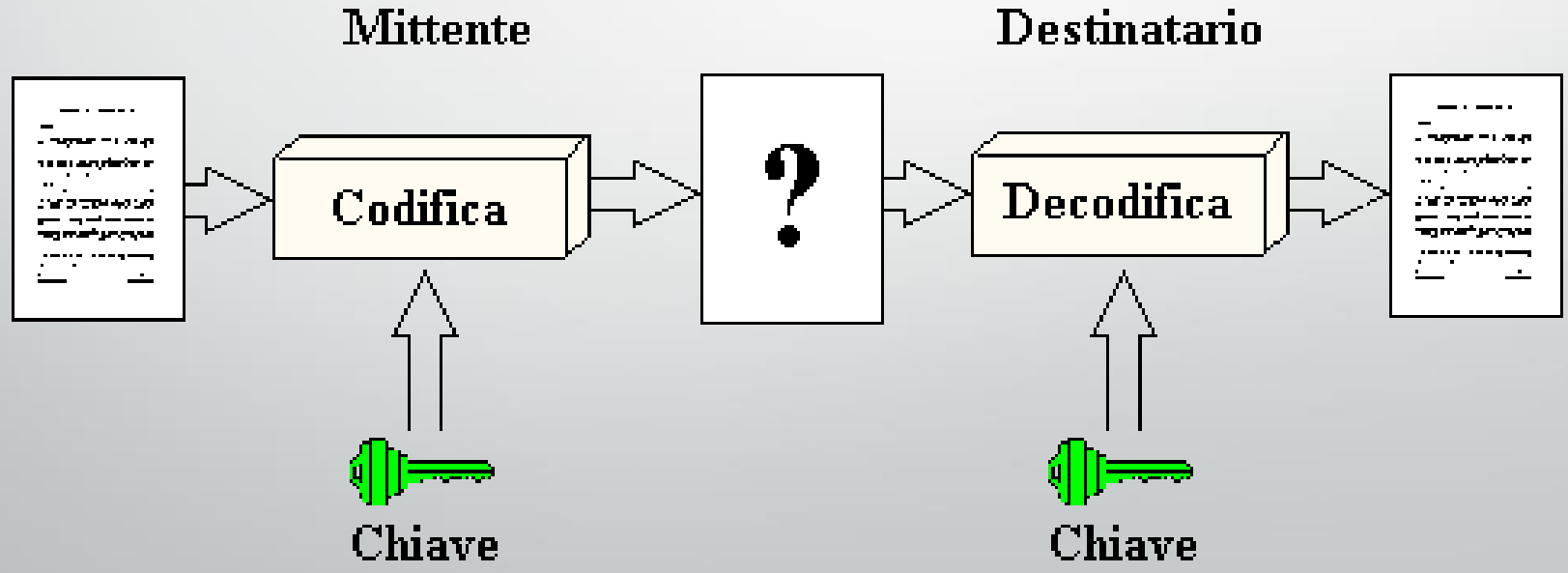
CENNI SULLA CRITTOGRAFIA

MODULO 7

CRITTOGRAFIA

- Il termine crittografia deriva dal greco (cryptòs + gràphein) ovvero scrittura nascosta
- Descrive la disciplina che tratta i metodi necessari per rendere un messaggio comprensibile solo alle persone autorizzate
- È una tecnica molto antica: circa quinto secolo a. C.



CRITTOGRAFIA

SCITALA SPARTANA: (V sec a.C.)

- Consiste in un bastone di lunghezza e larghezza noti nel quale si avvolge un nastro di cuoio.
- Sul nastro si scrive il messaggio, lettera per lettera su colonne parallele.
- Si elimina il bastone (che rappresenta la chiave segreta)

CRITTOGRAFIA

SCACCHIERA DI POLIBIO: (III sec a.C.)

- Ad ogni lettera dell'alfabeto si associa una coppia di numeri
- Si modifica il messaggio originale sostituendo le lettere coi numeri

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K/Q	L	M	N	O
4	P	R	S	T	U
5	W	V	X	Y	Z

ESEMPIO								
TESTO IN CHIARO	S	P	E	C	C	H	I	O
TESTO CIFRATO	43	41	15	13	13	23	24	35

CRITTOGRAFIA

TELEGRAFO OTTICO DI POLIBIO:

- Si usano 10 fiaccole (5 a sinistra ed 5 a destra).
- Si alza un numero di torce a sinistra corrispondente al numero di riga e un numero di torce a destra corrispondente al numero di colonna, individuando così una lettera precisa.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K/Q	L	M	N	O
4	P	R	S	T	U
5	W	V	X	Y	Z

CRITTOGRAFIA

CIFRARIO ATBASH: (IV sec a.C.)

- Ideato dal popolo ebraico: usato nella Bibbia, nel libro di Geremia, per cifrare il nome della città di Babilonia
- Le lettere dell'alfabeto sono capovolte:

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

ESEMPIO								
TESTO IN CHIARO	S	P	E	C	C	H	I	O
TESTO CIFRATO	H	K	V	X	X	S	R	L

CRITTOGRAFIA

CIFRARIO DI CESARE: (I sec a.C.)

- Giulio Cesare usava per le sue corrispondenze riservate un algoritmo crittografico molto semplice: ogni lettera chiara è sostituita dalla lettera che la segue di "D" posti nell'alfabeto

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
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

D=5

ESEMPIO								
TESTO IN CHIARO	S	P	E	C	C	H	I	O
TESTO CIFRATO	X	U	J	H	H	M	N	T

CRITTOGRAFIA

CIFRARIO DI CESARE: (I sec a.C.)

- Giulio Cesare usava per le sue corrispondenze riservate un algoritmo crittografico molto semplice: ogni lettera chiara è sostituita dalla lettera che la segue di “D” posti nell'alfabeto

- Il codice è poco sicuro: esistono solo 26 possibili combinazioni per cifrare lo stesso messaggio: con un attacco a forza bruta si

CRITTOGRAFIA

CIFRARIO A SOSTITUZIONE MONOALFABETICA:

- Consiste nel sostituire ogni lettera con un'altra in maniera del tutto casuale.
- Le possibili combinazioni sono: 26! (fattoriale), cioè circa 4*10^26
- La chiave segreta consiste nella tabella sottostante

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
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

ESEMPIO								
TESTO IN CHIARO	S	P	E	C	C	H	I	O
TESTO CIFRATO	L	H	Y	E	E	I	O	G

CRITTOGRAFIA

CIFRARIO DI VIGENERE (1586):

- Consiste nell'utilizzare il cifrario di Cesare, ma lo spostamento D non è costante, ma varia periodicamente

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Si definisce una parola chiave: ex. VISTA

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

ESEMPIO								
TESTO IN CHIARO	S	P	E	C	C	H	I	O
PAROLA CHIAVE	V	I	S	T	A	V	I	S
TESTO CIFRATO	O	Y	X	W	D	D	R	H

CRITTOGRAFIA

CRITTOGRAFIA MODERNA

- La chiave è il segreto tra il mittente e il destinatario
- Nel 1976 Diffie, Hellman e Merke idearono la crittografia asimmetrica:
- Un anno dopo, Rivest, Shamir e Adleman crearono il protocollo RSA:
  - Chiave privata: mantenuta segreta
  - Chiave pubblica: può essere divulgata

- Durante la fase crittografica si utilizza la chiave pubblica del destinatario
- Durante la fase decrittografica il destinatario usa la propria chiave privata