Crittografia
Progetto Piano Lauree Scientifiche per la Matematica

Marco Caliari e Simone Zuccher

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

Agenda

1. Introduzione
   - Steganografia e crittografia
2. Crittografia
   - Descrizione di alcuni metodi

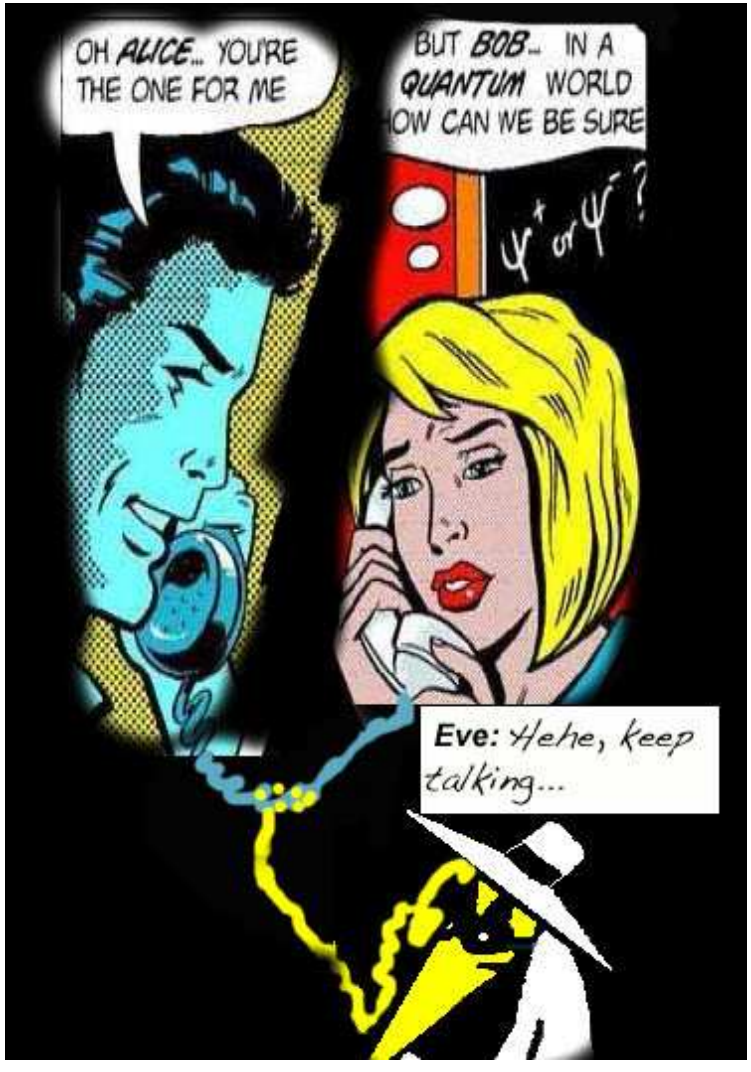
Agenda

1. Introduzione
   - Steganografia e crittografia
2. Crittografia
   - Descrizione di alcuni metodi

Agenda

1. Introduzione
   - Steganografia e crittografia
2. Crittografia
   - Descrizione di alcuni metodi

Motivazione



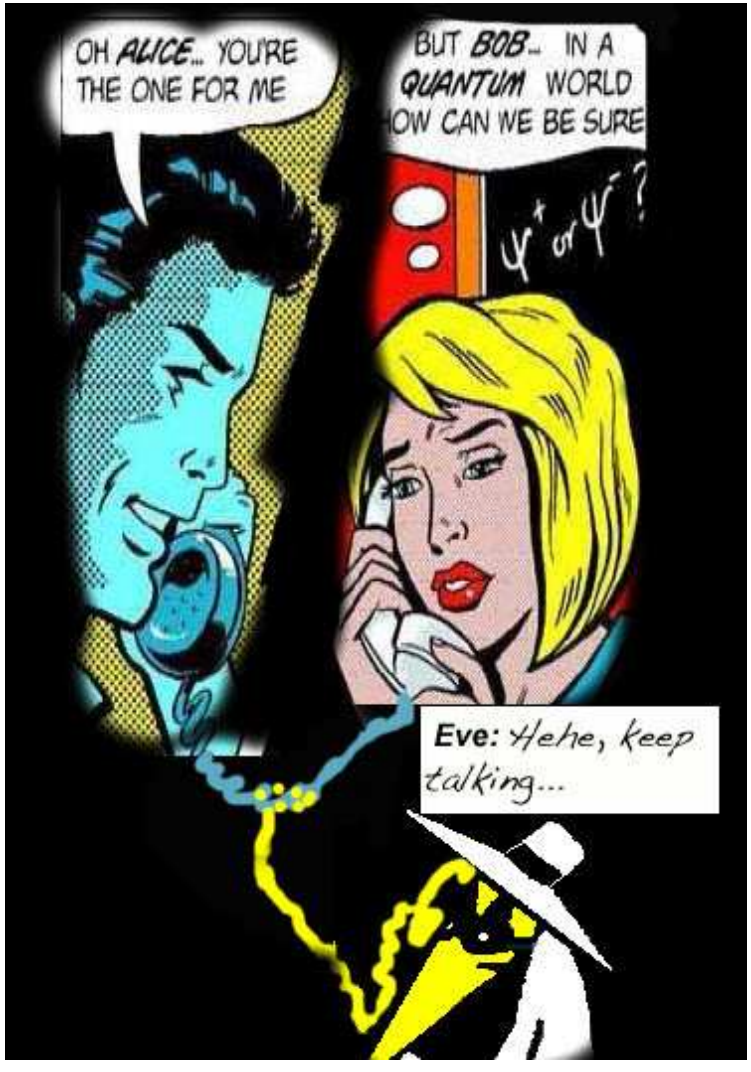
A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

Motivazione



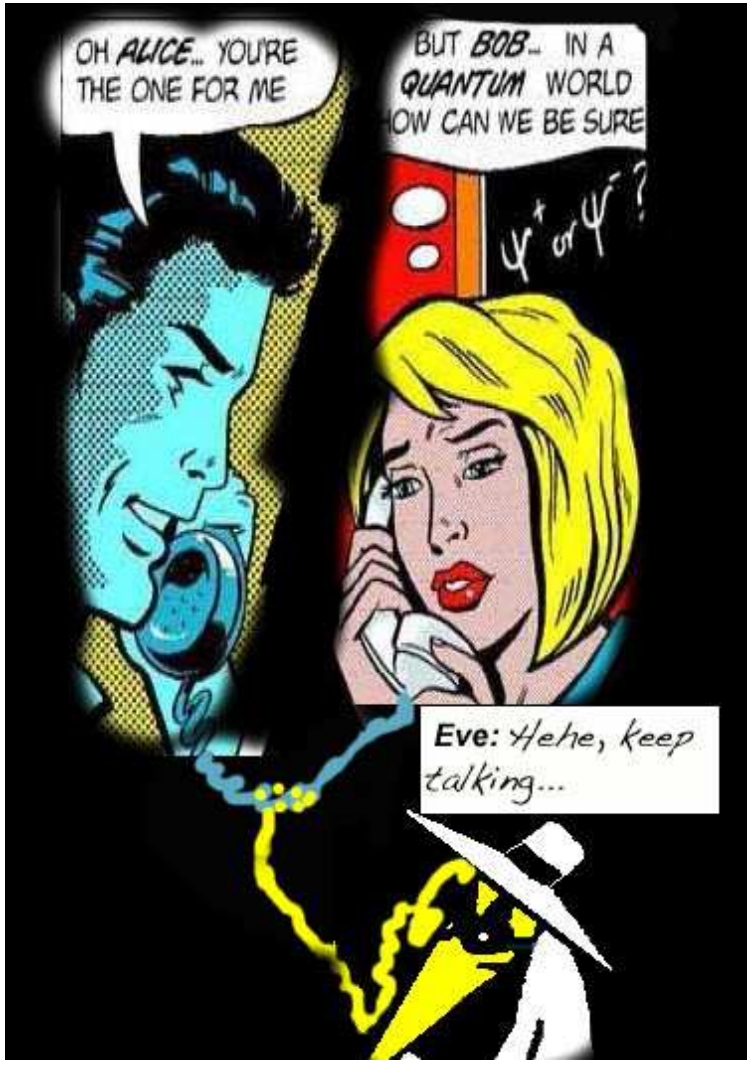
A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

Motivazione



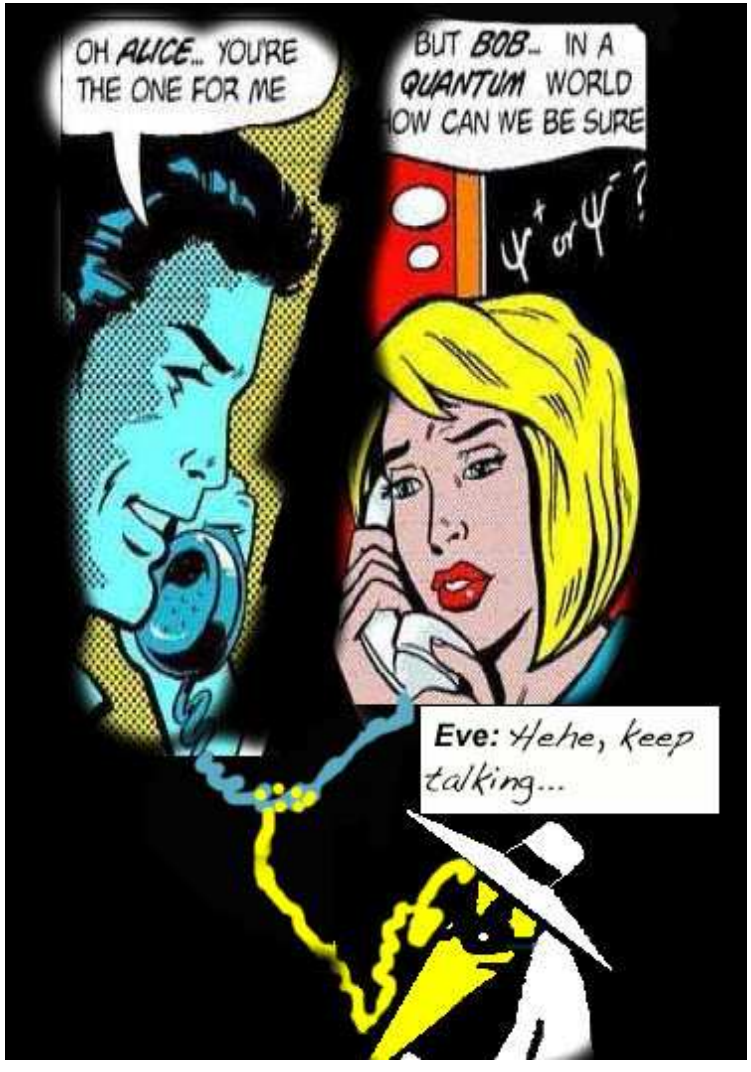
A (Alice) e **B** (Bob) devono scambiarsi delle **informazioni** (messaggi d'amore, appuntamenti segreti, data e ora per sferrare un attacco, ecc.) ma vogliono farlo senza essere **intercettati** da **E** (Eve, alternativamente **M**, Mallory).

Domanda: come fare?

Risposta: basta occultare il messaggio!

1. Steganografia
2. Crittografia

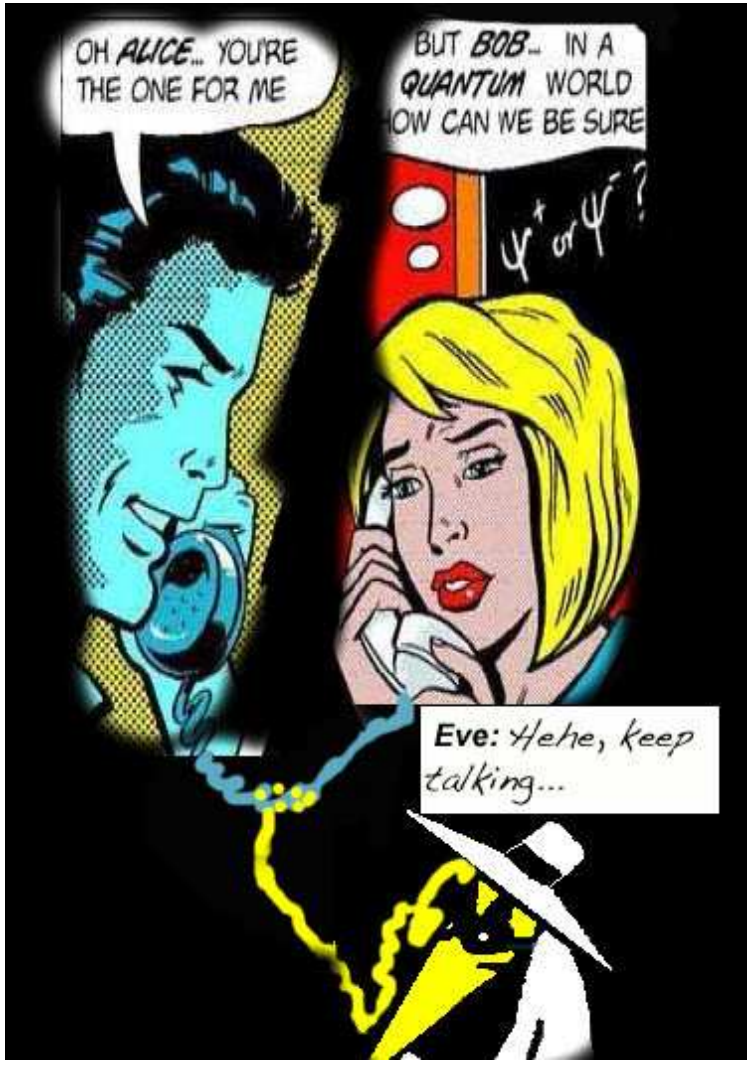
Motivazione



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...

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 (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.

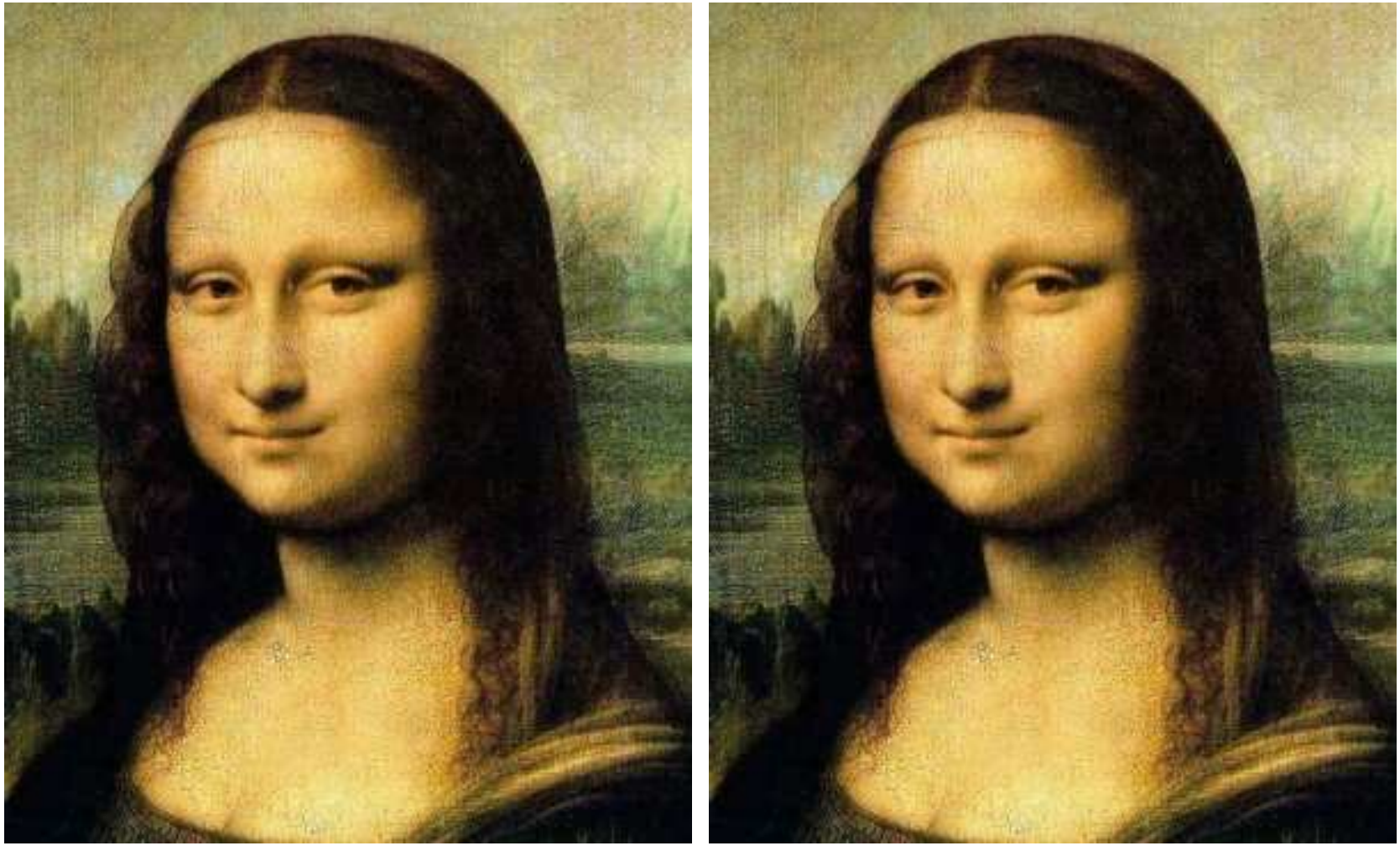
Steganografia (2/3)

- **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

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!**

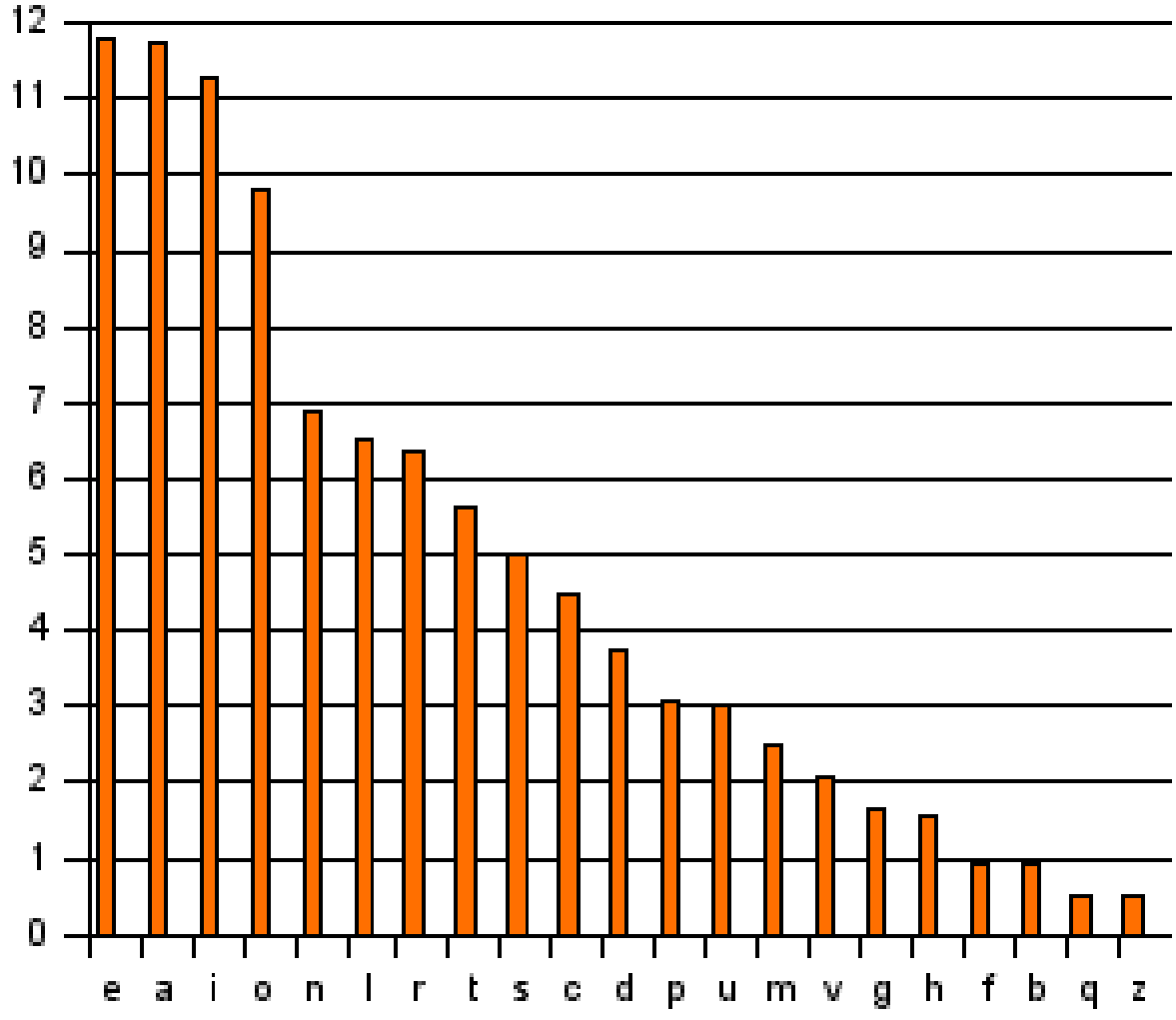
...analizziamo la frequenza di ogni lettera

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).