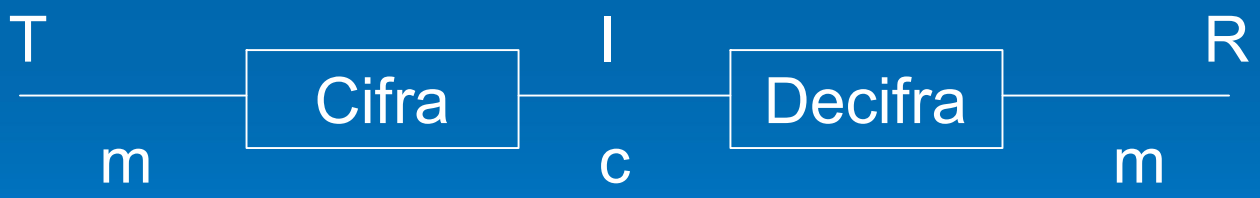
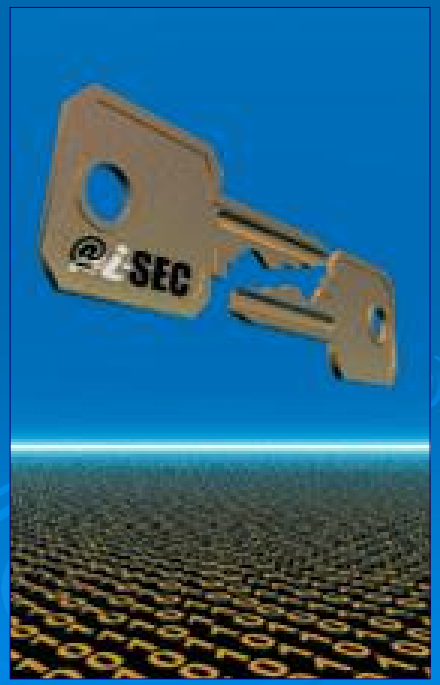
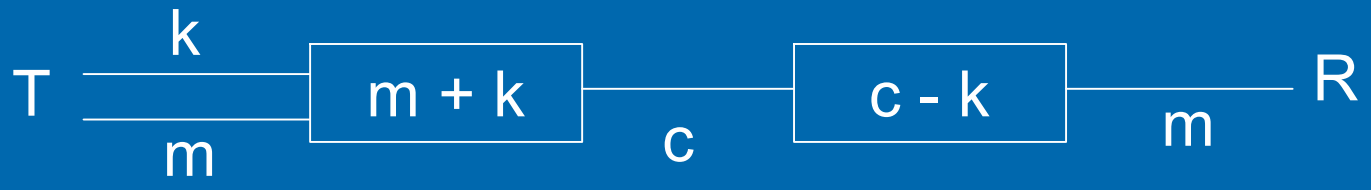
La Crittografia

Il problema fondamentale della crittografia è quello di trasmettere riservato in forma cifrata o, dal punto di vista duale, quello di intercettare e decrittare un messaggio cifrato.





Il Codice di Cesare



c = dxjxul gl exrq fgpsohdqqr

k = 3

m = auguri di buon compleanno

Chiaro: 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

Cifrato: 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

Cifrario di Vigenère

Proposto dal diplomatico francese Blaise de Vigenère e ritenuto inattaccabile fino alla metà dell'Ottocento. Si utilizza una tabella di dimensione 26x26 in cui la riga i-sima contiene l'alfabeto ruotato verso sinistra di i-1, ed una chiave che è una parola segreta k. Dato un messaggio m, lo si allinea con la chiave k. Ogni lettera del messaggio viene sostituita con la lettera della tabella che è all'incrocio tra la riga che inizia con la lettera del messaggio e la colonna che inizia con la lettera della chiave (allineata con quella del messaggio)

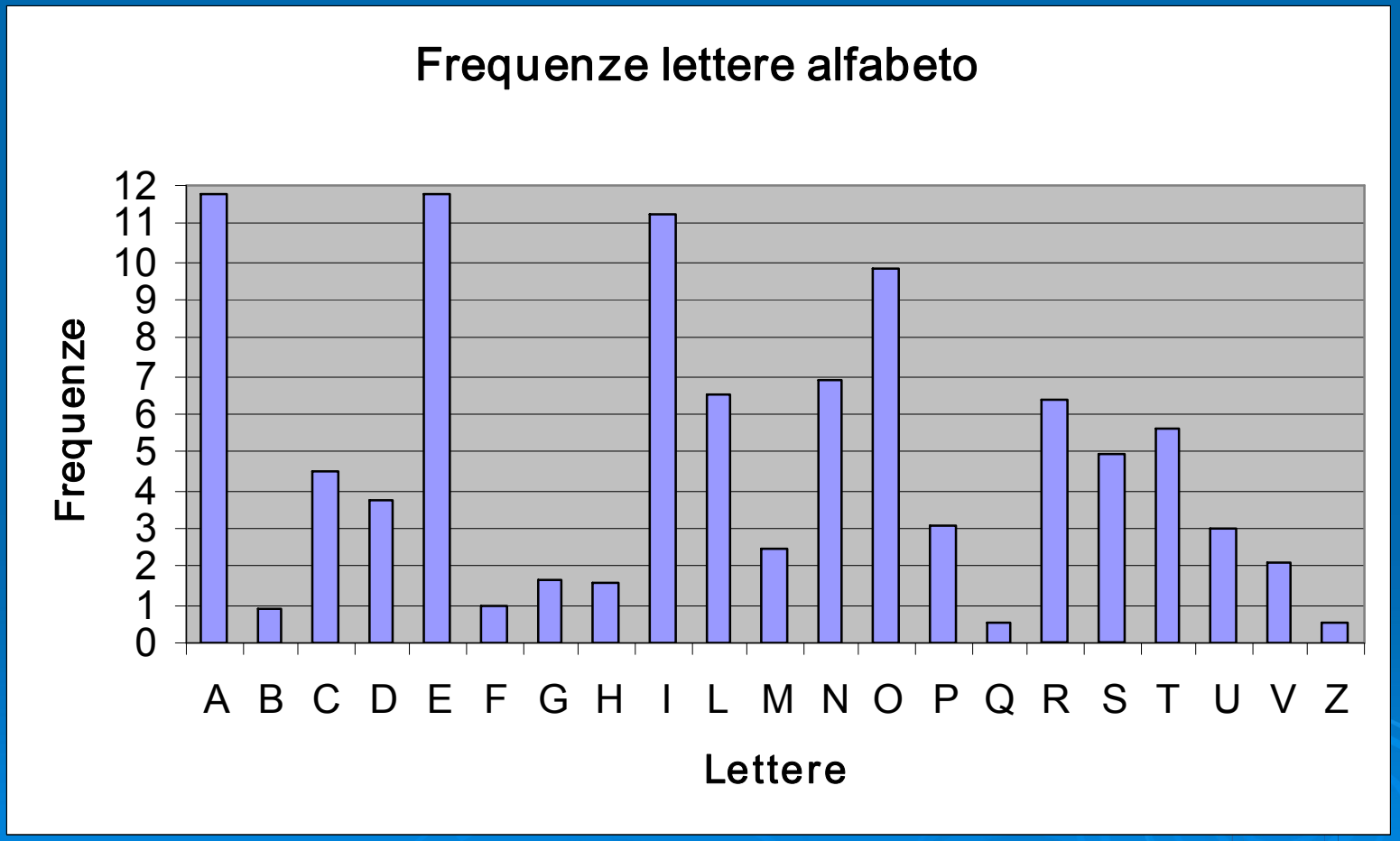
Tabella di Vigenère

A	B	C	…..	X	Y	Z
B	C	D	…..	Y	Z	A
C	D	E	…..	Z	A	B
…..	…..	…..	…..	…..	…..	…..
X	Y	Z	…..	U	V	W
Y	Z	A	…..	V	W	X
Z	A	B	…..	W	X	Y

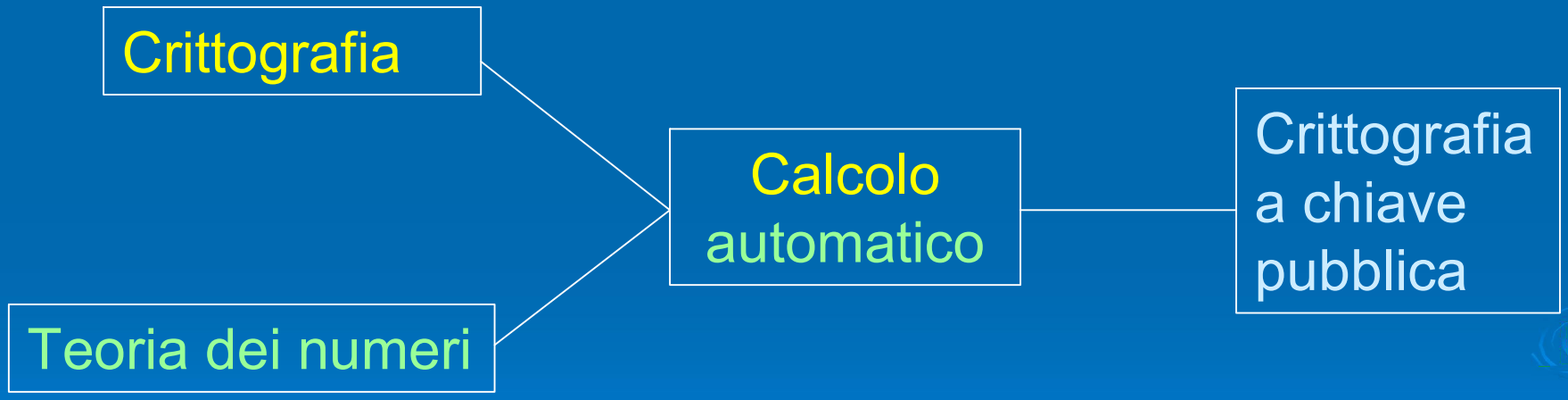
Chiave k = ABRA, M = Il DELFINO

I	L	D	E	L	F	I	N	O
A	B	R	A	A	B	R	A	A
↓	↓	↓	↓	↓	↓	↓	↓	↓
I	M	U	E	L	G	Z	N	O

Crittoanalisi Statistica

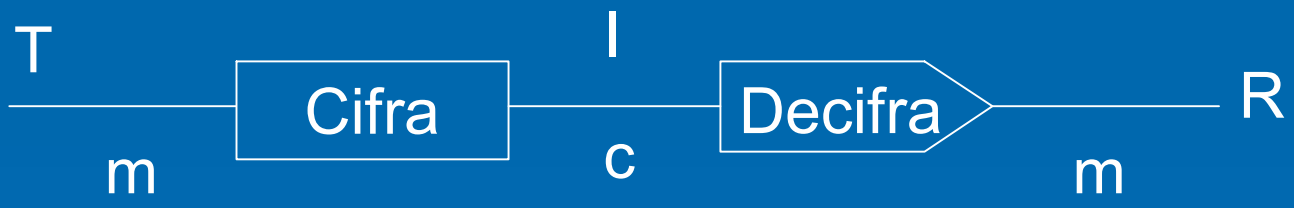


L’antica arte della crittografia è diventata una disciplina moderna grazie alla teoria dei numeri ed allo sviluppo dei computers



Crittografia a chiave pubblica

Il destinatario R pubblica la propria chiave e chiunque voglia mandargli i messaggi dovrà usarla. La sua chiave è pubblica ed anche il messaggio cifrato lo è, ma solo R sa come decifrarlo. Tale metodo è ignoto anche a T.



Protocollo RSA: la chiave pubblica è un numero N molto grande. Per decodificare il messaggio bisogna conoscere i fattori primi di N.

Protocollo RSA

- Sceglie due numeri primi p e q;
- Calcola $N = pq$ e $\varphi(N) = (p - 1)(q - 1)$;
- Sceglie intero $E < \varphi(N)$ e $(E, \varphi(N)) = 1$;
- Calcola d tale che $d \times E \equiv 1 \bmod(\varphi(N))$;
- Rende pubblica la chiave (E, N);

Cifratura e Decifratura

Per inviare m, si invia $c \equiv m^E \bmod(N)$;

Per decifrare c : $m \equiv c^d \bmod(N)$

Esempio

$p = 5 \quad e \quad q = 11$

$N = 55 \quad e \quad \varphi(N) = 40$

$E = 7$ e $23 \times 7 \equiv 1 \mod(40)$

Chiave pubblica (7, 55)

Per spedire m, si spedisce $c \equiv m^7 \mod(55)$

Per decifrare c, $m \equiv c^{23} \mod(55)$

Applicazioni

- Identificazione: un sistema di elaborazione isolato o inserito in una rete deve essere in grado di accertare l'identità di un utente che accede ai suoi servizi. (E-mail)
- Autenticazione: il destinatario di un messaggio deve poter accertare l'identità del mittente e l'integrità del crittogramma.
- Firma digitale: risulta necessaria se mittente e distinatario non si devono fidare l'uno dell'altro.

Unità	Modalità di lavoro	tempi
Storia della crittografia	Seminario comune	1 ora
I Cifrari Storici e Crittoanalisi statistica	Seminario comune	1 ora
Crittografia a chiave pubblica: cifrario RSA	Seminario comune	1 ora
Identificazione, autenticazione e firma digitale	Seminario comune	1 ora
Approfondimento	Lezione ed esercitaz.	4 ore
Preparazione dei materiali	Lavoro di gruppo	18 ore
Presentazione dei materiali e conclusioni	Dibattito	2 ore