Crittografia

MIL

LiceoPeanoMonterotondo

2 Febbraio 2017

Il frammento che abbiamo visto è tratto dal film:

Il frammento che abbiamo visto è tratto dal film:

Il protagonista è:

Il protagonista è:

Alan Turing: Matematico, Logico e Crittografo,

Il protagonista è:

Alan Turing: Matematico, Logico e Crittografo,

- nasce a Londra nel 1912;

Il protagonista è:

Alan Turing: Matematico, Logico e Crittografo,

- nasce a Londra nel 1912;
- nel 1940, a 28 anni, è a capo del gruppo di ricercatori impegnati a decifrare i messaggi in codice della marina tedesca prodotti dalla macchina **ENIGMA**;

Il protagonista è:

Alan Turing: Matematico, Logico e Crittografo,

- nasce a Londra nel 1912;
- nel 1940, a 28 anni, è a capo del gruppo di ricercatori impegnati a decifrare i messaggi in codice della marina tedesca prodotti dalla macchina **ENIGMA**;
- nel 1942 sulla base delle idee create da Turing per decifrare i messaggi di ENIGMA viene realizzata la macchina **Colossus** antesignana dei moderni computer;

- nel 1952 viene arrestato per omosessualità e, per evitare la prigione, sceglie la castrazione chimica mediante assunzione di estrogeni;

- nel 1952 viene arrestato per omosessualità e, per evitare la prigione, sceglie la castrazione chimica mediante assunzione di estrogeni;
- nel 1954 in seguito a depressione e umiliazione si toglie la vita mangiando una mela avvelenata al cianuro di potassio.

- nel 1952 viene arrestato per omosessualità e, per evitare la prigione, sceglie la castrazione chimica mediante assunzione di estrogeni;
- nel 1954 in seguito a depressione e umiliazione si toglie la vita mangiando una mela avvelenata al cianuro di potassio.

una "leggenda metropolitana" vuole che il logo della Apple sia un omaggio a Turing....

- nel 1952 viene arrestato per omosessualità e, per evitare la prigione, sceglie la castrazione chimica mediante assunzione di estrogeni;
- nel 1954 in seguito a depressione e umiliazione si toglie la vita mangiando una mela avvelenata al cianuro di potassio.

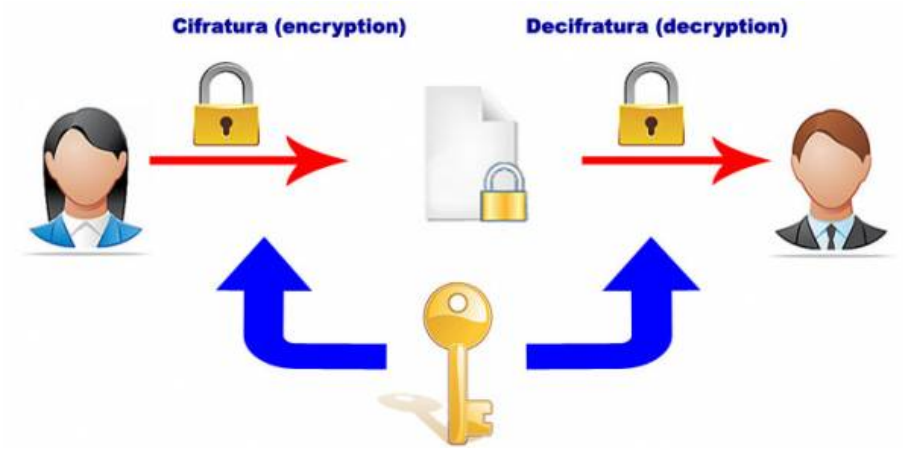
una "leggenda metropolitana" vuole che il logo della Apple sia un omaggio a Turing.... il designer Rob Janoff, che ha ideato il logo su richiesta di Steve Jobs nel 1977, ha smentito tale leggenda....

- nel 1952 viene arrestato per omosessualità e, per evitare la prigione, sceglie la castrazione chimica mediante assunzione di estrogeni;
- nel 1954 in seguito a depressione e umiliazione si toglie la vita mangiando una mela avvelenata al cianuro di potassio.

una "leggenda metropolitana" vuole che il logo della Apple sia un omaggio a Turing.... il designer Rob Janoff, che ha ideato il logo su richiesta di Steve Jobs nel 1977, ha smentito tale leggenda.... quel che è certo è che ogni volta che utilizziamo una strumento informatico lo dobbiamo in parte a Turing

Introduzione

La `crittografia` , letteralmente "scrittura segreta" (dal greco $\kappa\varrho\upsilon\pi\tau\acute{o}\varsigma$ = nascosto e $\gamma\varrho\alpha\varphi\acute{\iota}\alpha$=scrittura) è l'insieme delle tecniche che consentono di trasmettere messaggi mantenendoli segreti a tutti, tranne ad alcune persone che posseggano la chiave per comprenderli



Alcuni termini importanti:

Alcuni termini importanti:

- **testo in chiaro** è il messaggio da cifrare;

Alcuni termini importanti:

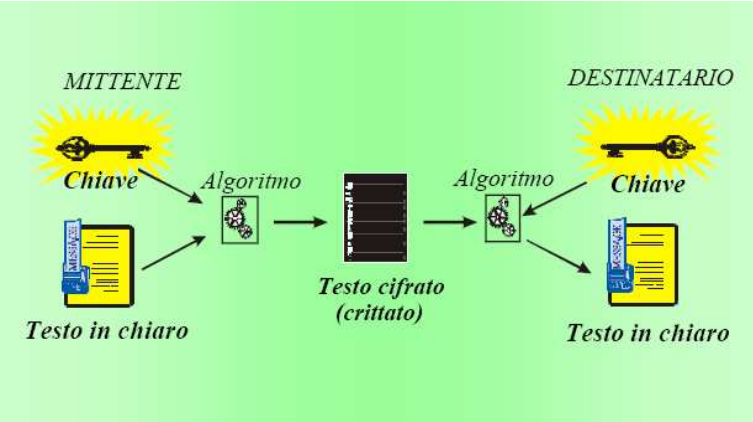
- **testo in chiaro** è il messaggio da cifrare;
- **cifrario o algoritmo di cifratura** è la procedura con la quale si nascondono le informazioni;

Alcuni termini importanti:

- **testo in chiaro** è il messaggio da cifrare;
- **cifrario o algoritmo di cifratura** è la procedura con la quale si nascondono le informazioni;
- **decrittazione** è la riconversione di un testo cifrato nella sua forma originale (testo in chiaro);

Alcuni termini importanti:

- **testo in chiaro** è il messaggio da cifrare;
- **cifrario o algoritmo di cifratura** è la procedura con la quale si nascondono le informazioni;
- **decrittazione** è la riconversione di un testo cifrato nella sua forma originale (testo in chiaro);
- **crittoanalisi** è lo studio dei sistemi in grado di svelare il contenuto di un messaggio segreto;



Come nasce l'esigenza di trasmettere informazioni in segreto?

Come nasce l'esigenza di trasmettere informazioni in segreto?
vediamo alcuni esempi storici...

Come nasce l'esigenza di trasmettere informazioni in segreto?
vediamo alcuni esempi storici...

SCITALA LACEDEMONICA 400 a.C.

È una delle più antiche forme di crittografia, consiste in un bastone in cui si avvolgeva ad elica un nastro di cuoio. La chiave consiste nel diametro del bastone.

CIFRARIO DI CESARE I sec. a.C.

Svetonio riporta che Giulio Cesare cifrava la sua corrispondenza privata grazie ad un algoritmo di sostituzione delle lettere

DISCO DI LEON BATTISTA ALBERTI 1400

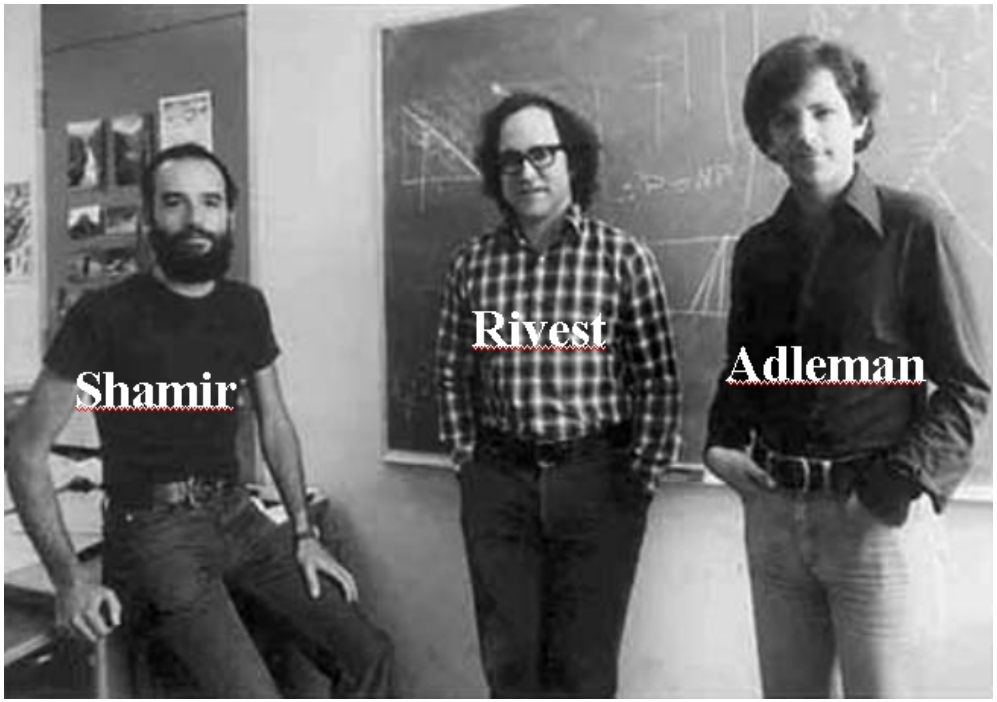
Nel suo trattato *De Cifris*, Alberti introduce il primo **codice polialfabetico** in cui si crea una corrispondenza tra lettere grazie alla rotazione di due dischi

MACCHINA ENIGMA 1923

Macchina cifratrice utilizzata dal Terzo Reich durante la Seconda Guerra Mondiale

algoritmo RSA 1977

Metodo inventato negli anni settanta da Rivest, Shamir e Adleman e usato oggi da milioni di persone per la sicurezza delle transazioni in INTERNET, si basa su una doppia chiave: pubblica e privata.



Il cifrario di Cesare

Per cifrare un messaggio si sostituisce ad ogni lettera dell'alfabeto quella che si trova tre passi più avanti nell'alfabeto stesso.
Si ottiene la seguente corrispondenza:

Il cifrario di Cesare

Per cifrare un messaggio si sostituisce ad ogni lettera dell'alfabeto quella che si trova tre passi più avanti nell'alfabeto stesso.
Si ottiene la seguente corrispondenza:

The Caesar cipher 	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	v	z	a	b	c

Possiamo ottenere questa trasformazione mediante una rotazione del disco che avete a disposizione. Chiamiamola ROT3. In generale ROTn sarà la rotazione del disco di n passi.

Ora proviamo a cifrare il seguente messaggio usando ROT1:

A SETTENTRIONE SCOPPIA UNA GUERRA

Ora proviamo a cifrare il seguente messaggio usando ROT1:

A SETTENTRIONE SCOPPIA UNA GUERRA

otteniamo

Ora proviamo a cifrare il seguente messaggio usando ROT1:

A SETTENTRIONE SCOPPIA UNA GUERRA

otteniamo

B TFUUFOUSJPOF TDPQQJB VOB HVFSSB

Ora provate a **decifrare** il seguente messaggio usando ROT1:

MB QSPG EJ NBUFNBUJDB OPO WJFOF, FWWJWB OPO TJ GB MFAJPOF

Ora provate a **decifrare** il seguente messaggio usando ROT1:

MB QSPG EJ NBUFNBUJDB OPO WJFOF, FWWJWB OPO TJ GB MFAJPOF

cosa ottieniamo?

Ora proviamo a cifrare il seguente messaggio usando ROT3:

AMBASCIATORE IN PRIGIONE

Ora proviamo a cifrare il seguente messaggio usando ROT3:

AMBASCIATORE IN PRIGIONE

otteniamo

Ora proviamo a cifrare il seguente messaggio usando ROT3:

AMBASCIATORE IN PRIGIONE

otteniamo

DPEDVFLDWRUH LQ SULJLRQH

Ora provate a **decifrare** il seguente messaggio usando ROT3:

FRPSOLPHQWL FL VLHWH ULXVFLWL

Ora provate a **decifrare** il seguente messaggio usando ROT3:

FRPSOLPHQWL FL VLHWH ULXVFLWL

cosa ottieniamo?

Ora in gruppi:

Ora in gruppi:

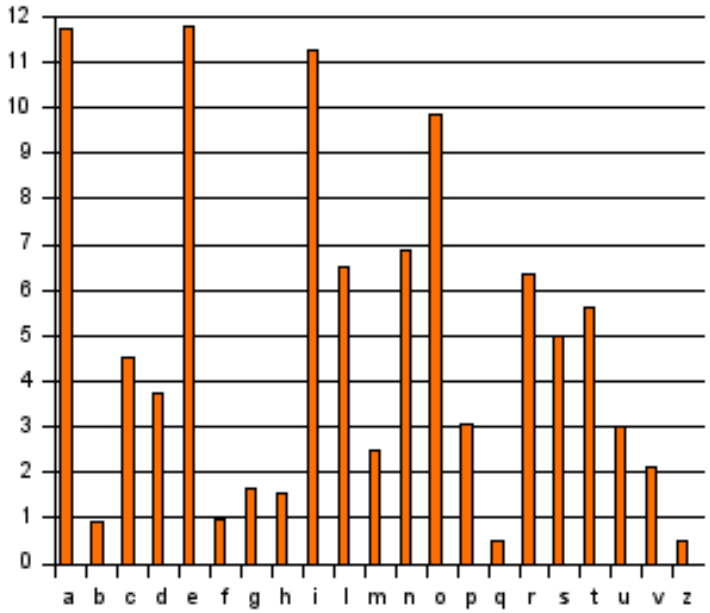
- un gruppo scrive un messaggio (di senso compiuto) di quattro parole e lo cifra usando ROTn (il numero n deve rimanere segreto!)

Ora in gruppi:

- un gruppo scrive un messaggio (di senso compiuto) di quattro parole e lo cifra usando ROTn (il numero n deve rimanere segreto!)
- il secondo gruppo intercetta il messaggio e lo deve decifrare

Come si può decifrare un messaggio scritto con un cifrario di tipo ROTn senza sapere n?

Come si può decifrare un messaggio scritto con un cifrario di tipo ROTn senza sapere n? Uno strumento usato per la crittanalisi è l'**ANALISI DELLE FREQUENZE**



è lo studio della frequenza con cui compaiono delle lettere in un testo. Nel grafico precedente abbiamo la frequenza percentuale con cui le varie lettere compaiono mediamente nei testi scritti in Italiano.

Esistono metodi di cifratura che non possono essere decodificati con l'analisi delle frequenze, ad esempio vediamo....

Esistono metodi di cifratura che non possono essere decodificati con l'analisi delle frequenze, ad esempio vediamo....

IL CIFRARIO DI VIGENÈRE

ideato dal diplomatico francese Blaise de Vigenère (1523-1596) si basa sulla seguente tabella.

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	Q
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	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	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	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	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	D
X	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	C
Y	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	B
Z	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

Come funziona?

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;
  2. per cifrare la lettera *o* usiamo la riga *m* e otteniamo *a* ;

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;
  2. per cifrare la lettera *o* usiamo la riga *m* e otteniamo *a* ;
  3. per cifrare la lettera *m* usiamo la riga *o* e otteniamo *a* ;

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;
  2. per cifrare la lettera *o* usiamo la riga *m* e otteniamo *a* ;
  3. per cifrare la lettera *m* usiamo la riga *o* e otteniamo *a* ;
  4. per cifrare la lettera *a* usiamo la riga *r* e otteniamo *r* ;

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;
  2. per cifrare la lettera *o* usiamo la riga *m* e otteniamo *a* ;
  3. per cifrare la lettera *m* usiamo la riga *o* e otteniamo *a* ;
  4. per cifrare la lettera *a* usiamo la riga *r* e otteniamo *r* ;
  5. ....

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;
  2. per cifrare la lettera *o* usiamo la riga *m* e otteniamo *a* ;
  3. per cifrare la lettera *m* usiamo la riga *o* e otteniamo *a* ;
  4. per cifrare la lettera *a* usiamo la riga *r* e otteniamo *r* ;
  5. ....

- avremo quindi

Come funziona?

- bisogna innanzitutto scegliere una parola chiave (Ad esempio scegliamo AMORE)
- bisogna scrivere il testo da cifrare (per esempio DOMANIPIOVE) sopra la parola chiave ripetuta, nel modo seguente:

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A

- ora, per cifrare ogni lettera, useremo la riga della matrice indicata dalla lettera sottostante.
  Per esempio:
  1. per cifrare la lettera *d* usiamo la riga *a* quindi *d* resta *d* ;
  2. per cifrare la lettera *o* usiamo la riga *m* e otteniamo *a* ;
  3. per cifrare la lettera *m* usiamo la riga *o* e otteniamo *a* ;
  4. per cifrare la lettera *a* usiamo la riga *r* e otteniamo *r* ;
  5. ....
- avremo quindi

D	O	M	A	N	I	P	I	O	V	E
A	M	O	R	E	A	M	O	R	E	A
D	A	A	R	R	I	B	W	F	Z	E

Ora proviamo a cifrare il seguente messaggio usando la tabella di Vigenère e la parola chiave UOVO:

LE RONDINI VOLANO

Ora proviamo a cifrare il seguente messaggio usando la tabella di Vigenère e la parola chiave UOVO:

LE RONDINI VOLANO

otteniamo

Ora proviamo a cifrare il seguente messaggio usando la tabella di Vigenère e la parola chiave UOVO:

LE RONDINI VOLANO

otteniamo

FSMCHRDBCJJZUBJ

Ora provate a **decifrare** il seguente messaggio usando la tabella di Vigenère e la parola chiave PALO:

XPCWVIZBXECWHOYCUURUXTT

Ora provate a **decifrare** il seguente messaggio usando la tabella di Vigenère e la parola chiave PALO:

XPCWVIZBXECWHOYCUURUXTT

cosa ottieniamo?