MATEMATICA E CRITTOGRAFIA

"Se vuoi costruire una nave, non radunare uomini per raccogliere il legno, distribuire i compiti e suddividere il lavoro, ma insegna alla gente la nostalgia del mare infinito"

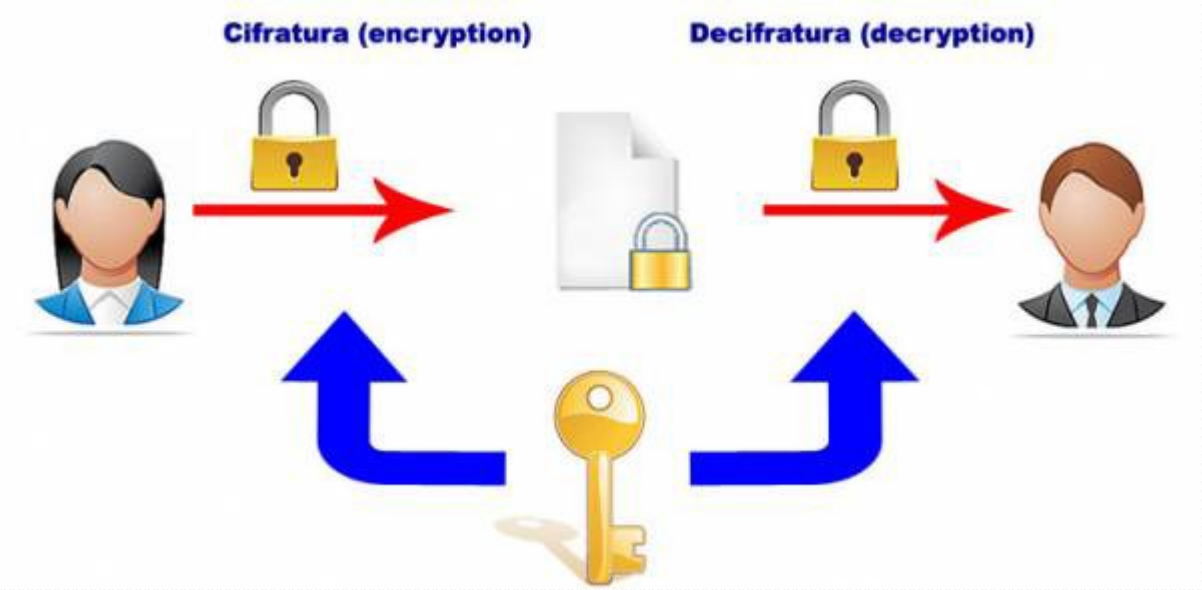
(Antoine De Saint-Exupéry)

Prof. Fabio Bellini

Prof.ssa Maria Antonella Pugliese

I.I.S CROCE-ALERAMO a.s 2019/2020

La *crittografia*, letteralmente "scrittura segreta"(dal greco) 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:

- 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);

Crittografia simmetrica e asimmetrica

SIMMETTRICA

- viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Le informazioni (la chiave e l'algoritmo) necessarie per chi deve inviare il messaggio sono quindi le stesse di quelle necessarie a chi deve leggerlo.

SVANTAGGIO: Problema della sicurezza nella distribuzione della chiave

VANTAGGIO: Efficienza

ASIMMETRICA

- esistono due chiavi: una pubblica da distribuire a tutti quelli con cui si vuole comunicare, e una privata da tenere segreta.

SVANTAGGIO: Complessità algoritmica

VANTAGGIO: Sicurezza/fruibilità

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

- **SCITALA LACEDEMONICA 400 a.C.**

  E' 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

CIFRARIO DI CESARE I sec. a.C.

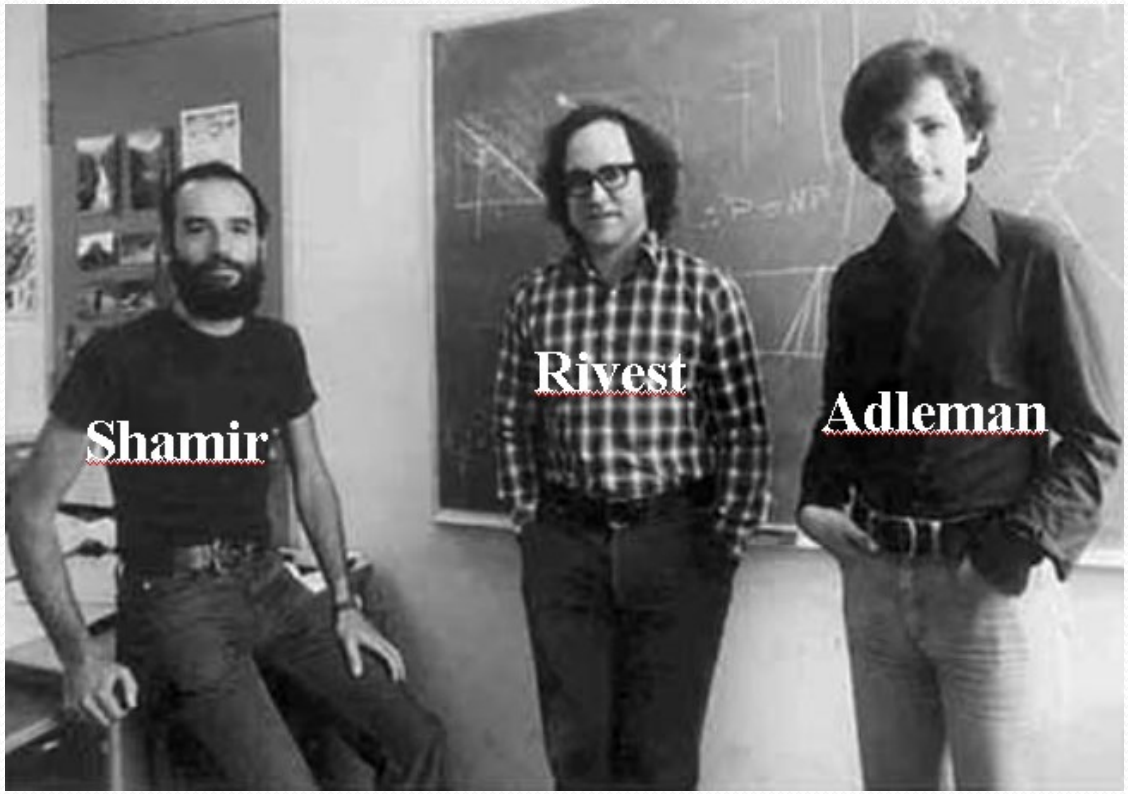
Svetonio riporta che Giulio Cesare cifrava la sua corrispondenza privata grazie ad un algoritmo di sostituzione delle lettere

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

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.



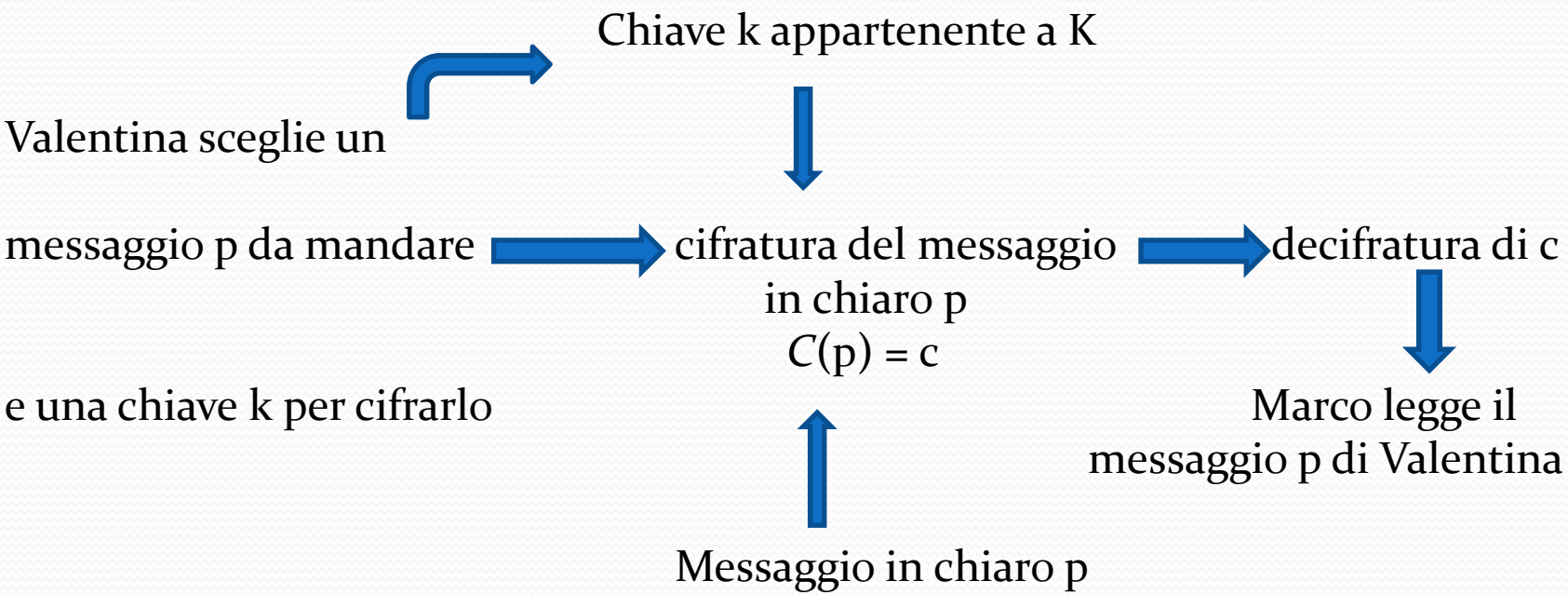
CIFRARIO DI CESARE

Analizziamo il metodo di cifratura prestando particolare attenzione all'impianto matematico che ne consente la realizzazione.

Un **CRITTOSISTEMA (P, K, *C*)** è costituito da:

- L'insieme dei messaggi in chiaro P di cui indichiamo gli elementi con la lettera p
- L'insieme delle chiavi K in cui ogni elemento k determina una trasformazione di cifratura
- L'insieme dei messaggi cifrati *C* i cui elementi sono indicati con la lettera c

la comunicazione tra due persone,
Valentina e Marco, può essere riassunta dal seguente diagramma:



Nel cifrario di Cesare:

- gli elementi p sono le parole che vogliamo inviare;
- la chiave consiste in fase di cifratura nello spostare di tre posti le varie lettere e in fase di decifratura nel rimetterle nella loro corretta posizione ;
- gli elementi c sono il risultato dell'operazione di cifratura.

Se indichiamo con lettere minuscole le 21 lettere dell'alfabeto, ciascuna lettera del nostro messaggio (testo in chiaro) sarà sostituita con la lettera che si trova tre posizioni più avanti, e che per comodità indicheremo con caratteri maiuscoli, ottenendo così un nuovo messaggio (testocifrato) apparentemente privo di significato

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 decidere di generalizzare questo sistema utilizzando una chiave diversa cioè decidendo di spostare le lettere non più di tre posizioni ma di una quantità arbitraria. Un sistema di questo tipo, in cui l'alfabeto cifrante è ottenuto dall'alfabeto in chiaro spostando di un certo numero di posizioni le lettere, prende il nome di **cifrario di Cesare o di cifratura per traslazione.**

Le possibilità per i cifrari di Cesare nel caso della lingua italiana sono solamente 20 perché ovviamente se una lettera si sposta di 21 posizioni, ritorna al punto di partenza. Mentre nel caso dell'alfabeto inglese abbiamo 25 alfabeti cifranti possibili dato che le lettere sono 26.

Abbiamo visto che volendo cifrare un messaggio usando il metodo di Cesare dobbiamo sostanzialmente traslare le lettere di un certa quantità di posizioni (che decidiamo noi e rappresenta la chiave utilizzata per cifrare).

In effetti possiamo interpretare così la procedura che attuiamo:

Assegniamo ad ogni lettera dell'alfabeto in chiaro un numero corrispondente alla sua posizione (la A occupa la posizione 0 e la Z la posizione 20), dopo ciò decidiamo un numero (ad esempio 5) che rappresenta la nostra chiave e lo sommiamo ad ogni posizione così da ottenere che nell'alfabeto cifrante la A corrisponda alla lettera in posizione 5 cioè alla F, la B alla G,…, la R alla Z, la S che occupa la posizione 16 corrisponda alla A, la T alla B,…., la Z alla E.

Il nodo fondamentale di questa procedura sta nel fatto che quando abbiamo deciso la corrispondenza tra la T e la B abbiamo sostanzialmente ragionato cosi:

• la lettera T occupa la posizione 17 (ricorda che partiamo dalla posizione 0),

• 17 + 5=22 ma le posizioni possibili sono 21 e sono numerate da 0 a 20 quindi il numero 22 non corrisponderebbe a nessuna lettera

• 22 = 1 × 21 + 1 e abbiamo deciso che la lettera T doveva corrispondere a quella in posizione 1 cioè alla B

Ed è per questo motivo che la lettera S corrisponde alla A (perché S = posizione 16, 16 + 5 = 21, 21 = 1 × 21 + 0 e la lettera A occupa la posizione 0), la U alla C e così via.

Continua tu … completa l'alfabeto cifrante e traduci la seguente frase:

"**A SETTENTRIONE SCOPPIA UNA GUERRA** "

TRADUZIONE:

- **F ALBBLSBZPTSL AHTUUPF CSF NCLZZF**

Quindi da un punto di vista matematico quando cifriamo con questo metodo operiamo una somma (per traslare) dopodichè se il risultato è maggiore di 21 ci interessiamo solo al resto della divisione.

Questo modo di procedere può sembrare astruso ma in realtà lo utilizziamo quotidianamente ad esempio quando leggiamo l'ora sull'orologio.

Infatti quando leggiamo l'orologio sappiamo benissimo che, ad esempio, le 13:00 corrispondono all'1:00 e le 18:00 alle 6:00, e il motivo di questa corrispondenza sta nel fatto che il resto della divisione per 12 di 13 è 1 mentre di 18 è 6.

9 + 4 = 1

E’ ASSURDO?

Se ci pensiamo un momento .....

il primo numero rappresenta le ore 9 del mattino, dopo 4 ore, sono le tredici, cioè sul nostro orologio la lancetta è sul numero uno!

Ma allora, sempre pensando all'orologio, basta *sommare i due numeri e si ricava il resto dopo aver diviso il risultato per 12*

Quindi: 8+6=2, 10+6=4 e così via.

SEMBRA UN GIOCO!

In effetti, rappresenta una parte importante della matematica, detta appunto *aritmetica dell'orologio*, poiché su tale principio si basa il calcolo delle ore a cicli di 12 o 24.

Gauss introdusse questa notazione circa 200 anni fa!:

4 + 9 = 1 (modulo 12)

Carl Friedrich Gauss
(Brunswick, 30 aprile 1777 – Gottinga, 23 febbraio 1855)

La moltiplicazione o l'elevamento a potenza di un numero su un calcolatore di Gauss funzionano in modo simile: si calcola il risultato su un calcolatore convenzionale, lo si divide per dodici e si prende il resto della divisione.

Pensiamo ad un calcolo "più complicato" ….. 7 x 7…. l'aritmetica dell'orologio fornisce la divisione di 49 per 12,

→ 7 x 7 = 1 (mod.12)

Gauss capì inoltre che non era necessario attenersi al comune orologio da 12 ore per effettuare questo tipo di operazioni, poteva infatti utilizzare orologi con un numero primo di ore: orologi da 5 ore o da 7 ore ad esempio.

3 + 5= 3 (mod.5) se abbiamo scelto il numero 5

8 + 4 = 5 (mod. 7), se abbiamo scelto il numero 7

Nasce così l' aritmetica modulare

Cerchiamo di generalizzare il concetto.

Innanzi tutto diamo una definizione cercando di capire che connessione ha con quanto detto finora.

Definizione

Sia n un intero positivo fissato. Due numeri a ,b € Z sono congrui modulo n se e solo se (a - b) è un multiplo di n, ovvero, espresso in formule, a ≡ b modulo n ↔ (a – b) = n × h per qualche h€ Z .

Esempi:

1. 25 ≡ 1 modulo 3 perché 25 –1 = 24 = 3× **8**
2. 67 ≡ 55 modulo 6 perché 67 – 55 = 12 = 6 × **2**
3. 55 ≡ 1 modulo 6 perché 55 –1 = 54 = 6 ×**9**

Osservazioni.

1. Notiamo che gli esempi 2 e 3 ci suggeriscono l'idea di transitività della congruenza.

Infatti vale anche che 67 ≡ 1 modulo 6 perché 67 –1 = 66 = 6 ×**11.**

Ora possiamo dire che quando dobbiamo criptare un messaggio operiamo modulo 21. Per di più invece di lavorare con tutti i possibili numeri interi lavoriamo solo con quelli compresi tra 0 e 20 (che sono le posizioni possibili).

Infatti se, per assurdo, volessimo operare una traslazione di 63 posizioni, per trovare come criptare, ad esempio, la lettera B dovremmo capire a quale numero b è congruo modulo 21 il numero a = 64= 63 + 1 (che rappresenta la posizione traslata della lettera B).

Ovviamente scoprire che $64 \equiv 43$ modulo 21 anche se è un risultato esatto non ci fornisce nessuna informazione utile perché la lettera numero 43 non esiste! Quindi, in realtà, quando vogliamo capire a "cosa" è congruo un certo numero a modulo n siamo interessati a trovare quell'unico numero b compreso tra 0 e n-1 tale che sia verificata la congruenza.

ESERCIZI DI CIFRATURA E DECIFRATURA

Usando le congruenze:

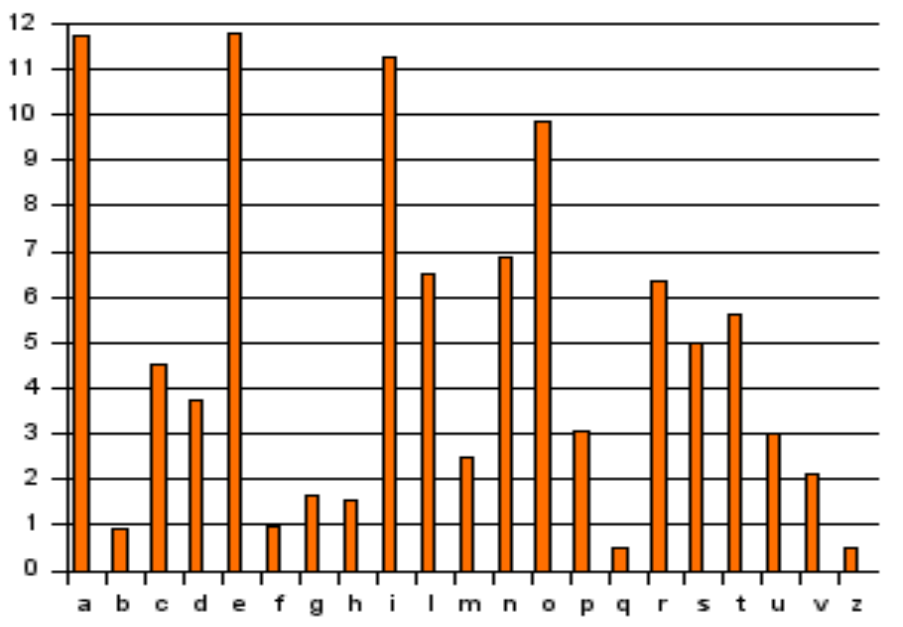
1. Criptare il messaggio “AMBASCIATORE IN PRIGIONE” utilizzando k=7
2. Decriptare il seguente messaggio sapendo che k=16

DE UHMNH GPFZMD IMDFD Z UMDOOHBMSADS Z DGOZMZNNSGOZ

(il corso numeri primi e crittografia è interessante)

Come si puo decifrare un messaggio scritto con un cifrario di tipo k = n 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 decodicati con l'analisi delle frequenze, ad esempio vediamo....

IL CIFRARIO DI VIGENERE

ideato dal diplomatico francese Blaise de Vigenere (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?

- 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 Vigenere e la parola chiave UOVO:

LE RONDINI VOLANO

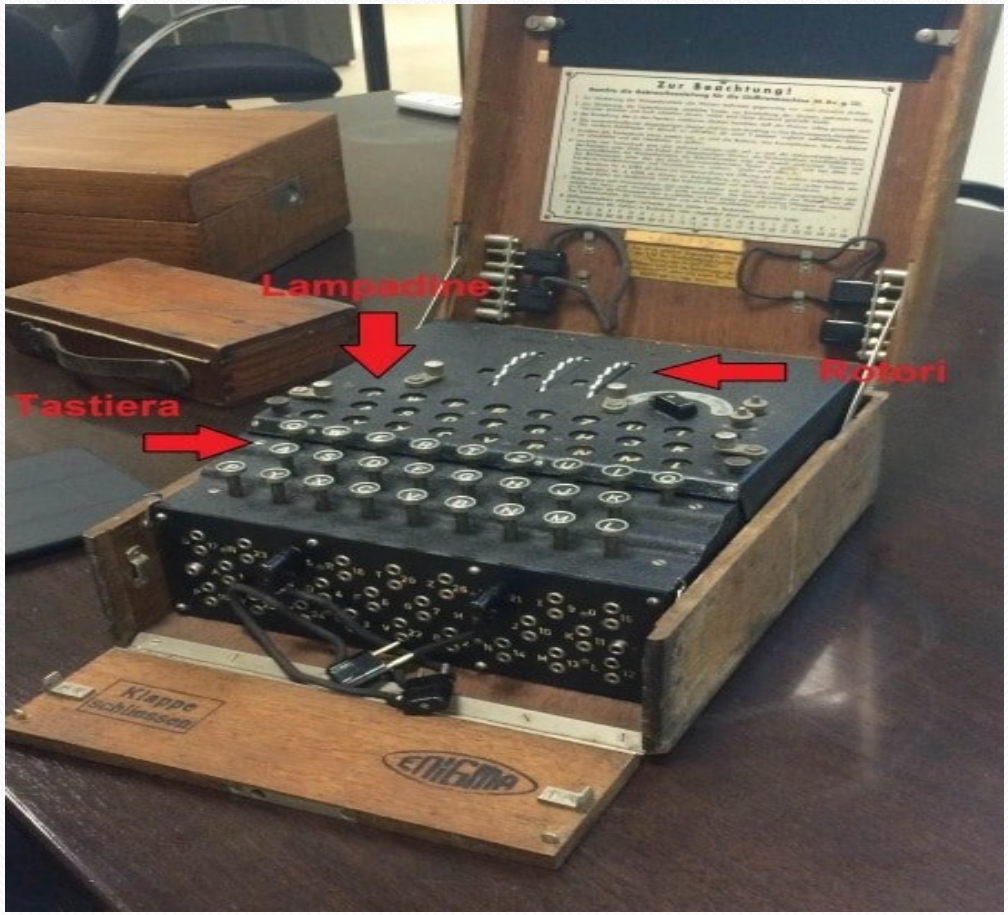
Ora provate a decifrare il seguente messaggio usando la tabella di Vigenere e la parola chiave PALO:

XPCWVIZBXECWHOYCUURUXTT

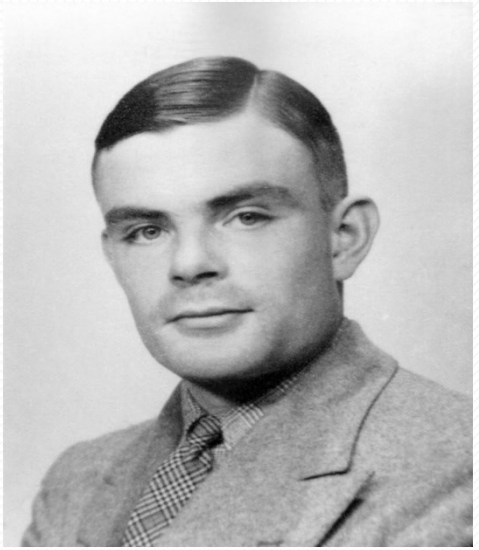
cosa ottieniamo?

MACCHINA ENIGMA 1923

Macchina cifratrice utilizzata dal Terzo Reich durante la Seconda Guerra Mondiale



Alan Turing: Matematico, Logico e Crittografo,



- nasce a Londra nel 1912;
- nel 1940, a 28 anni, e 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 omosessualita 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 Jano, che ha ideato il logo su richiesta di Steve Jobs nel 1977, ha smentito tale leggenda…. *quel che è certo e che ogni volta che utilizziamo una strumento informatico lo dobbiamo in parte a Turing*