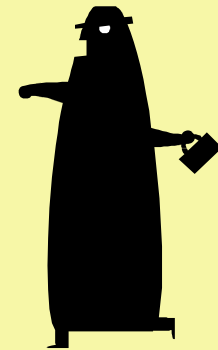


# CRITTOGRAFIA

## la matematica in un mondo di spie

Sebastiano Rizzo – Università del Salento



Il secolo in cui viviamo viene chiamato "il secolo dell' informazione".  
Informazione comporta messaggi inviati da un capo all'altro della Terra  
veicolati dai mezzi più disparati, dal piccione viaggiatore ai cavi ottici al  
web.

Mandare e ricevere messaggi vuol dire "comunicare" e molto spesso la  
necessità di tenere segreti i messaggi è di importanza vitale.

Bisogna quindi saper **criptare**, cioè nascondere il contenuto dei messaggi,  
ma, di contro, vi sarà sempre qualcuno interessato a decifrarli.

Durante la seconda Guerra Mondiale gli Alleati si trovarono a dover  
affrontare una difficoltà apparentemente insormontabile: decifrare i  
messaggi cifrati con la **macchina Enigma** il sistema di cifratura dei  
messaggi segreti dell' Alto Comando Tedesco.

Alla vittoria degli Alleati contribuirono sicuramente gli sforzi dei crittografi inglesi  
che, guidati dal matematico Alan Turing, riuscirono a decifrare tali messaggi.

La macchina Enigma



# Crittografia

Il pericolo di intercettazione di un messaggio da parte di persone indesiderate è stato fin dall'antichità il principale motivo della ricerca di tecniche di alterazione dei messaggi in modo da renderli comprensibili solo alle persone autorizzate.

La crittografia si occupa delle **tecniche matematiche** che consentono di modificare un messaggio in modo che sia comprensibile dal destinatario stabilito, ma sia incomprensibile da un estraneo.

Cosa ha a che fare la matematica con il problema di decifrare un messaggio in codice?

Un argomento apparentemente lontano dalla matematica; in verità, la matematica è presente, anzi incombente, in queste situazioni.

Un messaggio nascosto, un messaggio criptato o meglio un messaggio **cifrato** attiene al campo della matematica già nel nome.

**Per cifrare e decifrare un messaggio in codice occorre quella parte della matematica che si occupa di statistica , di calcolo delle probabilità e di aritmetica modulare .**

## La steganografia

- Una delle prime tecniche di comunicazione segreta, era basata sull'occultamento del messaggio e si chiama **steganografia**, dalle parole greche στεγανός, che significa coperto, e γραφειν, che significa scrivere.
- In tutto il mondo sono state utilizzate innumerevoli forme di steganografia.
- Ad esempio si può nascondere un messaggio con l'inchiostro simpatico, oppure si può nascondere un messaggio in una fotografia pubblicata sul web.

Chi guarda la foto non rileva alcuna anomalia; chi utilizza un adeguato software ed è in possesso della opportuna chiave è in grado di leggere il messaggio nascosto, come è avvenuto, anche recentemente, per alcuni proclami diffusi da terroristi.

## La steganografia

Uno dei metodi più bizzarri per trasmettere le informazioni segrete era utilizzato nell'antica Persia e viene raccontato da Erodoto. Tale metodo consisteva nel rasare i capelli di uno schiavo e nello scrivergli il messaggio sulla testa. Lo schiavo si recava poi dal destinatario del messaggio dopo che gli erano ricresciuti i capelli e il messaggio era recuperato rasandogli nuovamente i capelli.

## Introduzione alla crittografia

Parallelamente allo sviluppo della steganografia ci fu l'evoluzione della *crittografia*, dal greco κρύπτος che significa nascosto.

La crittografia non mira a nascondere il messaggio in sé, ma il suo significato.

Per rendere incomprensibile un testo, lo si altera per mezzo di un procedimento concordato preventivamente dal mittente e dal legittimo destinatario.

Questi può quindi invertire il procedimento per ricavare il messaggio originale.

Il vantaggio della crittografia è che il messaggio eventualmente intercettato da una spia risulta incomprensibile e quindi inutilizzabile.

Infatti l'eventuale intruso, non conoscendo il procedimento di alterazione del messaggio, dovrebbe trovare difficile, se non impossibile, ricostruirne il significato.

E' bene osservare che il mittente e il legittimo destinatario devono condividere a priori una “conoscenza” che consenta la cifratura e la decifratura del messaggio.

Ma tale conoscenza non è il metodo di alterazione del messaggio che può essere noto a tutti, ma è la cosiddetta *chiave segreta* cioè, di solito, una stringa alfanumerica che costituisce un parametro della funzione di cifratura e decifratura e che è condivisa soltanto tra il mittente ed il destinatario.

## La “scitala”

Il più antico crittosistema di cui si ha notizia è probabilmente la *scitala*, citata da Plutarco come in uso dai tempi di Licurgo (IX sec a.C.) ma più sicuramente usata ai tempi di Lisandro (verso il 400 a.C.).

Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio; sul nastro si scriveva per colonne parallele all'asse del bastone, lettera per lettera, il testo segreto.

Tolto il nastro dal bastone, il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la comprensione senza un secondo bastone uguale al primo.



Questo è un breve messaggio cifrato, a prima vista incomprensibile, proviamo a decifrarlo

**PDQGDZH OD FDBDOOHUND**

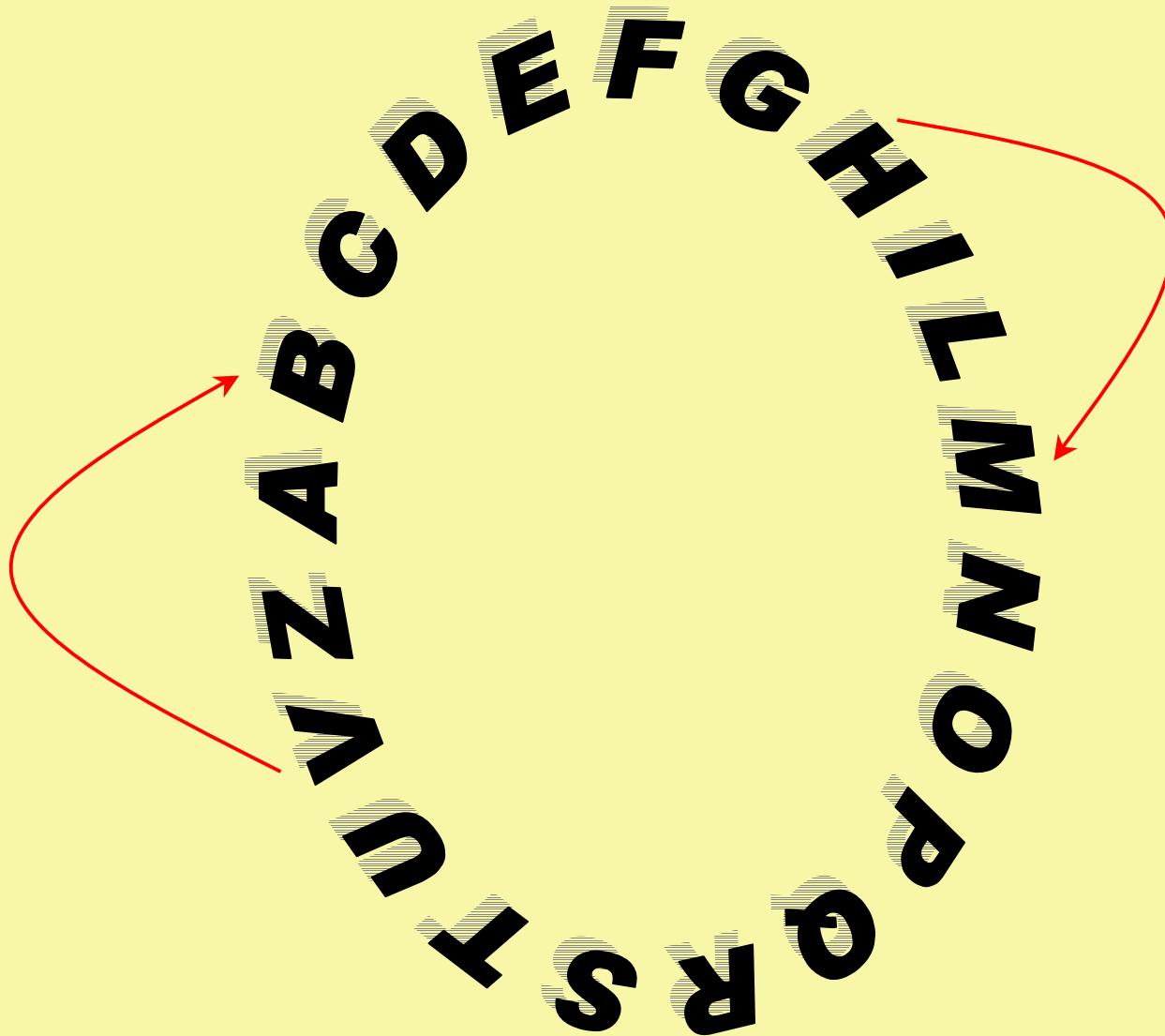


Qual' è la lettera dell'alfabeto italiano più frequente?  
la lettera A

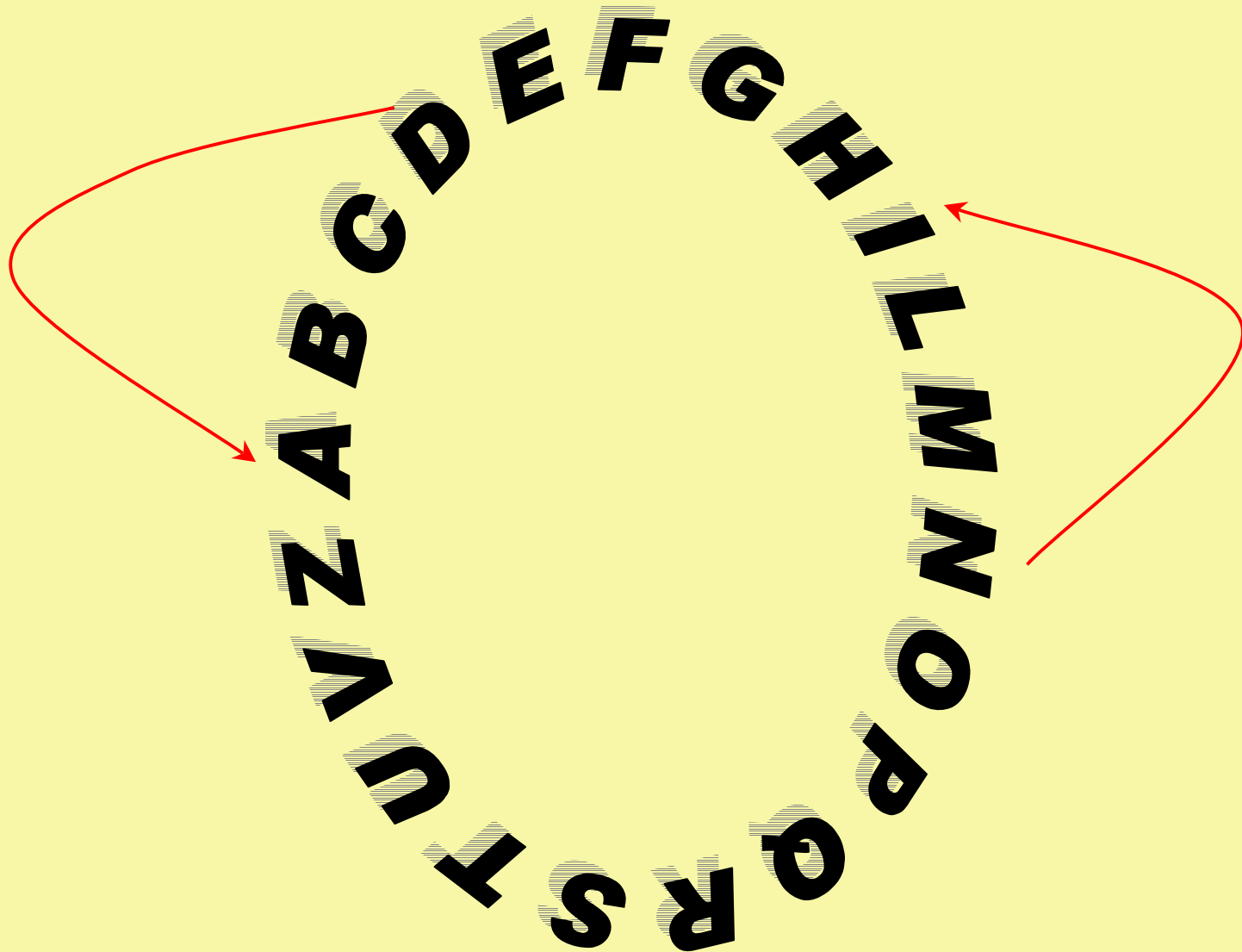
Nel testo "incomprensibile" la lettera più frequente è la D.  
Sostituiamo la D con la A e poiché la A precede di 3 posti la D,  
proviamo a sostituire ad ogni lettera che compare nel  
messaggio cifrato quella che la precede di 3 posti

Quello che si ottiene è il messaggio:  
**MANDATE LA CAVALLERIA**

Ecco brevemente come si può descrivere l'operazione che cifra il messaggio



E quella che lo decifra



## IL "CODICE DI CESARE"

*"... Restano quelle [lettere] a Cicerone, così come quelle ai familiari sugli affari domestici, nelle quali, se doveva fare delle comunicazioni segrete, le scriveva in codice, cioè con l'ordine delle lettere così disposto che nessuna parola potesse essere ricostruita: se qualcuno avesse voluto capire il senso e decifrare, avrebbe dovuto cambiare la quarta lettera degli elementi, cioè D, per A e così via per le rimanenti"*

*(Svetonio, Vita di Cesare, capitolo 56)*

Svetonio quindi ci racconta come già Cesare usasse cifrare i messaggi con il metodo appena visto.

L'antico crittosistema detto "Codice di Cesare" utilizzava quindi come **chiave** il numero 3.

Se indichiamo con  $c_k$  la funzione di cifratura e con  $d_k$  la funzione di decifratura :

Per cifrare :  $c_k(x) = x+3$

E per decifrare :  $d_k(y) = y-3$

## IL "CODICE DI CESARE"

Ma per inviare un messaggio cifrato, spesso è più semplice inviare dei numeri al posto delle lettere.

Vediamo cosa occorre fare nel caso di un messaggio cifrato col codice di Cesare.

# IL "CODICE DI CESARE"

a	b	c	...	...	...	u	v	z
d	e	f	...	...	...	a	b	c

→ **A alfabeto**

→ **Traslazione di A  
(ad esempio 3)**

Sostituiamo ogni lettera con un numero

a	b	c	...	...	...	u	v	z
0	1	2	...	...	...	18	19	20

**E se il valore della traslazione è 3**

0	1	2	...	...	...	18	19	20
(+3)	(+3)	(+3)	...	...	...	(+3)	(+3)	(+3)
3	4	5				0	1	2

E' un modo strano di fare le somme !

Ma siamo sicuri che é tanto strano ?

Eppure è un procedimento che  
usiamo spesso in modo naturale e che  
in Matematica si chiama

*aritmetica modulare*

ma si può anche chiamare

*aritmetica dell'orologio.*

## L'aritmetica dell'orologio



Se un orologio segna l' 1.30, che ora segnerà tra 15 ore ?

Dopo 12 ore le lancette si ritroveranno nella stessa posizione.  
Quindi basta aggiungere 3 ore: le lancette segneranno le 4.30.

Cioè nel conto che facciamo trascuriamo **12** ;  
ma abitualmente trascuriamo anche i **multipli di 12**.

Un altro esempio.

Se adesso sono le 7, tra 40 ore che ore sono ?

Ogni 12 ore le lancette ritornano nella stessa posizione (le 7). Poiché 40 diviso 12 è uguale a 3 con il resto di 4, e occorre trascurare i multipli di 12, la lancetta farà 3 giri completi, più 4 ore. Quindi l'orologio segnerà le 11.

In linguaggio matematico si dice che si è sommato 40 a 7 (*modulo 12*) considerando cioè solo il resto della divisione per 12 :

$(40+7) \pmod{12} = \text{resto della divisione di } 47 \text{ per } 12 = 11.$

Anche il calcolo modulo 7 ci è familiare: esso interviene attraverso i giorni della settimana.

Se oggi è **venerdì**, che giorno sarà tra 33 giorni?

33 diviso 7 è uguale a 4 col resto di 5.

Cioè  $33 \pmod{7}$  è uguale a 5, bisogna avanzare di 5 giorni: sarà **mercoledì**.

## L'aritmetica modulare

Fissiamo un numero naturale  $n > 1$ ; i resti della divisione per  $n$  di un qualunque numero intero relativo possono essere soltanto  $0, 1, 2, \dots, n-1$ .

Denotiamo inoltre con :

$$a \pmod{n}$$

il resto della divisione di  $a$  per  $n$ .

Ad esempio l'espressione  $x = 53 \pmod{15}$ , assegna a  $x$  il valore 8 ( $53 = 3 \cdot 15 + 8$ ).

Quindi, fissato  $n$ , tutti i numeri interi relativi si possono suddividere in  $n$  classi, mettendo in ogni classe i numeri che divisi per  $n$  danno lo stesso resto.

$$\mathbb{Z}_n = \{ [0], [1], [2], \dots, [n-1] \}$$

insieme delle classi di resto modulo  $n$

## L'aritmetica modulare

Per indicare che due interi  $a$ ,  $b$  stanno nella stessa classe di resto modulo  $n$  si scriverà

$$a = b \pmod{n}$$

Ciò significherà che  $a$  e  $b$  divisi per  $n$  danno lo stesso resto o equivalentemente

$$a - b \text{ è un multiplo di } n$$

Ad esempio

$$30 = 51 \pmod{7}$$

Infatti 30 e 51 appartengono alla stessa classe di resto modulo 7, la classe del resto 2.

## L'aritmetica modulare

La somma, la differenza e la moltiplicazione (mod  $n$ ) si effettuano così :  
si esegue in  $\mathbb{Z}$  e si sostituisce a tale numero  $x$  il corrispondente  $x \pmod{n}$ .

**Esempi :**

$$\text{Se } n=4 : 13+8 = 21 \rightarrow (13 + 8) \pmod{4} = 1;$$

$$\text{Se } n=3 : 5-18 = -13 = (-5) \cdot 3 + 2 \rightarrow (5-18) \pmod{3} = 2;$$

$$\text{Se } n = 10 : 7 \cdot 6 = 42 \rightarrow 7 \cdot 6 \pmod{10} = 2$$

## IL "CODICE DI CESARE"

Il codice di Cesare è un esempio di codice o cifrario a sostituzione monoalfabetica : ogni simbolo del testo in chiaro viene sostituito in un altro simbolo e conserverà tale sostituzione durante tutta la fase di cifratura.

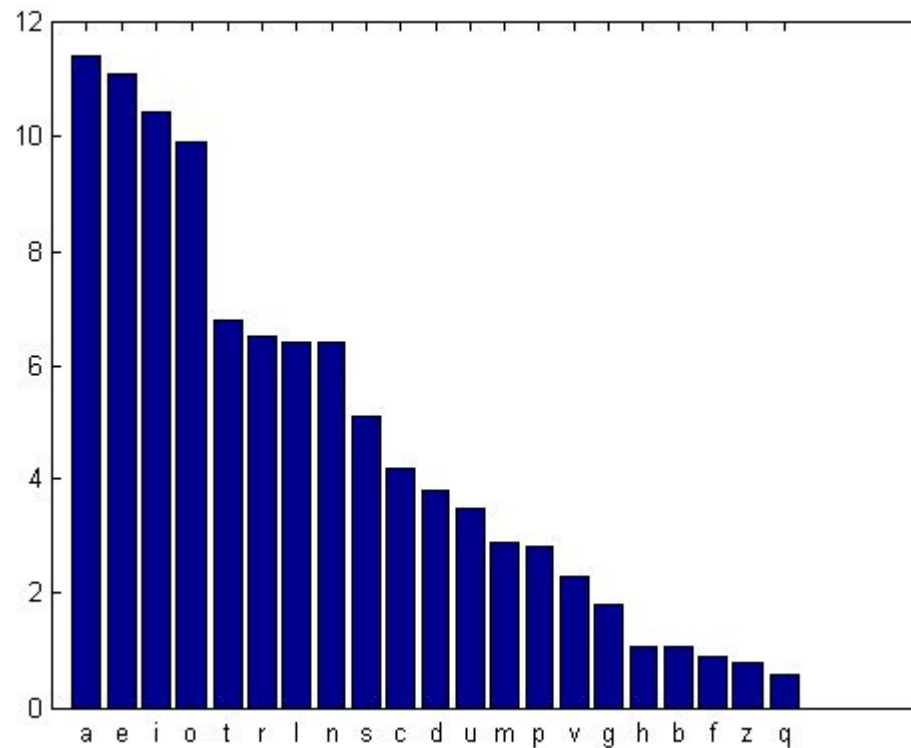
Il cifrario per sostituzione monoalfabetica è forse il più classico dei cifrari; la sua sicurezza è però accettabile solo per messaggi molto brevi.

La crittanalisi di questi sistemi si fonda infatti su metodi statistici tanto più efficienti quanto più lunghi e numerosi sono i testi cifrati che si hanno a disposizione.

Si sfrutta il fatto che ogni lingua ha una distribuzione delle frequenze dei caratteri molto caratteristica.

## IL “CODICE DI CESARE”

In italiano p.es. le lettere più frequenti sono le vocali A, E, I; in francese la E è di gran lunga la lettera più frequente ...



Ancor più caratteristica è la frequenza dei bigrammi e dei trigrammi.

## IL "CODICE DI CESARE"

Per forzare un testo cifrato monoalfabetico, si esegue un'analisi della frequenza delle lettere presenti. È molto utile rilevare anche i bigrammi e trigrammi più frequenti.

I caratteri più frequenti nel testo cifrato, saranno le lettere più frequenti nella lingua; e così i bigrammi e i trigrammi ...

In genere è sufficiente qualche tentativo per riconoscere qualche parola e a questo punto il lavoro è ... in discesa.

## Il cifrario di Vigenère

Il punto di debolezza del cifrario di Cesare fu superato da Blaise de Vigenère che propose nel 1586 un cifrario a sostituzione polialfabetica che per la sua ingegnosità e semplicità è stato usato per quasi 3 secoli.

Il metodo è una generalizzazione del cifrario di Cesare; invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato dalla **chiave** che in questo caso non è un numero ma una **parola**, che comunque può essere trasformata, come anche il testo in chiaro, in una sequenza di numeri :

A=0, B=1, ..., Y=24, Z=25 (utilizzando l'alfabeto inglese).

## Il cifrario di Vigenère

Supponiamo di voler cifrare il messaggio

DOMANIATTACCHIAMO

con la chiave

SALENTO

Si procede in questo modo:

1. Si ripete la parola chiave sotto il messaggio quante volte entra

D	O	M	A	N	I	A	T	T	A	C	C	H	I	A	M	O
S	A	L	E	N	T	O	S	A	L	E	N	T	O	S	A	L

2. Si trasformano il testo e la chiave in sequenze di numeri
3. Si cifrano le lettere sommando (modulo 26) il numero associato alla lettera in chiaro con il numero associato alla sottostante lettera della chiave.

# Il cifrario di Vigenère

D	O	M	A	N	I	A	T	T	A	C	C	H	I	A	M	O
S	A	L	E	N	T	O	S	A	L	E	N	T	O	S	A	L

3	14	12	0	13	8	0	19	19	0	2	2	7	8	0	12	14
18	0	11	4	13	19	14	18	0	11	4	13	19	14	18	0	11
21	14	23	4	0	1	14	11	19	11	6	15	0	22	18	12	25
V	O	X	E	A	B	O	L	T	L	G	P	A	W	S	M	Z

## Alfabeto numerico

A = 0	O = 14
B = 1	P = 15
C = 2	Q = 16
D = 3	R = 17
E = 4	S = 18
F = 5	T = 19
G = 6	U = 20
H = 7	V = 21
I = 8	W = 22
J = 9	X = 23
K = 10	Y = 24
L = 11	Z = 25
M = 12	
N = 13	

Ovviamente chi riceve il messaggio usa il procedimento opposto per decifrarlo : sottrae (mod 26) da ogni lettera ( o numero) del messaggio cifrato ricevuto, la lettera ( o il numero) corrispondente della parola chiave.

Per esempio nel messaggio precedente il 1° numero ricevuto è 21 e la prima cifra della chiave è 18 ; allora

$$(21 - 18) \pmod{26} = 3 \pmod{26} = 3 \rightarrow \mathbf{D}$$

L'ottavo numero ricevuto è 11 e l'ottava cifra della chiave è 18

$$11 - 18 = -7 \rightarrow -7 = (-1) \cdot 26 + 19 \rightarrow$$

$$(11 - 18) \pmod{26} = -7 \pmod{26} = 19 \rightarrow \mathbf{T}$$

## Il cifrario di Vigenère

Per semplificare l'operazione precedente, si può usare una tavola quadrata, composta da alfabeti ordinati (ad esempio di 26 lettere) spostati di una lettera; quindi la prima riga è formata dall' ALFABETO decifrante; le righe sottostanti sono ciascuna ottenuta da un "Codice di Cesare" di chiave 1 rispetto alla riga precedente.

Ecco la tavola:

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

## Il cifrario di Vigenère

Il testo cifrato si ottiene sostituendo alla lettera in chiaro quella che si trova, nella tavola, all'incrocio tra la lettera in chiaro e quella corrispondente della chiave.

Mess. chiaro	D	O	M	A	N	I	A	T	T	A	C	C	H	I	A	M	O
CHIAVE	S	A	L	E	N	T	O	S	A	L	E	N	T	O	S	A	L
Mess. cifrato	V	O	X	E	A	B	O	L	T	L	G	P	A	W	S	M	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	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



Per esempio la D di DOMANI e la S di SALENTO, si trovano rispettivamente sulla quarta colonna e sulla diciannovesima riga: il carattere del testo cifrato è quello che si trova all'incrocio : la V.

D	O	M	A	N	I	A	T	T	A	C	C	H	I	A	M	O
S	A	L	E	N	T	O	S	A	L	E	N	T	O	S	A	L
V	O	X	E	A	B	O	L	T	L	G	P	A	W	S	M	Z

## Il cifrario di Vigenère

Osserviamo che accadono due cose fondamentali:

una lettera del messaggio in chiaro può essere trasformata in lettere diverse nel testo cifrato; nel primo esempio,

D	O	M	A	N	I	A	T	T	A	C	C	H	I	A	M	O
S	A	L	E	N	T	O	S	A	L	E	N	T	O	S	A	L
V	O	X	E	A	B	O	L	T	L	G	P	A	W	S	M	Z

le due T , le quattro A e le due M sono cifrate con caratteri differenti.

nel caso considerato la A diventa una volta E, una volta O, una volta L e una volta S.

Lettere diverse del testo in chiaro possono essere trasformate in una stessa lettera; nell'esempio T ed A sono cifrate entrambe con la L; N ed H sono cifrate entrambe con la A.

## Il cifrario di Vigenère

E' evidente che questo tende a distruggere la corrispondenza tra le frequenze relative delle lettere nel testo in chiaro e quelle dei simboli nel messaggio cifrato (corrispondenza che era proprio il punto debole dei codici monoalfabetici).

## Il cifrario di Vigenère

Un appassionato della crittografia che diede un notevole contributo alla decifrazione dei messaggi, fu Friedrich Kasiski (1805-1881), un ufficiale prussiano che pubblicò un trattato crittografico in cui illustrava una tecnica per demolire il cifrario di Vigenère.

In realtà la scoperta della tecnica risale a qualche anno prima ed è da attribuire al matematico inglese Charles Babbage (1791-1871).

Kasiski fornì un metodo per individuare dapprima la lunghezza della chiave e successivamente il suo valore.

## Il cifrario di Vigenère

Per trovare la lunghezza della chiave occorre fare la seguente osservazione :

due porzioni identiche del testo in chiaro vengono cifrate allo stesso modo solo se la porzione di chiave atta a cifrarle è la stessa per entrambe.

Quindi, se troviamo due porzioni identiche del testo cifrato, ciascuna di lunghezza almeno tre, allora ci sono buone probabilità che esse corrispondano a pezzi identici del testo in chiaro.

Il test di Kasiski cerca le coppie di porzioni identiche nel testo cifrato di lunghezza almeno tre e memorizza la distanza tra le posizioni iniziali delle due porzioni.

## Il cifrario di Vigenère

Se si ottengono le distanze  $d_1, d_2, \dots$ ; allora si può dedurre che la lunghezza della chiave è il massimo comune divisore delle  $d_i$ .

Questo metodo fornisce solo la probabile lunghezza della chiave e non il suo valore.

Ma una volta stabilita la lunghezza della parola chiave, il crittoanalista può decomporre il testo cifrato in tante sottosequenze quante sono le lettere della chiave e analizzarle singolarmente dato che ogni sottosequenza è cifrata attraverso un semplice cifrario monoalfabetico.

## Il cifrario di Vigenère

### Esempio

t	i	a	m	o	c	i	t	r	o	v	i	a	m	o	a	l	l	e	t	r	e	
v	e	r	d	e	v	e	r	d	e	v	e	r	d	e	v	e	r	d	e	v	e	e
o	m	r	p	s	x	m	k	u	s	q	m	r	p	s	v	p	c	h	x	m	i	

La distanza tra due porzioni del testo cifrato è 10,  
allora la lunghezza della parola chiave sarà 5 o 10  
(e in effetti è 5)

## Il cifrario di Vigenère

Se la parola chiave è lunga  $m$ , formiamo una matrice di  $m$  righe mettendo in colonna una dopo l'altra le lettere ( o i numeri) del messaggio cifrato. Otteniamo così in ogni riga un messaggio cifrato con un codice di sostituzione monoalfabetica che si può attaccare con il metodo statistico



Se per esempio la chiave è lunga 5 ed il messaggio cifrato è di 1001 caratteri

$c_1 c_2 c_3 c_4 \dots c_{1001}$

scriviamo:

riga 1 :  $c_1 c_6 c_{11} \dots c_{996} c_{1001}$

riga 2 :  $c_2 c_7 c_{12} \dots c_{997}$

riga 3 :  $c_3 c_8 c_{13} \dots c_{998}$

riga 4 :  $c_4 c_9 c_{14} \dots c_{999}$

riga 5 :  $c_5 c_{10} c_{15} \dots c_{1000}$

## Crittografia a chiave pubblica

Nei metodi di cifratura monoalfabetici e polialfabetici, è abbastanza semplice ottenere la chiave di decifratura da quella di cifratura : in alcuni casi è identica, in altri è ottenibile mediante una funzione facilmente calcolabile. Nasce quindi la necessità di costruire un metodo **asimmetrico** di crittografia cioè di un crittosistema con la proprietà che chi conosce solo la chiave di cifratura non può risalire alla chiave di decifratura (senza dover affrontare calcoli di lunghezza proibitiva).



## Crittografia a chiave pubblica

Il *sistema crittografico a chiave pubblica* è basato sull'uso di due chiavi generate in modo che sia impossibile ricavare una dall'altra.

Le due chiavi vengono chiamate **pubblica** e **privata**: la prima serve per codificare i messaggi e la seconda per decodificare gli stessi.

Una persona che deve comunicare con un'altra non deve fare altro che codificare il messaggio con la chiave **pubblica** del destinatario, che una volta ricevuto il messaggio, non dovrà fare altro che decodificarlo con la chiave segreta **privata**.

Ogni utente possiede quindi, una *coppia di chiavi* quella **pubblica** può essere tranquillamente distribuita e resa di pubblico dominio, perché consente solo di cifrare il messaggio, mentre quella **privata**, che serve per decifrare, deve essere mantenuta segreta.

## Crittografia a chiave pubblica

Testo in chiaro  $\longrightarrow$   $f$   $\longrightarrow$  Testo codificato

Testo codificato  $\longrightarrow$   $f^{-1}$   $\longrightarrow$  Testo in chiaro

Ma la funzione di cifratura  $f$  è tale che da essa non si può ottenere la funzione di decifratura  $f^{-1}$

## Crittografia a chiave pubblica

La prima applicazione pratica basata sulle tecniche di crittografia a chiave pubblica fu sviluppata nel 1978 da tre professori: R. **R**ivest, A. **S**hamir e L. **A**dleman che realizzarono una procedura di calcoli matematici che prese il nome di “algoritmo **RSA**”, dalle iniziali dei suoi inventori.

## Crittografia a chiave pubblica

La funzione unidirezionale, che sta alla base dell'**RSA**, viene costruita sfruttando il fatto che è abbastanza facile trovare due numeri primi di centinaia di cifre, ma dato il loro prodotto, è oltremodo difficile risalire ai fattori che lo compongono.

Occorrerebbero molti anni di calcolo su migliaia di computers per fattorizzare il prodotto di due numeri primi molto grandi (ognuno cioè di 300 cifre).

## Crittografia a chiave pubblica

### Qualche notazione matematica

Sia  $n$  un numero naturale, usiamo il simbolo  $\varphi(n)$  per indicare quanti sono i numeri minori di  $n$  e primi con esso :

per indicare che due numeri  $a$  e  $b$  sono primi tra loro si scrive

$$(a,b) = 1$$

In maniera rigorosa occorre introdurre la definizione di **funzione di Eulero** :

chiamiamo **funzione di Eulero** la funzione  $\varphi$  che ad ogni numero naturale  $n$  associa il numero

$$\varphi(n) = |\{ b \in \mathbb{N} \mid 0 < b < n \text{ e } (b, n) = 1 \}|$$

# Crittografia a chiave pubblica

## Esempi

$$\text{Se } n = 5 \rightarrow \varphi(5) = |\{1,2,3,4\}| = 4$$

$$\text{Se } n = 7 \rightarrow \varphi(7) = |\{1,2,3,4,5,6\}| = 6$$

$$\text{Se } n = 10 \rightarrow \varphi(10) = |\{1,3,7,9\}| = 4$$

$$\text{Se } n = 11 \rightarrow \varphi(11) = |\{1,2,3,4,5,6,7,8,9,10\}| = 10$$

## Due Proprietà

I) Se  $n$  è un numero primo, allora  
$$\varphi(n) = n - 1.$$

II) Se  $m, n \in \mathbb{N}$  e sono tali che  $(m, n) = 1$ .  
Allora la funzione  $\varphi$  di Eulero è  
moltiplicativa, cioè:  
$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

## Crittografia a chiave pubblica

Per quello che verrà in seguito occorre introdurre il concetto di inverso (mod  $n$ ) di un numero.

**Def.** Se  $a$  è un intero, si chiama **inverso di  $a$  (mod  $n$ )** un numero  $b$  (se esiste) tale che :

$$a \cdot b = 1 \pmod{n}$$

$$( \text{ e quindi } a \cdot b - 1 = kn , k \in \mathbb{Z} )$$

Il seguente Teorema ci dice quali sono i numeri che sicuramente ammettono inverso

**Teorema** Se  $a$  è primo con  $n$ , allora  $a$  ammette inverso (mod  $n$ ) .

## Crittografia a chiave pubblica

Per quello che segue occorre anche il seguente :

**Teorema di Eulero :**

Se  $a (< n)$  è primo con  $n$  , allora :

$$a^{\varphi(n)} = 1 \pmod{n}$$

$$( \text{cioè } a^{\varphi(n)} - 1 = k \cdot n , k \in \mathbb{Z} )$$

## Crittografia a chiave pubblica Cifrario RSA

Come si cifra e successivamente si decifra un messaggio con il metodo RSA ?

Supponiamo che Bob debba mandare un messaggio ad Alice

Alice sceglie a caso due numeri primi molto grandi  $p$  e  $q$  e pone  $n = p \cdot q$ .

Conoscendo la fattorizzazione di  $n$  Alice può calcolare:

$$\varphi(n) = \varphi(p) \cdot \varphi(q) = (p - 1)(q - 1).$$

Chi conosce  $n$  ma non la sua fattorizzazione non è in grado di calcolare  $\varphi(n)$ .

## Crittografia a chiave pubblica Cifrario RSA

Alice sceglie poi un intero  $e$  tale che:

$$1 < e < \varphi(n) \quad e \quad (e, \varphi(n)) = 1$$

e rende pubblico sia  $n$  che  $e$ .

Ossia la chiave pubblica è la coppia  $(n, e)$ .

Poiché  $e$  è primo con  $\varphi(n)$ ,  $e$  ammette inverso (mod  $\varphi(n)$ ) e

Alice calcola tale inverso  $d$  :

quindi,  $d$  è un intero tale che

$$e \cdot d = 1 \pmod{\varphi(n)}$$

Poiché solo Alice conosce  $\varphi(n)$ , nessun altro all'infuori di lei può calcolare  $d$ .

La chiave che Alice tiene segreta è quindi  $d$ .

$d$  rappresenta l'informazione aggiuntiva senza la quale è impossibile invertire la funzione di cifratura.

## Crittografia a chiave pubblica Cifrario RSA

In che modo Bob manda un messaggio ad Alice?

Bob trasforma dapprima il messaggio in una sequenza di numeri utilizzando ad esempio la seguente tabella in cui l'alfabeto ordinario con maiuscole e minuscole e i simboli di punteggiatura sono messi in corrispondenza con un alfabeto numerico.

a = 00	u = 20	O = 40
b = 01	v = 21	P = 41
c = 02	w = 22	Q = 42
d = 03	x = 23	R = 43
e = 04	y = 24	S = 44
f = 05	z = 25	T = 45
g = 06	A = 26	U = 46
h = 07	B = 27	V = 47
i = 08	C = 28	W = 48
j = 09	D = 29	X = 49
k = 10	E = 30	Y = 50
l = 11	F = 31	Z = 51
m = 12	G = 32	Spazio bianco = 52
n = 13	H = 33	Punto = 53
o = 14	I = 34	Virgola = 54
p = 15	J = 35	Punto e virgola = 55
q = 16	K = 36	Punto interrogativo = 56
r = 17	L = 37	Punto esclamativo = 57
s = 18	M = 38	Apostrofo/accento = 58
t = 19	N = 39	

## Crittografia a chiave pubblica

### Cifrario RSA

1. Dopo Bob fraziona il messaggio in una successione  $P_i$  di blocchi di numeri tutti con lo stesso numero di cifre. Ogni  $P_i$  si chiama unità elementare di messaggio.
2. Per ogni unità elementare  $P$ , Bob calcola  $C = P^e \pmod{n}$  e spedisce  $C$  ad Alice.
3. Alice riceve  $C$  ed è l'unica che può decifrare  $P$  poiché, per il Teorema di Eulero, risulta  $P = C^d \pmod{n}$ .

## Crittografia a chiave pubblica Cifrario RSA

Infatti, per il Teorema di Eulero, risulta

$$P^{\varphi(n)} = 1 \pmod{n}$$

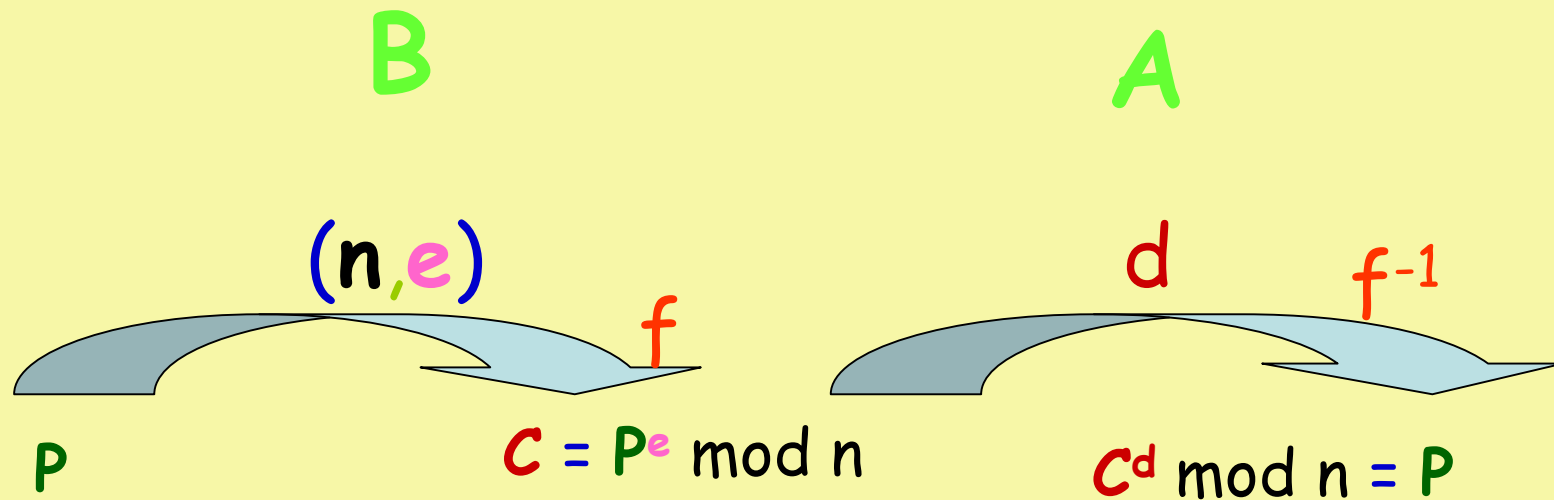
$$\text{ed inoltre } e \cdot d = k \cdot \varphi(n) + 1$$

Quindi :

$$\begin{aligned} C^d \pmod{n} &= (P^e)^d \pmod{n} = P^{ed} \pmod{n} = \\ P^{k \cdot \varphi(n) + 1} \pmod{n} &= (P^{\varphi(n)})^k \cdot P \pmod{n} = \\ 1^k \cdot P \pmod{n} &= P \pmod{n} = P \end{aligned}$$

# Crittografia a chiave pubblica

## Cifrario RSA

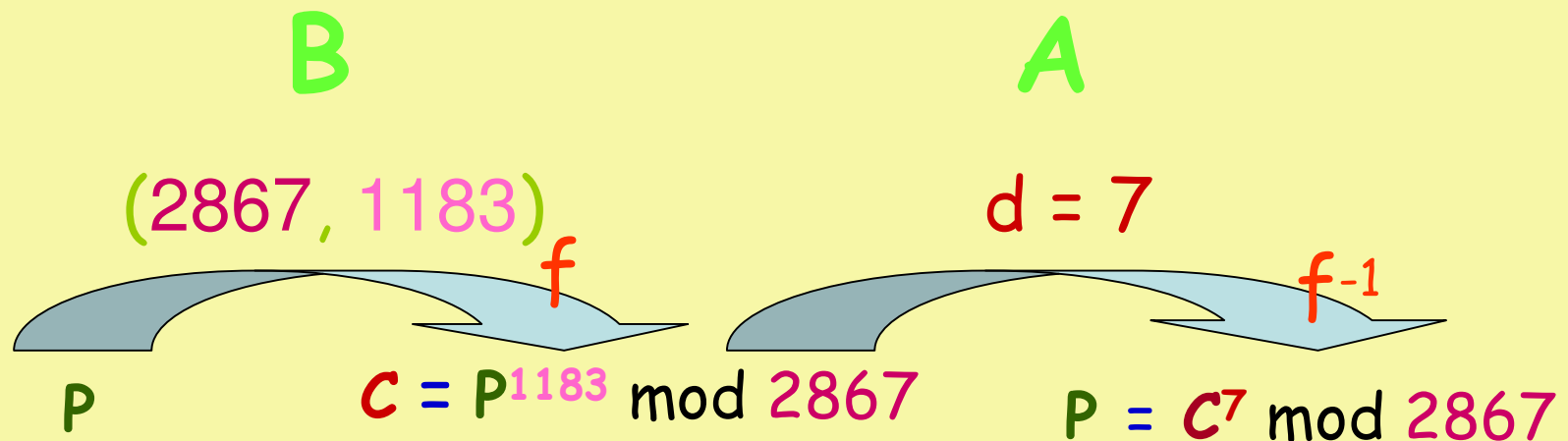


# Crittografia a chiave pubblica

## Cifrario RSA

Esempio

I due primi di Alice siano  $p = 47$  e  $q = 61$  ( $n = 47 \cdot 61 = 2867$ ) e supponiamo che abbia scelto  $e = 1183$ .



## Crittografia a chiave pubblica Cifrario RSA

Supponiamo inoltre che il messaggio che Bob vuole inviare ad Alice sia:

“Sono uscito”.

Bob deve prima di tutto convertire il messaggio in un numero utilizzando l'alfabeto numerico.

## Crittografia a chiave pubblica Cifrario RSA

La versione numerica della frase “Sono uscito” diventa:

$P = 4414131452201802081914$

Bob effettua a questo punto il frazionamento del suddetto numero in una successione  $P_i$  di blocchi di numeri tutti con lo stesso numero di cifre ad esempio 3.

## Crittografia a chiave pubblica Cifrario RSA

$P = 441/413/145/220/180/208/191/4$

$P_1 = 441$     $P_2 = 413$     $P_3 = 145$     $P_4 = 220$

$P_5 = 180$     $P_6 = 208$     $P_7 = 191$     $P_8 = 452$

Osserviamo l'aggiunta del numero 52 all'ultimo blocco per fare in modo che anche  $P_8$  abbia 3 cifre.

## Crittografia a chiave pubblica Cifrario RSA

A questo punto Bob è pronto per cifrare il messaggio da inviare ad Alice.

Bob determina i blocchi cifrati  $C_i$  utilizzando la funzione di codifica.

Il primo blocco è dato da:

$$C_1 = 441^{1183} \bmod 2867 = 2515.$$

Analogamente calcola gli altri blocchi:

## Crittografia a chiave pubblica Cifrario RSA

$$C_1 = 2515 \quad C_2 = 1572 \quad C_3 = 1980$$

$$C_4 = 1426 \quad C_5 = 1376 \quad C_6 = 1338$$

$$C_7 = 1427 \quad C_8 = 728$$

Alice, una volta ricevuti i blocchi  $C_i$ , è l'unica in grado di ricavare gli 8 blocchi  $P_i$  utilizzando la funzione di decodifica .

$$(C_i)^d \pmod{n} = P_i \quad \text{e quindi per } C_1$$

$$2515^7 \pmod{2867} = 441 \quad \text{ecc.}$$