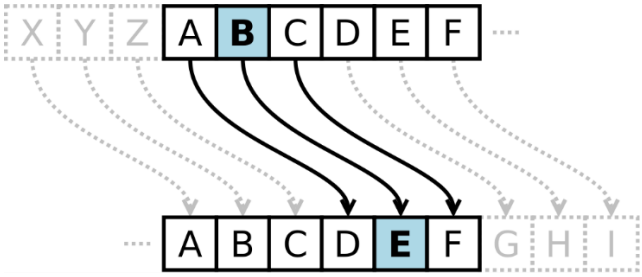
CRITTOGRAFIA E NUMERI PRIMI

La usiamo ogni giorno e non ce ne accorgiamo neppure: stiamo parlando della **crittografia**, un insieme di metodi che tiene al sicuro i nostri telefoni, i nostri acquisti e dovrebbe essere utilizzata per tutti i nostri dati sensibili. Ma che cos'è la crittografia, e come funzionano i sistemi che la sfruttano?

Che cos'è la crittografia? Come si è evoluta nella storia?

La crittografia si può definire come l'insieme delle tecniche utilizzabili per trasmettere **informazioni riservate**, in maniera comprensibile solo al legittimo destinatario. Si è sviluppata principalmente in **ambito spionistico e militare.** Il metodo più antico e forse più famoso è il **cifrario di Cesare**. Non sappiamo se lo avesse realmente inventato il condottiero romano, ma di certo lo aveva utilizzato, e consisteva nella sostituzione di una lettera dell'alfabeto latino con un'altra spostata di un certo numero di posizioni. Nella figura la B viene sostituita con la E; in termini tecnici si dice che la chiave di cifratura è 3.



Utilizzando la chiave 3, la parola CESARE diventa FHVDUH.

PRIMA ATTIVITA': Costruzione e utilizzo del cifrario di Cesare (10 minuti)

- Ritaglia i due dischi in figura e forali nel centro
- Sovrapponi i due dischi e fermali nel centro con l'aiuto di un fermacampioni.

Usa le ruote e le chiavi indicate per criptare i seguenti messaggi:

Chiave=3 NEL MEZZO DEL CAMMIN DI NOSTRA VITA

Chiave=15 FACCIAMO LA PACE

Usa le ruote per decriptare i seguenti messaggi:

Chiave=3 DWWDFFDUH JOL LUULGYFLELOL JDOOL DOOD RUD VHVWD

Chiave=5 HTIPHP L ALNZLBP

Decrittare un messaggio:

E se non si conosce la chiave? Per decifrare un messaggio si può utilizzare l'analisi delle frequenze. In ogni lingua la frequenza di comparsa di ogni lettera dell'alfabeto è molto particolare (vedi tavola delle frequenze della lingua italiana). In italiano poi si può sfruttare il fatto che spesso le parole finiscono con una vocale.

%	Lettera	%	Lettera	%	Lettera
11,79	*e*	*5,63*	t	2,10	v
11,74	*a*	*4,98*	s	1,65	g
11,28	*i*	*4,50*	c	1,54	h
9,83	*o*	*3,73*	d	0,95	f
6,88	n	*3,05*	p	0,92	b
6,51	l	*3,02*	u	0,51	q
6,38	r	*2,52*	m	0,49	z

Tavola delle frequenze lingua italiana

SECONDA ATTIVITA': Decrittazione (20-25 minuti)

Scegli un testo di 5 righe. Puoi scriverlo tu o utilizzare cinque righe di un libro di testo in lingua italiana.

Codifica il messaggio: scegli una chiave, che deve rimanere segreta.

Scambia il messaggio con un altro gruppo e prova a decifrare il messaggio dei tuoi compagni. Per farlo completa la tabella delle occorrenze, che ti serve per calcolare le frequenze di comparsa delle lettere.

Lettera	Occorrenze	Lettera	Occorrenze	Lettera	Occorrenze
A		H		Q	
B		I		R	
C		L		S	
D		M		T	
E		N		U	
F		O		V	
G		P		Z	

Qualche suggerimento: Aiutandoti con la tavola delle frequenze della lingua italiana, prova a sostituire le lettere terminali di una parola con una vocale dell'alfabeto in chiaro, in ordine di frequenza. Controlla quanto hai ottenuto e, se lo ritieni opportuno, prova a cambiare alcune scelte utilizzando le consonanti più frequenti. Ora prova a sostituire le consonanti più frequenti non ancora utilizzate, rivedendo le scelte se trovi parole prive di significato.

Il cifrario di Vigenère

Nel 1586 Blaise de Vigenère inventa un cifrario polialfabetico che prende il suo nome e che considerato per secoli inattaccabile. In realtà esso è il più facile da decrittare di tutti i cifrari **polialfabetici** oggi conosciuti e risulta essere una generalizzazione del cifrario di Cesare. Infatti, al posto di spostare dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base a una parola chiave da scrivere ripetutamente sotto il messaggio. Se ad esempio il messaggio da inviare segretamente è *"BUON APPETITO"* e la parola chiave segreta è *"TASSO"*, scriveremo una tabella come la seguente:

B	U	O	N	A	P	P	E	T	I	T	O
T	A	S	S	O	T	A	S	S	O	T	A

Per crittografare il messaggio, bisogna fare quindi riferimento alla tabella di Vigenère, molto simile per costituzione alla tavola pitagorica. Solitamente si individua nella prima colonna la lettera del messaggio in chiaro che si vuole cifrare e nella prima riga la lettera corrispondente della parola chiave (ad es. B nella prima colonna e T nella prima riga). In questo modo, come a battaglia navale, si ottiene la lettera cifrata.

	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	V
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	W
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	X
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

Ritornando alla nostra cifratura, il messaggio finale sarà allora *"UUGF OIPWLWMO"*.

TERZA ATTIVITA':

Usa il cifrario di Vigenère per decifrare il seguente messaggio, sapendo che la parola chiave utilizzata è PRATI:

Cfn aw errmqrfltzx kaemcki, lwcf shtirnmw pgptahzogiirmxviv cnzxfsh (Mxesmmxe)

Crittografia durante la II Guerra Mondiale

Per secoli la crittografia si è basata su strumenti simili a questo, ma nel XX secolo cominciarono a diffondersi anche complesse **macchine elettromeccaniche.** Le più famose sono sicuramente le **macchine Enigma**, attraverso le quali la Germania comunicava con i suoi sottomarini durante la Seconda guerra mondiale. Per decifrare gli incomprensibili messaggi intercettati, agli alleati non bastò mettere le mani su alcune delle macchine: il matematico britannico Alan Turing dovette costruire anche dei dispositivi speciali che possiamo considerare antenati degli odierni computer.

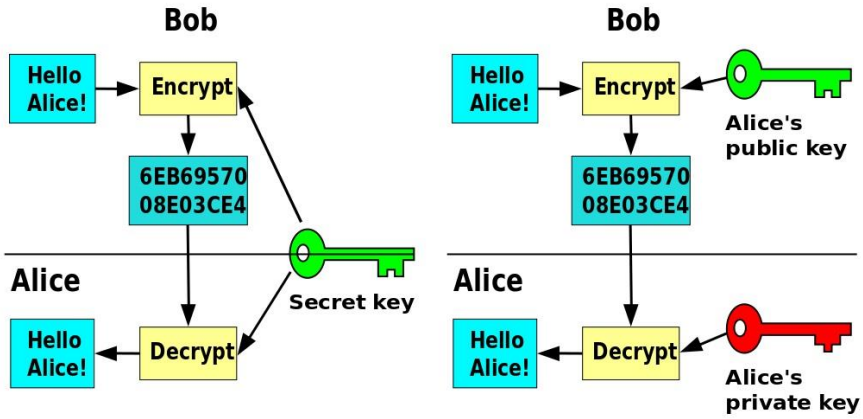
Per capire la potenzialità delle macchine Enigma usa il simulatore che trovi al seguente link:

http://mistic.web.cs.unibo.it/files/enigma/enigma.html#grafico

In cosa consiste oggi la crittografia? Ve li ricordate i numeri primi?

Lo sviluppo dell'informatica nel secondo dopoguerra segna un importante cambiamento nella crittografia. Per secoli il funzionamento di un sistema crittografico era legato alla **segretezza del meccanismo** utilizzato: per questo è stato necessario (anche se non sufficiente) trafugare esemplari di macchine Enigma per capire come decifrare messaggi. Ora invece la crittografia passa attraverso i **computer**, e tutti sanno come sono costruiti e come funzionano. Queste macchine permettono infatti di gestire **regole di codifica e decodifica** basate su **problemi matematici**. Anche questi problemi sono universalmente noti, quindi la segretezza deriva dall'**impossibilità pratica della loro risoluzione**. Un problema molto usato in crittografia è quello della **fattorizzazione in numeri primi**: moltiplicare tra loro dei numeri primi, anche molto grandi, è un'operazione semplicissima per un computer, ma è invece difficilissimo risalire da quel numero ai fattori primi che lo hanno generato.

Nella moderna crittografia la segretezza è quindi basata sulla **chiave,** cioè la sequenza di bit che permettono di codificare o decodificare l'informazione. La chiave può essere **simmetrica** (privata) o **asimmetrica** (coppia di chiavi pubblica/privata). Nei sistemi a chiave simmetrica la stessa chiave permette sia di codificare, sia di decodificare il messaggio. Gli interlocutori che vogliono scambiarsi informazioni in segretezza devono condividere tra loro questa chiave.



Nei sistemi a **chiave pubblica**, invece, la chiave usata per cifrare le informazioni è diversa da quella usata per decifrarle. Ogni interlocutore rende pubblica la propria chiave di cifratura, che viene utilizzata per l'invio del materiale riservato. La chiave di decrittazione, invece, rimane riservata, quindi solo il legittimo destinatario può leggere le informazioni codificate con la sua chiave pubblica.