ogni N byte un carattere alfabetico (come esempio precedente)... l'immagine o il file audio/video sembra inalterato!
- 440 a.C.: **Erodoto** racconta di un nobile persiano che fece tagliare a zero i capelli del suo schiavo più fidato, tatuò un messaggio sul suo cranio, una volta riscresciuti i capelli lo inviò con l'ordine di tagliarseli solo raggiunto il destinatario.

Steganografia (2/3)

- **Obiettivo**: non attrarre né attenzione né sospetti (usata da terroristi o nei paesi in cui la crittografia non è ammessa).
- **Debolezza**: se si intercetta il messaggero, basta un'attenta perquisizione per scovare il messaggio.
- Il **messaggio** è **nascosto** all'interno di: immagini (francobolli), lettere (corrispondenza), liste della spesa, puntini (sulle "i" e nei segni di punteggiatura), scritto con inchiostro invisibile sotto un messaggio insignificante, ecc.
- **Steganografia digitale**: in un file innoquo (immagine, file audio/video) si può trasmettere, ogni N byte un carattere alfabetico (come esempio precedente)... l'immagine o il file audio/video sembra inalterato!
- 440 a.C.: **Erodoto** racconta di un nobile persiano che fece tagliare a zero i capelli del suo schiavo più fidato, tatuò un messaggio sul suo cranio, una volta riscresciuti i capelli lo inviò con l'ordine di tagliarseli solo raggiunto il destinatario.

Steganografia (2/3)

- **Obiettivo**: non attrarre né attenzione né sospetti (usata da terroristi o nei paesi in cui la crittografia non è ammessa).
- **Debolezza**: se si intercetta il messaggero, basta un'attenta perquisizione per scovare il messaggio.
- Il **messaggio** è **nascosto** all'interno di: immagini (francobolli), lettere (corrispondenza), liste della spesa, puntini (sulle "i" e nei segni di punteggiatura), scritto con inchiostro invisibile sotto un messaggio insignificante, ecc.
- **Steganografia digitale**: in un file innoquo (immagine, file audio/video) si può trasmettere, ogni N byte un carattere alfabetico (come esempio precedente)... l'immagine o il file audio/video sembra inalterato!
- 440 a.C.: **Erodoto** racconta di un nobile persiano che fece tagliare a zero i capelli del suo schiavo più fidato, tatuò un messaggio sul suo cranio, una volta riscresciuti i capelli lo inviò con l'ordine di tagliarseli solo raggiunto il destinatario.

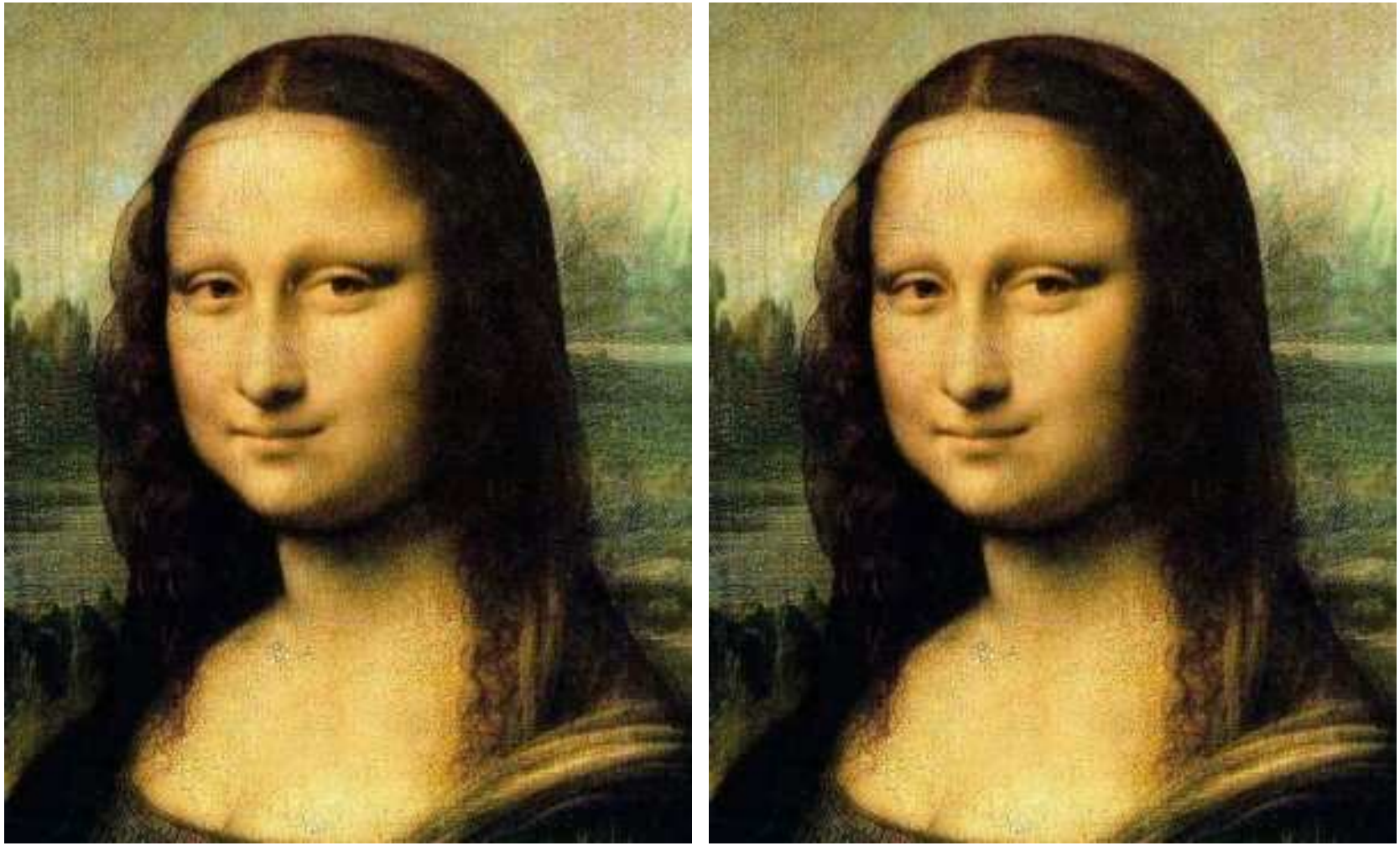
Steganografia (2/3)

- **Obiettivo**: non attrarre né attenzione né sospetti (usata da terroristi o nei paesi in cui la crittografia non è ammessa).
- **Debolezza**: se si intercetta il messaggero, basta un'attenta perquisizione per scovare il messaggio.
- Il **messaggio** è **nascosto** all'interno di: immagini (francobolli), lettere (corrispondenza), liste della spesa, puntini (sulle "i" e nei segni di punteggiatura), scritto con inchiostro invisibile sotto un messaggio insignificante, ecc.
- **Steganografia digitale**: in un file innoquo (immagine, file audio/video) si può trasmettere, ogni N byte un carattere alfabetico (come esempio precedente)... l'immagine o il file audio/video sembra inalterato!
- 440 a.C.: **Erodoto** racconta di un nobile persiano che fece tagliare a zero i capelli del suo schiavo più fidato, tatuò un messaggio sul suo cranio, una volta riscresciuti i capelli lo inviò con l'ordine di tagliarseli solo raggiunto il destinatario.

Steganografia (2/3)

- **Obiettivo**: non attrarre né attenzione né sospetti (usata da terroristi o nei paesi in cui la crittografia non è ammessa).
- **Debolezza**: se si intercetta il messaggero, basta un'attenta perquisizione per scovare il messaggio.
- Il **messaggio** è **nascosto** all'interno di: immagini (francobolli), lettere (corrispondenza), liste della spesa, puntini (sulle "i" e nei segni di punteggiatura), scritto con inchiostro invisibile sotto un messaggio insignificante, ecc.
- **Steganografia digitale**: in un file innoquo (immagine, file audio/video) si può trasmettere, ogni N byte un carattere alfabetico (come esempio precedente)... l'immagine o il file audio/video sembra inalterato!
- 440 a.C.: **Erodoto** racconta di un nobile persiano che fece tagliare a zero i capelli del suo schiavo più fidato, tatuò un messaggio sul suo cranio, una volta riscresciuti i capelli lo inviò con l'ordine di tagliarseli solo raggiunto il destinatario.

Steganografia (3/3)



Originale a sinistra, messaggio occultato a destra.

questo e un messaggio nascosto nella Gioconda, vedi

http://www.puremango.co.uk/php_steg.php

Agenda

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Crittografia: una classificazione

- **Trasposizione**: anagramma delle lettere (scitàla e tabelle con o senza chiave).
- Cifrari **monoalfabetici**: ad ogni lettera corrisponde un simbolo (cifrario di Atbash e di Cesare).
- Cifrari **polialfabetici**: ad ogni lettera corrispondono più simboli cambiati a ruota secondo una regola convenuta (il disco cifrante di Alberti, cifrario di Vigénère e di Vernam).
- Sistemi a **dizionario** o repertorio: alle parole più usate corrispondono dei simboli (nomenclatori), le altre sono cifrate lettera per lettera.
- **Sovracifratura**: il testo in chiaro viene cifrato in un modo (mono/poli-alfabetico) e poi il testo cifrato viene ricifrato in un altro modo (trasposizione).

Distinzione in **chiave segreta** e **chiave pubblica**.

Trasposizione: la scitàla (bastone) lacedemonica

Il metodo di **crittografia per trasposizione più antico** conosciuto. Molto usato dagli Spartani, secondo Plutarco (*Vita di Lisandro*) utilizzata da Lisandro nel 404 a.C. in un episodio risolutivo della Guerra del Peloponneso.

Trasposizione: la scitàla (bastone) lacedemonica

Il metodo di **crittografia per trasposizione più antico** conosciuto. Molto usato dagli Spartani, secondo Plutarco (*Vita di Lisandro*) utilizzata da Lisandro nel 404 a.C. in un episodio risolutivo della Guerra del Peloponneso.

Trasposizione: tabella con chiave

Testo in chiaro da trasporre:
la matematica non solo è molto bella ma anche molto utile

L	O	G	A	R	I	T	M	O
4	6	2	1	8	3	9	5	7
L	A	M	A	T	E	M	A	T
I	C	A	N	O	N	S	O	L
O	E	M	O	L	T	O	B	E
L	L	A	M	A	A	N	C	H
E	M	O	L	T	O	U	T	I
L	E							

Testo trasposto:
anoml-mamao-entao-liolel-aobct-acelme-tlehi-tolat-msonu

Trasposizione: tabella con chiave

Testo in chiaro da trasporre:
la matematica non solo è molto bella ma anche molto utile

L	O	G	A	R	I	T	M	O
4	6	2	1	8	3	9	5	7
L	A	M	A	T	E	M	A	T
I	C	A	N	O	N	S	O	L
O	E	M	O	L	T	O	B	E
L	L	A	M	A	A	N	C	H
E	M	O	L	T	O	U	T	I
L	E							

Testo trasposto:
anoml-mamao-entao-liolel-aobct-acelme-tlehi-tolat-msonu

Trasposizione: tabella con chiave

Testo in chiaro da trasporre:
la matematica non solo è molto bella ma anche molto utile

L	O	G	A	R	I	T	M	O
4	6	2	1	8	3	9	5	7
L	A	M	A	T	E	M	A	T
I	C	A	N	O	N	S	O	L
O	E	M	O	L	T	O	B	E
L	L	A	M	A	A	N	C	H
E	M	O	L	T	O	U	T	I
L	E							

Testo trasposto:
anoml-mamao-entao-liolel-aobct-acelme-tlehi-tolat-msonu

Trasposizione: tabella con chiave

Testo in chiaro da trasporre:
la matematica non solo è molto bella ma anche molto utile

L	O	G	A	R	I	T	M	O
4	6	2	1	8	3	9	5	7
L	A	M	A	T	E	M	A	T
I	C	A	N	O	N	S	O	L
O	E	M	O	L	T	O	B	E
L	L	A	M	A	A	N	C	H
E	M	O	L	T	O	U	T	I
L	E							

Testo trasposto:
anoml-mamao-entao-liolel-aobct-acelme-tlehi-tolat-msonu

Trasposizione: tabella con chiave

Testo in chiaro da trasporre:
la matematica non solo è molto bella ma anche molto utile

L	O	G	A	R	I	T	M	O
4	6	2	1	8	3	9	5	7
L	A	M	A	T	E	M	A	T
I	C	A	N	O	N	S	O	L
O	E	M	O	L	T	O	B	E
L	L	A	M	A	A	N	C	H
E	M	O	L	T	O	U	T	I
L	E							

Testo trasposto:
anoml-mamao-entao-liolel-aobct-acelme-tlehi-tolat-msonu

Sostituzione: il cifrario (monoalfabetico) Atbash

L'**atbash** è un semplice *cifrario a sostituzione monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

A B C D E H I J K L M N O P Q R S T U V W X Y Z
Z Y X W V S R Q P O N M L K J I H G F E D C B A

Usato nel libro di Geremia per codificare le parole *Kasdim* (Caldei) in *Leb Kamai* e *Babel* (Babele) in *Sheshakh*.
Origine di Atbash: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atbash*. Il testo

XRUIZGFIZGIZNRGVROXRUIZIRLZGYZHS

significa

CIFRATURA TRAMITE IL CIFRARIO ATBASH

Sostituzione: il cifrario (monoalfabetico) Atbash

L'**atbash** è un semplice *cifrario a sostituzione monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Usato nel libro di Geremia per codificare le parole *Kasdim* (Caldei) in *Leb Kamai* e *Babel* (Babele) in *Sheshakh*.
Origine di Atbash: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atbash*. Il testo

XRUIZGFIZGIZNRGVROXRUIZIRLZGYZHS

significa

CIFRATURA TRAMITE IL CIFRARIO ATBASH

Sostituzione: il cifrario (monoalfabetico) Atbash

L'**atbash** è un semplice *cifrario a sostituzione monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Usato nel libro di Geremia per codificare le parole *Kasdim* (Caldei) in *Leb Kamai* e *Babel* (Babele) in *Sheshakh*.

Origine di Atbash: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atbash*. Il testo

XRUIZGFIZGIZNRGVROXRUIZIRLZGYZHS

significa

CIFRATURA TRAMITE IL CIFRARIO ATBASH

Sostituzione: il cifrario (monoalfabetico) Atbash

L'**atbash** è un semplice *cifrario a sostituzione monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Usato nel libro di Geremia per codificare le parole *Kasdim* (Caldei) in *Leb Kamai* e *Babel* (Babele) in *Sheshakh*.
Origine di Atbash: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atbash*. Il testo

XRUIZGFIZGIZNRGVROXRUIZIRLZGYZHS

significa

CIFRATURA TRAMITE IL CIFRARIO ATBASH

Sostituzione: il cifrario (monoalfabetico) Atbash

L'**atbash** è un semplice *cifrario a sostituzione monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Usato nel libro di Geremia per codificare le parole *Kasdim* (Caldei) in *Leb Kamai* e *Babel* (Babele) in *Sheshakh*.
Origine di Atbash: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atbash*. Il testo

XRUIZGFIZGIZNRGVROXRUIZIRLZGYZHS

significa

CIFRATURA TRAMITE IL CIFRARIO ATBASH

Sostituzione: il cifrario (monoalfabetico) Atbash

L'**atbash** è un semplice *cifrario a sostituzione monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Usato nel libro di Geremia per codificare le parole *Kasdim* (Caldei) in *Leb Kamai* e *Babel* (Babele) in *Sheshakh*.
Origine di Atbash: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atbash*. Il testo

XRUIZGFIZGIZNRGVROXRUIZIRLZGYZHS

significa

CIFRATURA TRAMITE IL CIFRARIO ATBASH

Sostituzione: il cifrario (monoalfabetico) di Cesare

Svetonio in *De Vita Caesarum* racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice di sostituzione spostando a destra di 3 caselle ogni lettera.

A B C D E H I J K L M N O P Q R S T U V W X Y Z
D E F G H K L M N O P Q R S T U V W X Y Z A B C

Usato anche da Provenzano per proteggere informazioni rilevanti scritte nei suoi *pizzini*, però le lettere erano sostituite dai numeri (1 per A, 2 per B, ecc.) e poi sommati a 3.
Con il cifrario di Cesare, il testo

FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

significa

CIFRATURA TRAMITE IL CIFRARIO DI CESARE

Sostituzione: il cifrario (monoalfabetico) di Cesare

Svetonio in *De Vita Caesarum* racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice di sostituzione spostando a destra di 3 caselle ogni lettera.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Usato anche da Provenzano per proteggere informazioni rilevanti scritte nei suoi *pizzini*, però le lettere erano sostituite dai numeri (1 per A, 2 per B, ecc.) e poi sommati a 3.
Con il cifrario di Cesare, il testo

FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

significa

CIFRATURA TRAMITE IL CIFRARIO DI CESARE

Sostituzione: il cifrario (monoalfabetico) di Cesare

Svetonio in *De Vita Caesarum* racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice di sostituzione spostando a destra di 3 caselle ogni lettera.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Usato anche da Provenzano per proteggere informazioni rilevanti scritte nei suoi *pizzini*, però le lettere erano sostituite dai numeri (1 per A, 2 per B, ecc.) e poi sommati a 3.

Con il cifrario di Cesare, il testo

FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

significa

CIFRATURA TRAMITE IL CIFRARIO DI CESARE

Sostituzione: il cifrario (monoalfabetico) di Cesare

Svetonio in *De Vita Caesarum* racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice di sostituzione spostando a destra di 3 caselle ogni lettera.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Usato anche da Provenzano per proteggere informazioni rilevanti scritte nei suoi *pizzini*, però le lettere erano sostituite dai numeri (1 per A, 2 per B, ecc.) e poi sommati a 3.
Con il cifrario di Cesare, il testo

FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

significa

CIFRATURA TRAMITE IL CIFRARIO DI CESARE

Sostituzione: il cifrario (monoalfabetico) di Cesare

Svetonio in *De Vita Caesarum* racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice di sostituzione spostando a destra di 3 caselle ogni lettera.

A	B	C	D	E	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Usato anche da Provenzano per proteggere informazioni rilevanti scritte nei suoi *pizzini*, però le lettere erano sostituite dai numeri (1 per A, 2 per B, ecc.) e poi sommati a 3.
Con il cifrario di Cesare, il testo

FLIUDWXUDWUDPLWHLOFLIUDULRGLFHVDUH

significa

CIFRATURA TRAMITE IL CIFRARIO DI CESARE

Crittanalisi: dato un testo...

Quel ramo del lago di Como, che volge a mezzogiorno, tra due catene non interrotte di monti, tutto a seni e a golfi, a seconda dello sporgere e del rientrare di quelli, vien, quasi a un tratto, a ristringersi, e a prender corso e figura di fiume, tra un promontorio a destra, e un'ampia costiera dall'altra parte; e il ponte, che ivi congiunge le due rive, par che renda ancor più sensibile all'occhio questa trasformazione, e segni il punto in cui il lago cessa, e l'Adda rincomincia, per ripigliar poi nome di lago dove le rive, allontanandosi di nuovo, lascian l'acqua distendersi e rallentarsi in nuovi golfi e in nuovi seni. La costiera, formata dal deposito di tre grossi torrenti, scende appoggiata a due monti contigui, l'uno detto di san Martino, l'altro, con voce lombarda, il Resegone, dai molti suoi cocuzzoli in fila, che in vero lo fanno somigliare a una sega: talché non è chi, al primo vederlo, purché sia di fronte, come per esempio di su le mura di Milano che guardano a settentrione, non lo discerna tosto, a un tal contrassegno, in quella lunga e vasta giogaia, dagli altri monti di nome più oscuro e di forma più comune.

...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

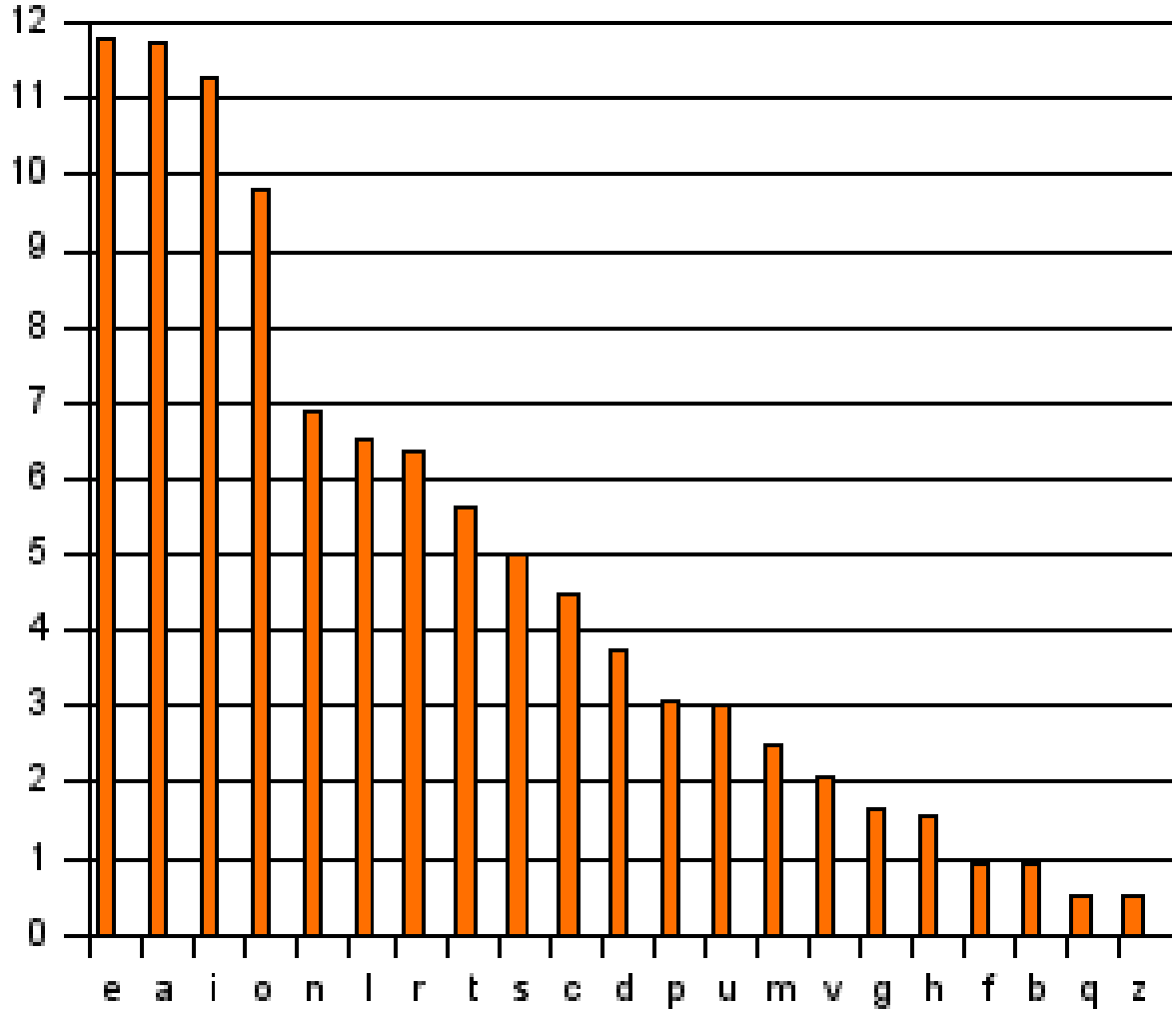
...analizziamo la frequenza di ogni lettera

1	i	98	10.76%
2	e	98	10.76%
3	o	92	10.10%
4	a	91	9.99%
5	n	73	8.01%
6	r	64	7.03%
7	l	56	6.15%
8	t	53	5.82%
9	s	42	4.61%
10	d	40	4.39%
11	u	37	4.06%
12	c	35	3.84%
13	g	27	2.96%
14	m	25	2.74%
15	p	21	2.31%
17	v	13	1.43%
18	f	10	1.10%
19	h	9	0.99%
20	q	6	0.66%
21	z	5	0.55%
22	b	2	0.22%

- Si contano le lettere totali nel testo
- Si conta quante volte ogni lettera compare
- Si calcola la frequenza come percentuale
- In Italiano alcune lettere sono molto più frequenti di altre...
- ...quindi per decifrare un **messaggio sufficientemente lungo** basta iniziare dalle lettere più frequenti...
- Conclusione: **la crittografia per sostituzione monoalfabetica non è per nulla sicura!**

Crittanalisi: analisi delle frequenze (1/2)

Se analizziamo la frequenze delle singole lettere in italiano si trova...



Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Crittanalisi: analisi delle frequenze (2/2)

- Oltre alla frequenza degli **unigrammi** (singole lettere) si può analizzare la frequenza di **bigrammi** (due lettere consecutive) e **trigrammi** (tre lettere consecutive).
- Per esempio, in italiano la lettera **Q** è sempre *seguita* dalla lettera **U**, mentre la **H** è sempre *preceduta* da **C** o **G**.
- Per effettuare una crittananalisi statistica il **crittogramma** deve essere **sufficientemente lungo**.
- La **crittananalisi statistica** utilizza strumenti matematici molto semplici e può *tranquillamente* decifrare un crittogramma ottenuto con sostiruzione monoalfabetica.
- Alternative:
  (a) aggiungere lettere inutili ogni tanto, specialmente quelle che compaiono poco frequentemente come **F B Q Z**
  (b) cambiare la corrispondenza dei simboli (alfabeto) dopo qualche lettera

Sostituzione: il disco cifrante di L. B. Alberti (1404-72)

Disco esterno: fisso, numeri 1, 2, 3, 4 + alfabeto in chiaro (20 lettere maiuscole escluse J, K, Y, W, Q, H (bassa frequenza).
Disco interno: mobile, alfabeto di ventiquattro lettere (esclusa W e U=V) scritte **disordinatamente**, e **l'ordine deve rimanere segreto**

Sostituzione: il disco cifrante di L. B. Alberti (1404-72)

Disco esterno: fisso, numeri 1, 2, 3, 4 + alfabeto in chiaro (20 lettere maiuscole escluse J, K, Y, W, Q, H (bassa frequenza).

Disco interno: mobile, alfabeto di ventiquattro lettere (esclusa W e U=V) scritte **disordinatamente**, e **l'ordine deve rimanere segreto**

Sostituzione: il disco cifrante di L. B. Alberti (1404-72)

Disco esterno: fisso, numeri 1, 2, 3, 4 + alfabeto in chiaro (20 lettere maiuscole escluse J, K, Y, W, Q, H (bassa frequenza).
Disco interno: mobile, alfabeto di ventiquattro lettere (esclusa W e U=V) scritte **disordinatamente**, e **l'ordine deve rimanere segreto**

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I

g m e o t i e d r t l h v g n c m k p & a

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.

AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Funzionamento del disco cifrante (polialfabetico)

ARRIVANO I RINFORZI: testo in chiaro.
AR4RIVA1NOI3RINF2ORZI: togliamo spazi, inseriamo *a caso* numeri da 1 a 4 dividendo doppie e bi/tri-grammi comuni.

```
A R 4 R I V A 1 N O I 3 R I N F 2 O R Z I
g m e o t i e d r t l h v g n c m k p & a
```

Vantaggi del disco cifrante (polialfabetico)

- Le lettere interne sono **disposte a caso**, pertanto i possibili dischi interni (dischi cifranti) sono $26! \approx 4 \times 10^{26}$
- Se i due interlocutori avessero anche solo 365 **dischi cifranti diversi** potrebbero usarne uno diverso per ogni giorno dell'anno facendo impazzire i crittanalisti!
- L'**alfabeto cifrante cambia** $\Rightarrow$ **cifrario polialfabetico**: crittanalisi statistica molto difficile, soprattutto se i dischi cifranti cambiano ogni giorno
- Inserendo nel testo in chiaro un **numero dopo ogni lettera** si hanno tanti alfabeti cifranti quanti il numero di caratteri del testo in chiaro: la crittanalisi statistica diventa veramente dura!

I dischi cifranti di L. B. Alberti sono **rimasti sconosciuti** per molto tempo (per suo stesso volere), ma sono **superiori ad altri cifrari polialfabetici** impiegati nei secoli successivi.

Vantaggi del disco cifrante (polialfabetico)

- Le lettere interne sono **disposte a caso**, pertanto i possibili dischi interni (dischi cifranti) sono $26! \approx 4 \times 10^{26}$
- Se i due interlocutori avessero anche solo 365 **dischi cifranti diversi** potrebbero usarne uno diverso per ogni giorno dell'anno facendo impazzire i crittanalisti!
- L'**alfabeto cifrante cambia** $\Rightarrow$ **cifrario polialfabetico**: crittanalisi statistica molto difficile, soprattutto se i dischi cifranti cambiano ogni giorno
- Inserendo nel testo in chiaro un **numero dopo ogni lettera** si hanno tanti alfabeti cifranti quanti il numero di caratteri del testo in chiaro: la crittanalisi statistica diventa veramente dura!

I dischi cifranti di L. B. Alberti sono **rimasti sconosciuti** per molto tempo (per suo stesso volere), ma sono **superiori ad altri cifrari polialfabetici** impiegati nei secoli successivi.

Vantaggi del disco cifrante (polialfabetico)

- Le lettere interne sono **disposte a caso**, pertanto i possibili dischi interni (dischi cifranti) sono $26! \approx 4 \times 10^{26}$
- Se i due interlocutori avessero anche solo 365 **dischi cifranti diversi** potrebbero usarne uno diverso per ogni giorno dell'anno facendo impazzire i crittanalisti!
- L'**alfabeto cifrante cambia** $\Rightarrow$ **cifrario polialfabetico**: crittanalisi statistica molto difficile, soprattutto se i dischi cifranti cambiano ogni giorno
- Inserendo nel testo in chiaro un **numero dopo ogni lettera** si hanno tanti alfabeti cifranti quanti il numero di caratteri del testo in chiaro: la crittanalisi statistica diventa veramente dura!

I dischi cifranti di L. B. Alberti sono **rimasti sconosciuti** per molto tempo (per suo stesso volere), ma sono **superiori ad altri cifrari polialfabetici** impiegati nei secoli successivi.

Vantaggi del disco cifrante (polialfabetico)

- Le lettere interne sono **disposte a caso**, pertanto i possibili dischi interni (dischi cifranti) sono $26! \approx 4 \times 10^{26}$
- Se i due interlocutori avessero anche solo 365 **dischi cifranti diversi** potrebbero usarne uno diverso per ogni giorno dell'anno facendo impazzire i crittanalisti!
- L'**alfabeto cifrante cambia** $\Rightarrow$ **cifrario polialfabetico**: crittanalisi statistica molto difficile, soprattutto se i dischi cifranti cambiano ogni giorno
- Inserendo nel testo in chiaro un **numero dopo ogni lettera** si hanno tanti alfabeti cifranti quanti il numero di caratteri del testo in chiaro: la crittanalisi statistica diventa veramente dura!

I dischi cifranti di L. B. Alberti sono **rimasti sconosciuti** per molto tempo (per suo stesso volere), ma sono **superiori ad altri cifrari polialfabetici** impiegati nei secoli successivi.

Vantaggi del disco cifrante (polialfabetico)

- Le lettere interne sono **disposte a caso**, pertanto i possibili dischi interni (dischi cifranti) sono $26! \approx 4 \times 10^{26}$
- Se i due interlocutori avessero anche solo 365 **dischi cifranti diversi** potrebbero usarne uno diverso per ogni giorno dell'anno facendo impazzire i crittanalisti!
- L'**alfabeto cifrante cambia** $\Rightarrow$ **cifrario polialfabetico**: crittanalisi statistica molto difficile, soprattutto se i dischi cifranti cambiano ogni giorno
- Inserendo nel testo in chiaro un **numero dopo ogni lettera** si hanno tanti alfabeti cifranti quanti il numero di caratteri del testo in chiaro: la crittanalisi statistica diventa veramente dura!

I dischi cifranti di L. B. Alberti sono **rimasti sconosciuti** per molto tempo (per suo stesso volere), ma sono **superiori ad altri cifrari polialfabetici** impiegati nei secoli successivi.

Vantaggi del disco cifrante (polialfabetico)

- Le lettere interne sono **disposte a caso**, pertanto i possibili dischi interni (dischi cifranti) sono $26! \approx 4 \times 10^{26}$
- Se i due interlocutori avessero anche solo 365 **dischi cifranti diversi** potrebbero usarne uno diverso per ogni giorno dell'anno facendo impazzire i crittanalisti!
- L'**alfabeto cifrante cambia** $\Rightarrow$ **cifrario polialfabetico**: crittanalisi statistica molto difficile, soprattutto se i dischi cifranti cambiano ogni giorno
- Inserendo nel testo in chiaro un **numero dopo ogni lettera** si hanno tanti alfabeti cifranti quanti il numero di caratteri del testo in chiaro: la crittanalisi statistica diventa veramente dura!

I dischi cifranti di L. B. Alberti sono **rimasti sconosciuti** per molto tempo (per suo stesso volere), ma sono **superiori ad altri cifrari polialfabetici** impiegati nei secoli successivi.

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**

```
ARRIVANOIRINFORZI
VERMEVERMEVERMEVE
VVIUZVRFUVDRWAVUM
```

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**

   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Sostituzione: il cifrario (polialfabetico) di Vigènére

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

1. 1518: Tritemio, **tabula recta**
2. 1553: Belaso, **parola chiave**
3. 1586: Vigènére, variante: **fama immeritata**
4. **Funzionamento**:
   Testo: *Arrivano i rinforzi*
   Chiave: **VERME**
   ARRIVANOIRINFORZI
   VERMEVERMEVERMEVE
   VVIUZVRFUVDRWAVUM

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Vantaggi/svantaggi del cifrario di Vigènére

+ È **polialfabetico**, quindi la crittanalisi statistica è difficile
+ È **semplice**, nessun marchingegno fisico
– Gli **alfabeti** che si usano sono tanti quanti le lettere della parola-chiave: se è corta sono **pochi**!
– Gli **alfabeti si ripetono ciclicamente** per cui, individuata la lunghezza della chiave, la crittanalisi statistica ha certamente successo

- Questo cifrario funziona tanto meglio quanto più **lunga** è la parola-chiave, che può diventare una **frase-chiave**.
- 1863 Friedrich **Kasiski** pubblicò per primo una tecnica generale per la **decrittazione**, tuttavia già prima qualche crittanalista bravo c'era riuscito.

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???

Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!

La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.

Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!

La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Sostituzione: il cifrario (polialfabetico) di Vernam

Domanda: esiste il cifrario inviolabile???
Risposta: **SÌ!!!**

...purché:

1. La parola-chiave (frase-chiave) sia **lunga** tanto **quanto il messaggio** da mandare
2. La parola-chiave sia generata in modo del tutto **casuale**
3. La parola-chiave venga usata **una sola volta** (*One-time pad*)

Un cifrario con queste caratteristiche si chiama **cifrario di Vernam** (idea del 1917, brevettata nel 1919) e si dimostra essere **INVIOLABILE** (Shannon, 1949)!
La **forza** del cifrario è nei criteri di scelta della **parola-chiave**.
Sembra sia stato usato durante la **guerra fredda** dai servizi segreti dell'Est, per il **telefono rosso** tra Washington e Mosca, e uno simile da **Che Guevara** (1967).

Agenda

Crittografia simmetrica (chiave privata)

Per tutti i cifrari visti fin qui (**crittografia simmetrica**):

- \+ sia la cifratura che la decifratura sono **veloci**
- – problema di **concordare** la chiave tra i due interlocutori, soprattutto se viene cambiata spesso (canale sicuro?)
- – la chiave di *decifratura* è facilmente deducibile da quella di *cifratura* (in generale **la chiave è la stessa**)
- – assoluta necessità di **segretezza**

Crittografia simmetrica (chiave privata)

Per tutti i cifrari visti fin qui (**crittografia simmetrica**):

+ sia la cifratura che la decifratura sono **veloci**
– problema di **concordare** la chiave tra i due interlocutori, soprattutto se viene cambiata spesso (canale sicuro?)
– la chiave di *decifratura* è facilmente deducibile da quella di *cifratura* (in generale **la chiave è la stessa**)
– assoluta necessità di **segretezza**

Crittografia simmetrica (chiave privata)

Per tutti i cifrari visti fin qui (**crittografia simmetrica**):

+ sia la cifratura che la decifratura sono **veloci**
– problema di **concordare** la chiave tra i due interlocutori, soprattutto se viene cambiata spesso (canale sicuro?)
– la chiave di *decifratura* è facilmente deducibile da quella di *cifratura* (in generale **la chiave è la stessa**)
– assoluta necessità di **segretezza**

Crittografia simmetrica (chiave privata)

Per tutti i cifrari visti fin qui (**crittografia simmetrica**):

+ sia la cifratura che la decifratura sono **veloci**
– problema di **concordare** la chiave tra i due interlocutori, soprattutto se viene cambiata spesso (canale sicuro?)
– la chiave di *decifratura* è facilmente deducibile da quella di *cifratura* (in generale **la chiave è la stessa**)
– assoluta necessità di **segretezza**

Crittografia simmetrica (chiave privata)

Per tutti i cifrari visti fin qui (**crittografia simmetrica**):

- \+ sia la cifratura che la decifratura sono **veloci**
- – problema di **concordare** la chiave tra i due interlocutori, soprattutto se viene cambiata spesso (canale sicuro?)
- – la chiave di *decifratura* è facilmente deducibile da quella di *cifratura* (in generale **la chiave è la stessa**)
- – assoluta necessità di **segretezza**

Crittografia asimmetrica (chiave privata+pubblica)

Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

Crittografia asimmetrica (chiave privata+pubblica)

Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

Crittografia asimmetrica (chiave privata+pubblica)

Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

Crittografia asimmetrica (chiave privata+pubblica)

Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

Crittografia asimmetrica (chiave privata+pubblica)

Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

Crittografia asimmetrica (chiave privata+pubblica)

Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

Crittografia asimmetrica (chiave privata+pubblica)

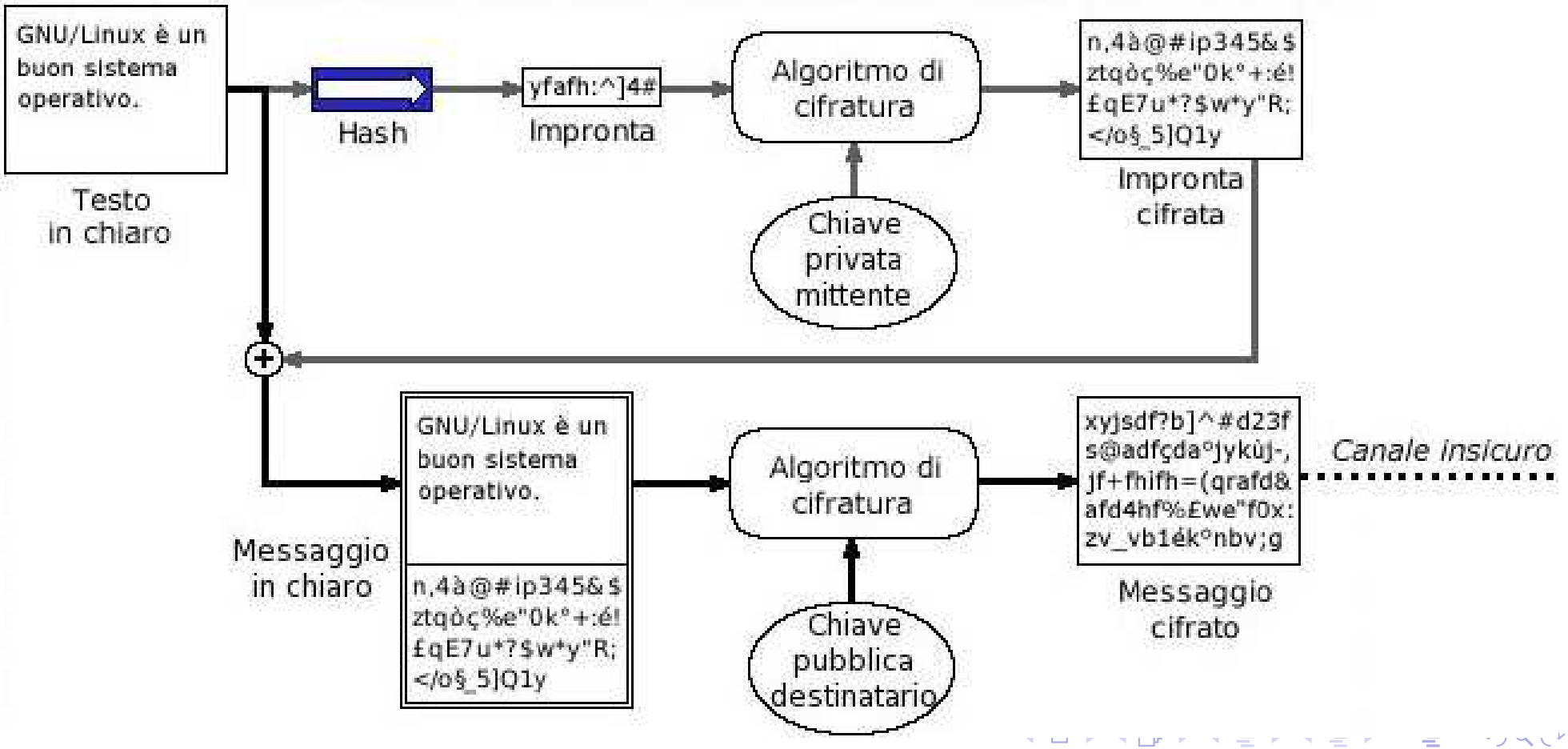
Alternativa: **crittografia asimmetrica**

+ due chiavi: la **chiave pubblica** chiude il lucchetto, la la **chiave privata** lo apre (asimmetria)
+ **tutti conoscono la chiave pubblica** di tutti
+ non esiste il problema di **concordare** la chiave
+ la chiave di *decifratura* (privata) **non è facilmente deducibile** da quella di *cifratura* (pubblica)
+ un testo cifrato con chiave pubblica è decifrabile **solo** con la chiave privata e **viceversa**
– sia la cifratura che la decifratura sono **piuttosto lenti**

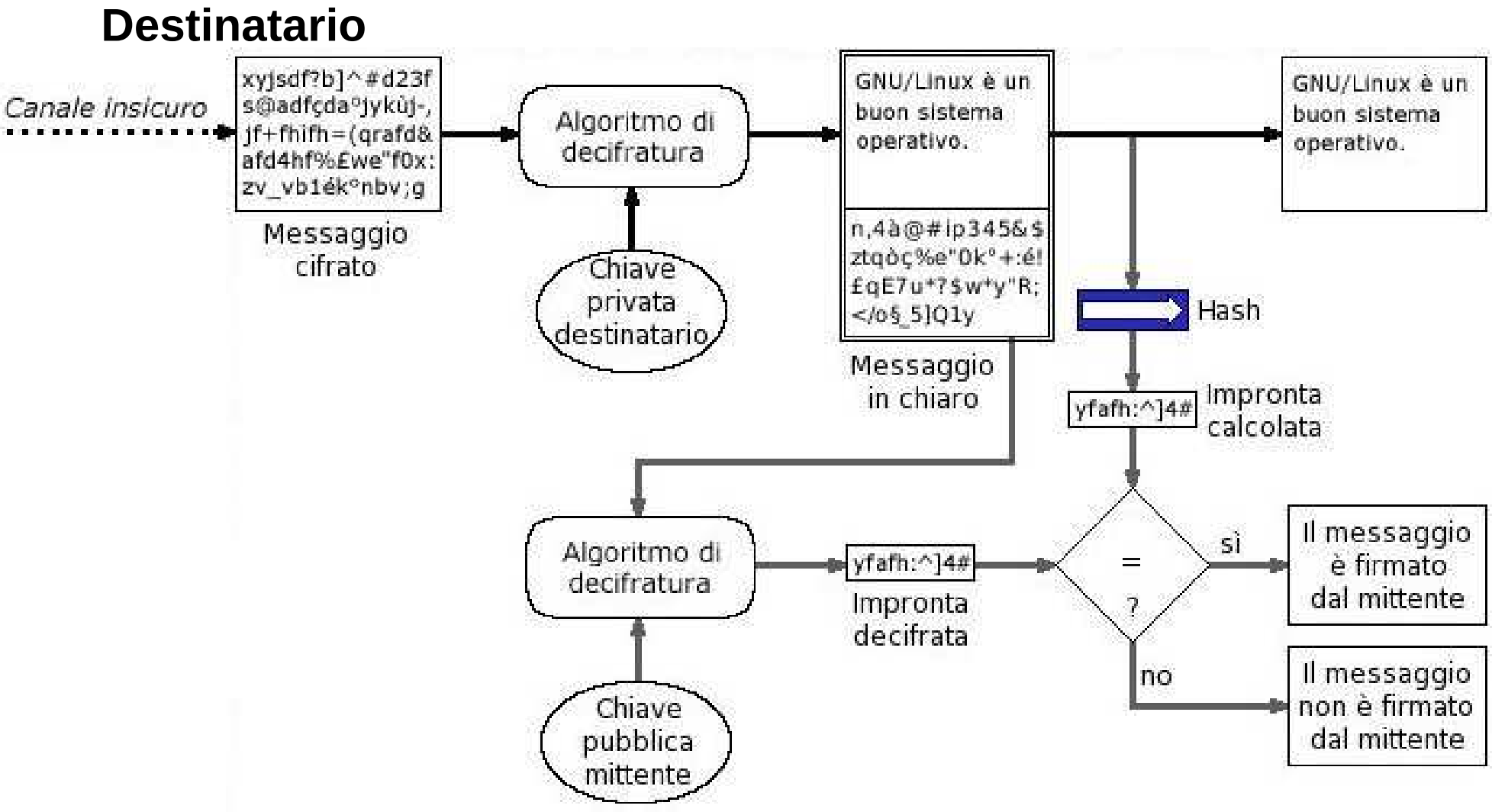
Firma digitale e autenticazione (1/2)

Come fa Bob a sapere che il messaggio è stato mandato proprio da Alice e non da Eve?

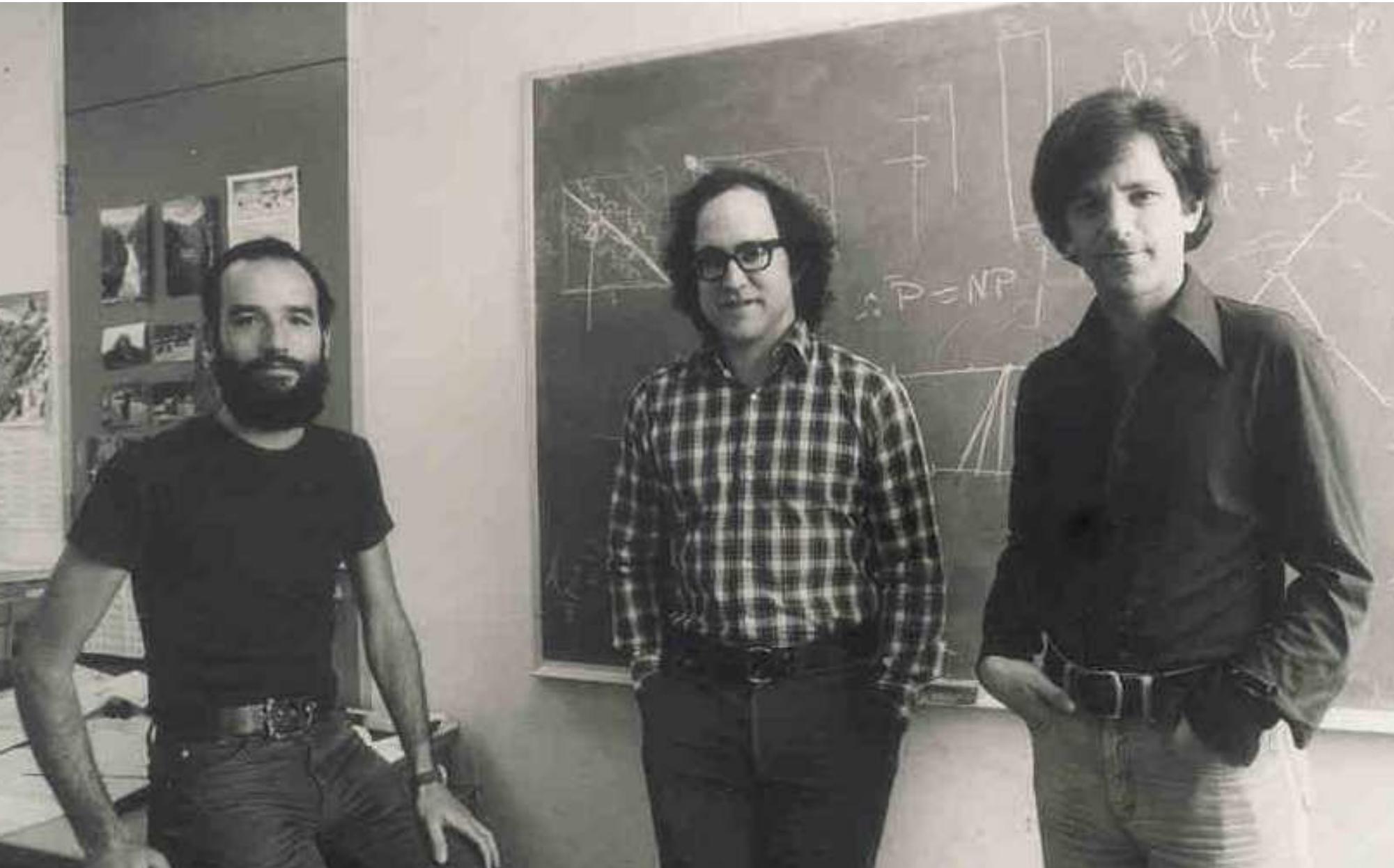
Mittente



Firma digitale e autenticazione (2/2)



RSA – Rivest Shamir Adleman, 1977, MIT



RSA – Rivest Shamir Adleman, 1977, MIT

- La crittografia con chiavi pubblica e privata si basa sull'ipotesi che la **chiave privata è difficilmente ricostruibile** a partire da quella pubblica: cosa vuol dire?
- Vuol dire che, con le conoscenze teoriche a noi note e con la potenza di calcolo oggi disponibile **ci vorrebbe troppo tempo**, da qualche decina a centinaia di anni (o più), dipende dalla lunghezza della chiave pubblica
- **Rivest Shamir Adleman** nel 1977 inventarono l'**algoritmo RSA**, oggi universalmente usato. Si basa sul fatto che fattorizzare un numero di centinaia di cifre come prodotto di due numeri primi è un'**operazione molto onerosa** (anche oggi)

$\Rightarrow$ **abbiamo bisogno di un po' di matematica per capirne il perché...**

RSA – Rivest Shamir Adleman, 1977, MIT

- La crittografia con chiavi pubblica e privata si basa sull'ipotesi che la **chiave privata è difficilmente ricostruibile** a partire da quella pubblica: cosa vuol dire?
- Vuol dire che, con le conoscenze teoriche a noi note e con la potenza di calcolo oggi disponibile **ci vorrebbe troppo tempo**, da qualche decina a centinaia di anni (o più), dipende dalla lunghezza della chiave pubblica
- **Rivest Shamir Adleman** nel 1977 inventarono l'**algoritmo RSA**, oggi universalmente usato. Si basa sul fatto che fattorizzare un numero di centinaia di cifre come prodotto di due numeri primi è un'**operazione molto onerosa** (anche oggi)

$\Rightarrow$ **abbiamo bisogno di un po' di matematica per capirne il perché...**

RSA – Rivest Shamir Adleman, 1977, MIT

- La crittografia con chiavi pubblica e privata si basa sull'ipotesi che la **chiave privata è difficilmente ricostruibile** a partire da quella pubblica: cosa vuol dire?
- Vuol dire che, con le conoscenze teoriche a noi note e con la potenza di calcolo oggi disponibile **ci vorrebbe troppo tempo**, da qualche decina a centinaia di anni (o più), dipende dalla lunghezza della chiave pubblica
- **Rivest Shamir Adleman** nel 1977 inventarono l'**algoritmo RSA**, oggi universalmente usato. Si basa sul fatto che fattorizzare un numero di centinaia di cifre come prodotto di due numeri primi è un'**operazione molto onerosa** (anche oggi)

$\Rightarrow$ **abbiamo bisogno di un po' di matematica per capirne il perché...**

RSA – Rivest Shamir Adleman, 1977, MIT

- La crittografia con chiavi pubblica e privata si basa sull'ipotesi che la **chiave privata è difficilmente ricostruibile** a partire da quella pubblica: cosa vuol dire?
- Vuol dire che, con le conoscenze teoriche a noi note e con la potenza di calcolo oggi disponibile **ci vorrebbe troppo tempo**, da qualche decina a centinaia di anni (o più), dipende dalla lunghezza della chiave pubblica
- **Rivest Shamir Adleman** nel 1977 inventarono l'**algoritmo RSA**, oggi universalmente usato. Si basa sul fatto che fattorizzare un numero di centinaia di cifre come prodotto di due numeri primi è un'**operazione molto onerosa** (anche oggi)

$\Rightarrow$ **abbiamo bisogno di un po' di matematica per capirne il perché...**

Agenda

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Numeri primi

Definizione (di numero primo)

Un **numero primo** è un numero naturale che ha *solo due divisori distinti*: 1 e se stesso

Conseguenze

- Il numero 1 non è primo, mentre sono primi 2, 3, 5, 7, ...
- A parte il 2, tutti gli altri numeri primi sono dispari
- Ci sono infiniti numeri primi
- **Teorema (fondamentale dell'aritmetica)**: *ogni numero naturale è fattorizzabile in uno ed un solo modo*

Definizione (fattorizzazione)

Fattorizzare un numero naturale significa riscriverlo come prodotto di numeri primi ($48510 = 2 \times 3 \times 3 \times 5 \times 7 \times 7 \times 11$).

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?

...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Fattorizzazione di un numero naturale

Come si procede per fattorizzare il numero 48510?
...l'abbiamo imparato alle medie...

48510	2
24255	3
8085	3
2695	5
539	7
77	7
11	11
1	

quindi: $48510 = 2 \times 3^2 \times 5 \times 7^2 \times 11$.

Per fattorizzare un numero naturale n bisogna sapere:

- I **criteri di divisibilità** per i numeri primi almeno fino al 17
- I **numeri primi** più piccoli di n

Criteri di divisibilità di un numero intero n

2: n termina con 0 o con un numero pari.

3: la somma delle cifre di n è 3 o un multiplo di 3.

5: n termina con 0 o 5.

7: se il doppio della cifra delle unità sottratta al numero senza la cifra delle unità dà 0 o un multiplo di 7. Esempio: 455 è divisibile per 7 perché $45 - 5 \times 2 = 35$ che è un multiplo di 7.

11: se il valore assoluto della differenza fra la somma delle cifre di posto pari e la somma delle cifre di posto dispari, è 0, 11 o un multiplo di 11. Esempio: 598279 è divisibile per 11 perché $|(5 + 8 + 7) - (9 + 2 + 9)| = |20 - 20| = 0$.

13: se la somma del quadruplo della cifra delle unità con il numero formato dalle rimanenti cifre è 0, 13 o un multiplo di 13. Esempio: 117 è divisibile per 13 perché $4 \times 7 + 11 = 39$ che è multiplo di 13.

17: se il valore assoluto della differenza tra il numero ottenuto eliminando la cifra delle unità e il quintuplo della cifra delle unità è 0, 17 o un multiplo di 17. Esmpio: 238 è divisibile per 17 perché $23 - 5 \times 8 = 17$.

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Cosa sappiamo sui numeri primi?

- **Non si conosce una formula** che permetta di generare i numeri primi *a priori*: qual è il 1000-esimo numero primo?
- La **distribuzione** dei numeri primi sembra a prima vista **casuale**; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità
- Sono frequenti i **numeri primi gemelli** cioè accoppiati a distanza di 2 (17 e 19, 29 e 31); non sappiamo se la serie dei primi gemelli sia finita o infinita.
- Non si conoscono metodi veloci per il **test di primalità**, ovvero per stabilire se un numero è primo.
- Non si conoscono metodi veloci per **scomporre un numero in fattori primi**.

Siccome **sappiamo così poco** sui numeri primi, li usiamo in crittografia!

Ricerca dei numeri primi

Domanda

Come si fa a determinare tutti i numeri primi minori o uguali a 100?

- Per ciascun numero da 2 a 100 controlliamo se **è divisibile per qualche numero** che lo precede: se sì, non è primo, altrimenti lo è.
- Prendiamo **solo i numeri *dispari*** tra 2 e 100 e facciamo quanto proposto sopra.
- Possiamo **fare di meglio**?

Ricerca dei numeri primi

Domanda

Come si fa a determinare tutti i numeri primi minori o uguali a 100?

- Per ciascun numero da 2 a 100 controlliamo se **è divisibile per qualche numero** che lo precede: se sì, non è primo, altrimenti lo è.
- Prendiamo **solo i numeri *dispari*** tra 2 e 100 e facciamo quanto proposto sopra.
- Possiamo **fare di meglio**?

Ricerca dei numeri primi

Domanda

Come si fa a determinare tutti i numeri primi minori o uguali a 100?

- Per ciascun numero da 2 a 100 controlliamo se **è divisibile per qualche numero** che lo precede: se sì, non è primo, altrimenti lo è.
- Prendiamo **solo i numeri *dispari*** tra 2 e 100 e facciamo quanto proposto sopra.
- Possiamo **fare di meglio**?

Ricerca dei numeri primi

Domanda

Come si fa a determinare tutti i numeri primi minori o uguali a 100?

- Per ciascun numero da 2 a 100 controlliamo se **è divisibile per qualche numero** che lo precede: se sì, non è primo, altrimenti lo è.
- Prendiamo **solo i numeri *dispari*** tra 2 e 100 e facciamo quanto proposto sopra.
- Possiamo **fare di meglio**?

Crivello (o setaccio) per determinare i primi fino a n

- Idea di **Eratostene di Cirene**: 276-194 a.C., matematico, astronomo, geografo, poeta, terzo bibliotecario della *Biblioteca di Alessandria*
- **Passiamo al setaccio** i numeri da 2 a 100 e **scartiamo quelli che non sono primi**: i rimanenti vanno bene

Crivello (o setaccio) per determinare i primi fino a *n*

- Idea di **Eratostene di Cirene**: 276-194 a.C., matematico, astronomo, geografo, poeta, terzo bibliotecario della *Biblioteca di Alessandria*
- **Passiamo al setaccio** i numeri da 2 a 100 e **scartiamo quelli che non sono primi**: i rimanenti vanno bene

Crivello (o setaccio) per determinare i primi fino a *n*

- Idea di **Eratostene di Cirene**: 276-194 a.C., matematico, astronomo, geografo, poeta, terzo bibliotecario della *Biblioteca di Alessandria*
- **Passiamo al setaccio** i numeri da 2 a 100 e **scartiamo quelli che non sono primi**: i rimanenti vanno bene

Crivello di Eratostene

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

togliamo i multipli di 2...

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

...ottenendo

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

Togliamo i multipli di 3...

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

...ottenendo

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83						89	
91				95		97			

togliamo i multipli di 5...

	2	3		5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
		53		55				59	
61				65		67			
71		73				77		79	
		83						89	
91				95		97			

...ottenendo

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

togliamo i multipli di 7...

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

...ottenendo

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

Crivello di Eratostene: quando fermarsi?

- Osserviamo che se $n = a \times b$ allora a che b **non** possono essere *simultaneamente* **entrambi maggiori di** $\sqrt{n}$.
- Quindi se cerchiamo i numeri primi fino ad n, **basta fermarsi** una volta superato il numero $\sqrt{n}$.
- Siccome il prossimo numero del quale eliminare i multipli sarebbe 11, e $11^2 = 121 > 100$, **possiamo fermarci!**

I numeri primi minori di 100 sono: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97. Il Crivello di Eratostene è ancor oggi il metodo **più efficiente** per trovare i numeri primi **fino a 1 000 000**. Oltre, si usano algoritmi decisamente più sofisticati.

Crivello di Eratostene: quando fermarsi?

- Osserviamo che se $n = a \times b$ allora a che b **non** possono essere *simultaneamente* **entrambi maggiori di** $\sqrt{n}$.
- Quindi se cerchiamo i numeri primi fino ad n, **basta fermarsi** una volta superato il numero $\sqrt{n}$.
- Siccome il prossimo numero del quale eliminare i multipli sarebbe 11, e $11^2 = 121 > 100$, **possiamo fermarci!**

I numeri primi minori di 100 sono: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97. Il Crivello di Eratostene è ancor oggi il metodo **più efficiente** per trovare i numeri primi **fino a 1 000 000**. Oltre, si usano algoritmi decisamente più sofisticati.

Crivello di Eratostene: quando fermarsi?

- Osserviamo che se $n = a \times b$ allora a che b **non** possono essere *simultaneamente* **entrambi maggiori di** $\sqrt{n}$.
- Quindi se cerchiamo i numeri primi fino ad n, **basta fermarsi** una volta superato il numero $\sqrt{n}$.
- Siccome il prossimo numero del quale eliminare i multipli sarebbe 11, e $11^2 = 121 > 100$, **possiamo fermarci!**

I numeri primi minori di 100 sono: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97. Il Crivello di Eratostene è ancor oggi il metodo **più efficiente** per trovare i numeri primi **fino a 1 000 000**. Oltre, si usano algoritmi decisamente più sofisticati.

Crivello di Eratostene: quando fermarsi?

- Osserviamo che se $n = a \times b$ allora a che b **non** possono essere *simultaneamente* **entrambi maggiori di** $\sqrt{n}$.
- Quindi se cerchiamo i numeri primi fino ad n, **basta fermarsi** una volta superato il numero $\sqrt{n}$.
- Siccome il prossimo numero del quale eliminare i multipli sarebbe 11, e $11^2 = 121 > 100$, **possiamo fermarci!**

I numeri primi minori di 100 sono: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97. Il Crivello di Eratostene è ancor oggi il metodo **più efficiente** per trovare i numeri primi **fino a 1 000 000**. Oltre, si usano algoritmi decisamente più sofisticati.

Crivello di Eratostene: quando fermarsi?

- Osserviamo che se $n = a \times b$ allora a che b **non** possono essere *simultaneamente* **entrambi maggiori di** $\sqrt{n}$.
- Quindi se cerchiamo i numeri primi fino ad n, **basta fermarsi** una volta superato il numero $\sqrt{n}$.
- Siccome il prossimo numero del quale eliminare i multipli sarebbe 11, e $11^2 = 121 > 100$, **possiamo fermarci!**

I numeri primi minori di 100 sono: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97. Il Crivello di Eratostene è ancor oggi il metodo **più efficiente** per trovare i numeri primi **fino a 1 000 000**. Oltre, si usano algoritmi decisamente più sofisticati.

Crivello di Eratostene: quando fermarsi?

- Osserviamo che se $n = a \times b$ allora a che b **non** possono essere *simultaneamente* **entrambi maggiori di** $\sqrt{n}$.
- Quindi se cerchiamo i numeri primi fino ad n, **basta fermarsi** una volta superato il numero $\sqrt{n}$.
- Siccome il prossimo numero del quale eliminare i multipli sarebbe 11, e $11^2 = 121 > 100$, **possiamo fermarci!**

I numeri primi minori di 100 sono: 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97. Il Crivello di Eratostene è ancor oggi il metodo **più efficiente** per trovare i numeri primi **fino a 1 000 000**. Oltre, si usano algoritmi decisamente più sofisticati.

Perché usiamo i numeri primi in crittografia?

- Il **test di primalità** per un numero n è **piuttosto veloce**
- La **fattorizzazione** di un numero n, soprattutto se n ha parecchie cifre, è **molto lenta**
- Il numero primo **più grande** a noi noto è $2^{243\,112\,609} - 1$, di $12\,978\,189$ cifre, calcolato il **23 Agosto del 2008** (da allora niente di nuovo!)

Perché usiamo i numeri primi in crittografia?

- Il **test di primalità** per un numero n è **piuttosto veloce**
- La **fattorizzazione** di un numero n, soprattutto se n ha parecchie cifre, è **molto lenta**
- Il numero primo **più grande** a noi noto è $2^{243\,112\,609} - 1$, di $12\,978\,189$ cifre, calcolato il **23 Agosto del 2008** (da allora niente di nuovo!)

Perché usiamo i numeri primi in crittografia?

- Il **test di primalità** per un numero n è **piuttosto veloce**
- La **fattorizzazione** di un numero n, soprattutto se n ha parecchie cifre, è **molto lenta**
- Il numero primo **più grande** a noi noto è $2^{243\,112\,609} - 1$, di 12 978 189 cifre, calcolato il **23 Agosto del 2008** (da allora niente di nuovo!)

Perché usiamo i numeri primi in crittografia?

- Il **test di primalità** per un numero n è **piuttosto veloce**
- La **fattorizzazione** di un numero n, soprattutto se n ha parecchie cifre, è **molto lenta**
- Il numero primo **più grande** a noi noto è $2^{243\,112\,609} - 1$, di $12\,978\,189$ cifre, calcolato il **23 Agosto del 2008** (da allora niente di nuovo!)

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p - 1) \times (q - 1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5 - 1) \times (11 - 1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p-1) \times (q-1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5-1) \times (11-1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p - 1) \times (q - 1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5 - 1) \times (11 - 1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p - 1) \times (q - 1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5 - 1) \times (11 - 1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p - 1) \times (q - 1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5 - 1) \times (11 - 1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p - 1) \times (q - 1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5 - 1) \times (11 - 1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Generazione delle chiavi per la crittografia RSA

- Scegliamo **due numeri primi molto grandi** (p, q) e li moltiplichiamo tra loro, $n = p \times q$.
  $p = 5, q = 11, n = 5 \times 11 = 55$.
- Calcoliamo $\varphi(n) = (p - 1) \times (q - 1)$ e **scegliamo** e che non abbia divisori comuni con $\varphi(n)$ e tale che $1 < e < \varphi(n)$. $\varphi(n) = (5 - 1) \times (11 - 1) = 40$, $e = 3$ perché 3 e 40 non hanno divisori comuni.
- La coppia $(n, e) = (55, 3)$ è la **chiave pubblica**.
- **Scegliamo** d in modo tale che la divisione $(d \times e) : \varphi(n)$ dia resto 1. $d = 27$, infatti $d \times e = 27 \times 3 = 81$, e $80 = \varphi(n) \times 2 = 40 \times 2$.
- La coppia $(n, d) = (55, 27)$ è la **chiave privata**.
- I numeri primi $(p, q) = (5, 11)$ **vengono eliminati**.

Utilizzo delle chiavi RSA

- Il mittente vuole mandare il messaggio m e utilizza la chiave pubblica del destinatario (n, e) calcolando il **messaggio cifrato c come resto della divisione** $(m^e) : n$. Se $m = 7, 7^3 = 343$ e il resto della divisione $343 : 55$ è $c = 13$.
- Il destinatario riceve il messaggio cifrato c e lo converte nel testo in chiaro calcolando il **messaggio originario m come resto della divisione** $(c^d) : n$. La potenza $c^d = 13^{27}$ non si calcola (troppo grande!) ma si calcola il resto della divisione per 55 per passi successivi. Viene proprio $m = 7$, provare per credere!

Utilizzo delle chiavi RSA

- Il mittente vuole mandare il messaggio m e utilizza la chiave pubblica del destinatario (n, e) calcolando il **messaggio cifrato c come resto della divisione** $(m^e) : n$. Se $m = 7, 7^3 = 343$ e il resto della divisione $343 : 55$ è $c = 13$.
- Il destinatario riceve il messaggio cifrato c e lo converte nel testo in chiaro calcolando il **messaggio originario m come resto della divisione** $(c^d) : n$. La potenza $c^d = 13^{27}$ non si calcola (troppo grande!) ma si calcola il resto della divisione per 55 per passi successivi. Viene proprio $m = 7$, provare per credere!

Utilizzo delle chiavi RSA

- Il mittente vuole mandare il messaggio m e utilizza la chiave pubblica del destinatario (n, e) calcolando il **messaggio cifrato c come resto della divisione** $(m^e) : n$. Se $m = 7, 7^3 = 343$ e il resto della divisione $343 : 55$ è $c = 13$.
- Il destinatario riceve il messaggio cifrato c e lo converte nel testo in chiaro calcolando il **messaggio originario m come resto della divisione** $(c^d) : n$. La potenza $c^d = 13^{27}$ non si calcola (troppo grande!) ma si calcola il resto della divisione per 55 per passi successivi. Viene proprio $m = 7$, provare per credere!

Sicurezza delle chiavi RSA

- Conoscendo solo la coppia (n, e) ed avendo utilizzato (p, q) con almeno 512 bit, che corrispondono a 170 cifre decimali, è **poco probabile che si riesca a calcolare d in tempi ragionevoli**. Pertanto la chiave privata è tanto più sicura quanto più (p, q) sono grandi!
- Si pensa che chiavi a 1024 bit per la crittografia RSA dovrebbero ormai essere crackabili, **chiavi a 2048 bit dovrebbero resistere fino al 2030**. Per custodire segreti fino a dopo il 2030, l'RSA consiglia chiavi di lunghezza superiore a 3072 bit.

Sicurezza delle chiavi RSA

- Conoscendo solo la coppia (n, e) ed avendo utilizzato (p, q) con almeno 512 bit, che corrispondono a 170 cifre decimali, è **poco probabile che si riesca a calcolare d in tempi ragionevoli**. Pertanto la chiave privata è tanto più sicura quanto più (p, q) sono grandi!
- Si pensa che chiavi a 1024 bit per la crittografia RSA dovrebbero ormai essere crackabili, **chiavi a 2048 bit dovrebbero resistere fino al 2030**. Per custodire segreti fino a dopo il 2030, l'RSA consiglia chiavi di lunghezza superiore a 3072 bit.

Sicurezza delle chiavi RSA

- Conoscendo solo la coppia (n, e) ed avendo utilizzato (p, q) con almeno 512 bit, che corrispondono a 170 cifre decimali, è **poco probabile che si riesca a calcolare d in tempi ragionevoli**. Pertanto la chiave privata è tanto più sicura quanto più (p, q) sono grandi!
- Si pensa che chiavi a 1024 bit per la crittografia RSA dovrebbero ormai essere crackabili, **chiavi a 2048 bit dovrebbero resistere fino al 2030**. Per custodire segreti fino a dopo il 2030, l'RSA consiglia chiavi di lunghezza superiore a 3072 bit.

Agenda

Conclusioni

- Nascondere messaggi è un **bisogno**; steganografia e crittografia sono state usate **fin dall'antichità**.
- La crittografia è un **terreno molto fertile per i matematici**.
- I **numeri primi** sono **ancora** piuttosto **sconosciuti** ai matematici e la ricerca in questo campo è apertissima.
- L'attuale crittografia RSA (la più usata) si basa sul fatto che **ci vuole tanto tempo** per **risolvere un problema "difficile"** come la fattorizzazione di un numero come prodotto di due soli numeri primi piuttosto grandi.
- Campi di **applicazione della crittografia**, in particolare quella RSA, sono il commercio elettronico, i sistemi di pagamento informatizzato, le transazioni via Internet, la protezione reti wireless, la posta elettronica certificata, ecc.

Conclusioni

- Nascondere messaggi è un **bisogno**; steganografia e crittografia sono state usate **fin dall'antichità**.
- La crittografia è un **terreno molto fertile per i matematici**.
- I **numeri primi** sono **ancora** piuttosto **sconosciuti** ai matematici e la ricerca in questo campo è apertissima.
- L'attuale crittografia RSA (la più usata) si basa sul fatto che **ci vuole tanto tempo** per **risolvere un problema "difficile"** come la fattorizzazione di un numero come prodotto di due soli numeri primi piuttosto grandi.
- Campi di **applicazione della crittografia**, in particolare quella RSA, sono il commercio elettronico, i sistemi di pagamento informatizzato, le transazioni via Internet, la protezione reti wireless, la posta elettronica certificata, ecc.

Conclusioni

- Nascondere messaggi è un **bisogno**; steganografia e crittografia sono state usate **fin dall'antichità**.
- La crittografia è un **terreno molto fertile per i matematici**.
- I **numeri primi** sono **ancora** piuttosto **sconosciuti** ai matematici e la ricerca in questo campo è apertissima.
- L'attuale crittografia RSA (la più usata) si basa sul fatto che **ci vuole tanto tempo** per **risolvere un problema "difficile"** come la fattorizzazione di un numero come prodotto di due soli numeri primi piuttosto grandi.
- Campi di **applicazione della crittografia**, in particolare quella RSA, sono il commercio elettronico, i sistemi di pagamento informatizzato, le transazioni via Internet, la protezione reti wireless, la posta elettronica certificata, ecc.

Conclusioni

- Nascondere messaggi è un **bisogno**; steganografia e crittografia sono state usate **fin dall'antichità**.
- La crittografia è un **terreno molto fertile per i matematici**.
- I **numeri primi** sono **ancora** piuttosto **sconosciuti** ai matematici e la ricerca in questo campo è apertissima.
- L'attuale crittografia RSA (la più usata) si basa sul fatto che **ci vuole tanto tempo** per **risolvere un problema "difficile"** come la fattorizzazione di un numero come prodotto di due soli numeri primi piuttosto grandi.
- Campi di **applicazione della crittografia**, in particolare quella RSA, sono il commercio elettronico, i sistemi di pagamento informatizzato, le transazioni via Internet, la protezione reti wireless, la posta elettronica certificata, ecc.

Conclusioni

- Nascondere messaggi è un **bisogno**; steganografia e crittografia sono state usate **fin dall'antichità**.
- La crittografia è un **terreno molto fertile per i matematici**.
- I **numeri primi** sono **ancora** piuttosto **sconosciuti** ai matematici e la ricerca in questo campo è apertissima.
- L'attuale crittografia RSA (la più usata) si basa sul fatto che **ci vuole tanto tempo** per **risolvere un problema "difficile"** come la fattorizzazione di un numero come prodotto di due soli numeri primi piuttosto grandi.
- Campi di **applicazione della crittografia**, in particolare quella RSA, sono il commercio elettronico, i sistemi di pagamento informatizzato, le transazioni via Internet, la protezione reti wireless, la posta elettronica certificata, ecc.

Conclusioni

- Nascondere messaggi è un **bisogno**; steganografia e crittografia sono state usate **fin dall'antichità**.
- La crittografia è un **terreno molto fertile per i matematici**.
- I **numeri primi** sono **ancora** piuttosto **sconosciuti** ai matematici e la ricerca in questo campo è apertissima.
- L'attuale crittografia RSA (la più usata) si basa sul fatto che **ci vuole tanto tempo** per **risolvere un problema "difficile"** come la fattorizzazione di un numero come prodotto di due soli numeri primi piuttosto grandi.
- Campi di **applicazione della crittografia**, in particolare quella RSA, sono il commercio elettronico, i sistemi di pagamento informatizzato, le transazioni via Internet, la protezione reti wireless, la posta elettronica certificata, ecc.

Domande?