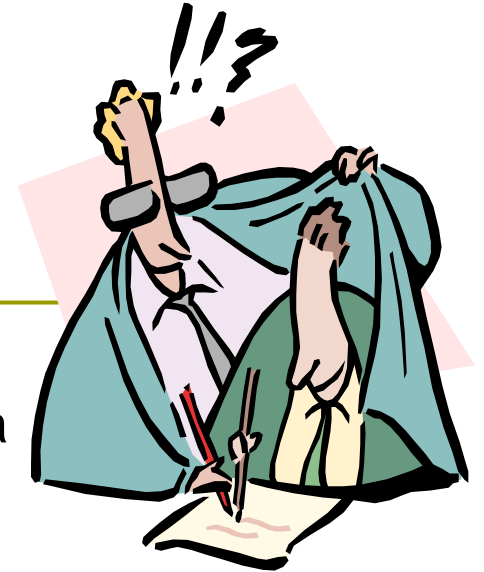




Breve storia della crittografia

CORSO SPECIALE ABILITANTE classe A042
Storia dell'Informatica e del Calcolo Automatico
Allieva: prof.ssa Mundo Gabriella

-
- La crittografia (dal greco Kryptòs, che significa "nascosto" e gràphein che significa "scrittura") è la scienza che si occupa dello studio delle scritture "segrete".
 - E' nata come branca della matematica e dell'informatica grazie all'utilizzo di tecniche di teoria dei numeri e di teoria dell'informazione.
 - E' entrata a far parte della nostra vita quotidiana per la protezione delle informazioni digitali, dalle smart card, ai cellulari, alle trasmissioni via Internet, alle tv satellitari, etc.



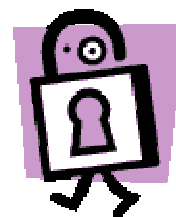
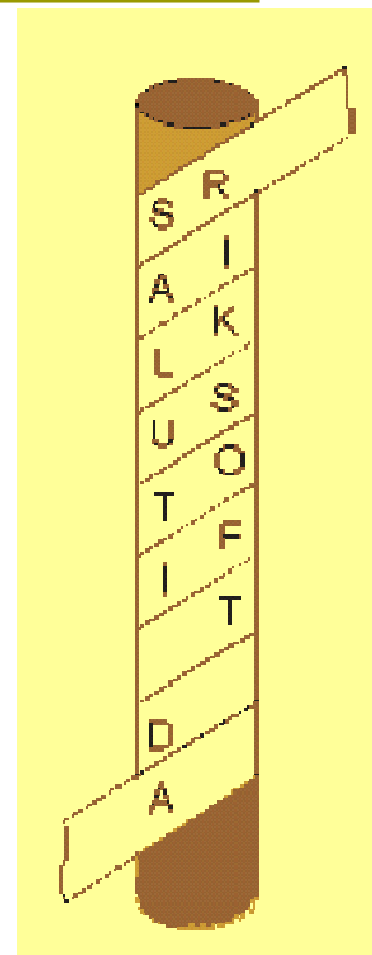
Le più antiche scritture cifrate

- ❑ La storia della crittografia è antica quasi quanto la scrittura stessa.
- ❑ Nella città di Menet Khufu (Nilo), sono state rilevate manomissioni volontarie in un testo ritrovato nella Tomba del faraone Knumotete II datato intorno al 1900 A.C.
- ❑ Anche nelle scritture cuneiformi sviluppate in Mesopotamia sono stati ritrovati esempi di crittografia.
- ❑ Sia presso gli Assiri sia presso i Babilonesi, le due grosse civiltà sorte sulle sponde del Tigri, è stata rinvenuta l'usanza di sostituire le parti terminali delle parole con elementi corti e stereotipati detti colofoni.
- ❑ In Iraq, nel periodo finale delle scritture cuneiformi, è presente per la prima volta la sostituzione di nomi con numeri.



La sciat ala lacedemonica (400 a.C.)

- ❑ Plutarco descrive la scitola lacedemonica come un codice di cifratura in uso dai tempi di Licurgo (IX sec a.C.), circa tremila anni fa. Si trattava di un dispositivo di cifratura costituito da un bastone e da un nastro di cuoio avvolto a spirale cilindrica, su cui il messaggio veniva scritto per colonne.
- ❑ Sul nastro srotolato le lettere risultavano trasposte in modo tale che solo l'adozione di un bastone identico a quello originariamente usato per la scrittura del messaggio consentiva di ricomporre il testo.





L'ATBASH ebraico

- ❑ E' una tecnica di trasformazione ad alfabeto capovolto:
- ❑ Il primo carattere dell'alfabeto viene sostituito con l'ultimo, il secondo con il penultimo e così via.

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

Quindi il messaggio "Corso Abilitante" diviene :

Messaggio:	C	O	R	S	O	A	B	I	L	I	T	A	N	T	E	
TestoCifrato	X	L	I	H	L	Z	Y	R	O	R	G	Z	M	G	V	



Scacchiera di Polibio (200-118 a.C.)

- Lo storico greco Polibio nelle sue Storie (Libro X) descrive un interessante metodo di cifratura. L'idea è quella di cifrare una lettera con una coppia di numeri compresi tra 1 e 5, in base ad una matrice 5x5, contenente le lettere dell'alfabeto. Ogni lettera viene rappresentata da due numeri, guardando la riga e la colonna in cui essa si trova.
- Ogni lettera può venire quindi rappresentata da due numeri guardando la riga e la colonna in cui la lettera si trova.

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

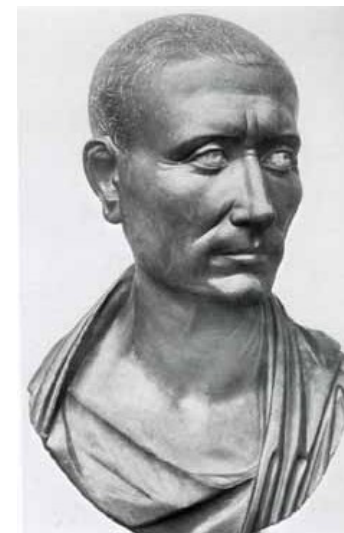
testo in chiaro: C o r S o

testo cifrato: (1,3) (3,5) (4,2) (4,3)(3,5)



Il cifrario di Cesare

Svetonio nella Vita dei dodici Cesari racconta che Giulio Cesare usava per le sue corrispondenze riservate un codice di sostituzione molto semplice, nel quale la lettera chiara veniva sostituita dalla lettera che la segue di tre posti nell'alfabeto: la lettera A è sostituita dalla D, la B dalla E e così via fino alle ultime lettere che sono cifrate con le prime.



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
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

TESTO	C	O	R	S	O	A	B	I	L	I	T	A	N	T	E
CIFRATURA	F	R	U	V	R	D	E	L	O	L	W	D	Q	W	H



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

Il cifrario di Augusto (100-44 a.C.)

Nel cifrario di Augusto viene utilizzata un testo chiave che viene sommato al testo da cifrare mediante la somma delle distanze da inizio alfabeto.

Riportiamo per semplicità la tabella delle corrispondenze tra lettere e posizione dell'alfabeto (riquadro in alto) e facciamo un esempio.



CHIAVE	C	O	R	S	O	A	B	I	L	I	T	A	N	T	E
	3	15	18	19	15	1	2	9	12	9	20	1	14	20	5

TESTO	I	N	F	O	R	M	A	T	I	C	A
	9	14	6	15	18	13	1	20	9	3	1

TESTO	12	29	24	34	33	14	3	29	21	12	21				
CIFRATO	L	C	X	H	G	N	C	C	U	L	U				



Gabriele Lavinde (1378)

Il nomenclatore di **Gabriele Lavinde**, sfrutta una lista di codici, un alfabeto di sostituzione, ed una lista di parole nulle.

La lista di parole nulle viene usata come disturbo per la crittoanalisi ed è composta da parole che devono semplicemente essere scartate dal destinatario che si appresta alla decifrazione.

CODICE

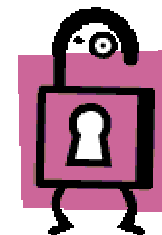
Laboratorio = Mare

Portare = Cavallo

Progetto = Dondolo

Segreto = Vento

un messaggio tipo: "Portare il progetto segreto al Laboratorio", sarebbe trasformato come "Cavallo il dondolo vento al mare".





Leon Battista Alberti (1466)

L. B. Alberti si servì di 2 dischi di rame, uno più piccolo dell'altro, collegati al centro e liberi di ruotare indipendentemente. Il disco esterno era costituito da 24 caselle contenenti 20 lettere latine (escluse H, K, W e Y, con U=V I=J) ed erano invece aggiunte le cifre 1, 2, 3 e 4.

Sul disco interno erano invece presenti tutte le lettere dell'alfabeto più "et", in ordine casuale.

Mittente e destinatario avevano entrambi la stessa macchinetta. Entrambi concordavano una lettera che sarebbe stata la chiave di partenza.

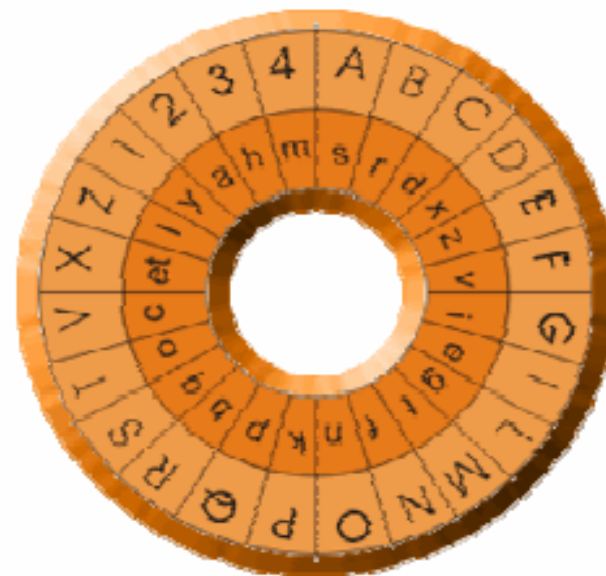
Esempio

chiave : C

testo : CIAO

Testo cifrato: DDESN

Disco di Leon Battista Alberti



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
0	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

Il cifrario di Vigenere (1608)

Il testo cifrato si ottiene spostando la lettera chiara di un numero fisso di caratteri, pari al numero ordinale della lettera corrispondente della chiave. Di fatto si esegue una somma aritmetica tra l'ordinale del chiaro (A = 0, B = 1, C = 2 ...) e quello della chiave; se si supera l'ultima lettera, la Z, si ricomincia dalla A, secondo la logica delle aritmetiche finite. Per facilitare tale operazione si utilizza la seguente tavola

ABCDEFGHI JKLMNOPQRSTU**V**WXYZ
 BCDEFGHI JKLMNOPQRSTUVWXY**Z**A

 DEFGHI JKLMNOPQRSTUVWXY**Z**ABC

 IJKLMNOPQRSTUVWXY**Z**ABCDEF**G**H
 VWXYZABCDEF**G**H IJKLMNO**P**QRSTU

Chiave : VDIVERS OMETOD OD ICHIAV ECONTINU
Testo in chiaro: DIVERSO METODO DI CHIAVE CONTINUA
Testo cifrato : YLDZVJG AQXHRR RL KJPI VZ GQBGBVHU



Il codice di Jefferson (1801-1804)

Si tratta del primo metodo di cifratura basato su cilindri e dischi ruotanti intorno ad un asse. Il dispositivo di Jefferson era composto da un cilindro di circa 15 cm di lunghezza e 4 cm di larghezza montato su un asse.



Questo cilindro era formato dall'insieme di 36 ruote di stessa misura (25 nella versione poi utilizzata dagli Americani). Esaminando ognuna di queste ruote, si poteva notare come avessero sull'esterno, tutte le 26 lettere dell'alfabeto, ma in ordine casuale e accuratamente diverso ognuna dalle altre. Inoltre ognuna di queste ruote aveva un numero di riconoscimento.

La cifratura di un messaggio avviene nel seguente modo: il messaggio viene prima di tutto diviso in blocchi di 36 caratteri. Per ogni blocco, i dischi vengono ruotati in modo tale da far comparire allineati su una riga i caratteri del blocco da cifrare.



Una volta effettuata tale operazione, si sceglie a caso un'altra riga, e si considera la corrispondente sequenza di 36 lettere come il messaggio cifrato. Il ricevente, che possiede un cilindro identico a quello del trasmittente, non deve far altro che ruotare i dischi in modo tale da far comparire il cifrato allineato su una riga. Compiuta questa operazione, deve analizzare le restanti righe. Una sola di queste è una frase di senso compiuto rappresentante il messaggio in chiaro.



Il cifrario di Playfair (1854)

Il sistema di cifratura prende il nome da colui che l'ha reso noto, Lyon Playfair, sebbene l'autore reale fosse stato Sir Charles Wheatstone (1802-1875). Il Playfair cipher viene riconosciuto come primo metodo di cifratura a bigrammi (coppie di caratteri).

Il metodo consiste nel posizionare dentro la tabella di 5x5 caselle, una parola chiave (nel nostro caso NAPOLI) seguendo l'ordine sinistra-destra ed alto basso, completando la matrice con le lettere dell'alfabeto nel loro ordine naturale, previa fusione di i e j e stando attenti a non ripetere le lettere già usate nella parola chiave inserita.



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

- Si dividono le parole in bigrammi.
- Si prendono le due che costituiscono un rettangolo con le due lettere del bigramma, cominciando da quella che si trova in linea con la prima lettera del bigramma del testo da cifrare;
- Qualora il bigramma del testo da cifrare presenti due lettere uguali si cercherà di eliminare questo raddoppio, oppure di romperlo inserendo una lettera rara (k, w, x, y).

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

testo in chiaro: SA LU TI
testo cifrato: RP EZ QD



Il cifrario di Delastelle (XIX sec.)

1. Innanzitutto viene trascritta la chiave dentro la tabella, eliminando le lettere doppie. Le restanti celle contengono i caratteri dell'alfabeto nel loro ordine naturale. Non viene introdotta la W per mancanza di spazio. La W sarà sostituita cifrando due V consecutive.

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

2. Il testo da cifrare viene spezzato in parole di 5 caratteri l'una. Qualora non vi siano lettere sufficienti per formare l'ultimo blocco, i posti mancanti saranno riempiti con delle X

Testo : IL CORSO ABILITANTE
ILCOR SOABI LITAN TEXXX

3. Ogni carattere del testo in chiaro viene cifrato usando la scacchiera, ovvero, si prendono in corrispondenza del carattere da cifrare, il numero di riga e colonna e si riportano in verticale sotto il testo in chiaro.

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

ILCOR SOABI LITAN TEXXX
21214 41122 12411 42555
15343 44221 51521 55333

4. I blocchi di numeri, vengono ora trascritti in orizzontale, leggendoli da sinistra a destra e dall'alto in basso, per ogni singolo blocco. Durante questa trascrizione i numeri vengono scritte a coppie.

21 21 41 53 43 41 12 24 42 21
 12 41 15 15 21 42 55 55 53 33

5. Si passa quindi a ritrasformare in lettere la riga di coppie di numeri appena formata, sfruttando di nuovo la scacchiera.

TESTO CIFRATO:

IIMXRMADQIAMLLIQZZXH



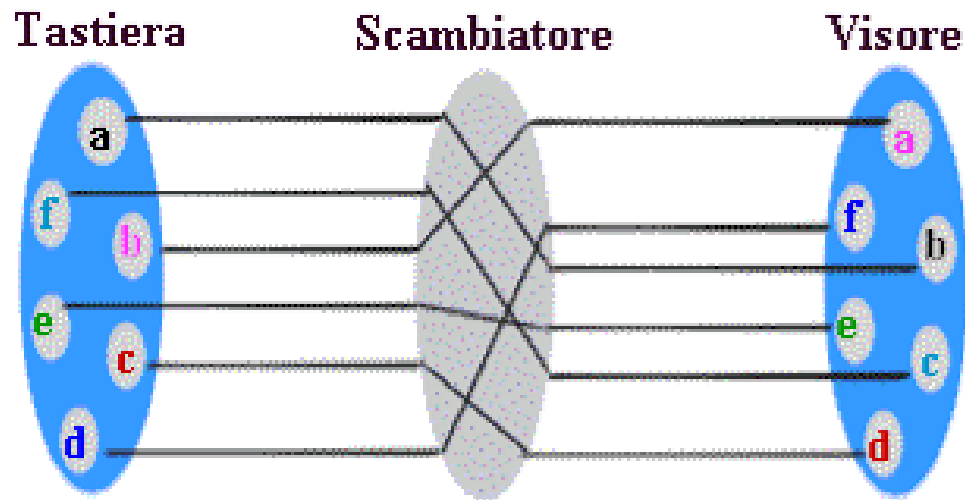
Enigma (1918)

- Nella prima metà del XX secolo cominciarono a diffondersi macchine cifranti a rotori. La più celebre di queste macchine è l'Enigma inventata nel 1918 e adottata dall'esercito e dalla marina tedesca fino alla seconda guerra mondiale.
- La macchina era stata inventata da un ingegnere polacco e non è chiaro come sia potuta finire in mano ai tedeschi.
- Ma resta il fatto che a causa della casualità delle chiavi utilizzate, gli inglesi hanno grossi problemi a decifrare i messaggi intercettati.
In una macchina Enigma utilizzata in quel tempo il numero di combinazioni di chiavi per forzare il cifrario era di:

16.900 x 6 x 100.391.791.500



La versione semplificata del congegno consiste in 3 componenti collegati da fili elettrici: una tastiera per immettere le lettere del testo in chiaro; un'unità scambiatrice che cifra la lettera trasformandola nel corrispondente elemento del crittogramma (testo cifrato); un visore con varie lampadine, che accendendosi indicano la lettera da inserire nel testo cifrato.



Versione semplificata di Enigma con un alfabeto di 6 lettere



Il cifrario perfetto di Vernam (1926)


Questo sistema è in assoluto il più sicuro che esista, tanto che è stato utilizzato per cifrare le comunicazioni tra i presidenti USA-URSS durante la guerra fredda (il famoso telefono rosso).

Il padre della Teoria dell'Informazione, Claude Shannon, ha dimostrato nel 1949 che:

**OGNI CIFRARIO TEORICAMENTE
SICURO E' UN CIFRARIO DI
VERNAM**



Gilbert Vernam



Il suo funzionamento è simile a quello realizzato dall'imperatore Augusto (cifrario monoalfabetico), con la differenza che la chiave di cifratura deve essere una sequenza casuale di caratteri ed avere una lunghezza pari o superiore al testo in chiaro da cifrare infatti la chiave generata è lunga come il testo (chiave a lunghezza infinita) ed è del tutto casuale e dunque imprevedibile;

Il testo in chiaro e la chiave vengono sommati proprio come nel cifrario di Vigenere, l'unica differenza sta nel fatto che si sommano non tanto gli ordinali delle lettere da cifrare ma i singoli bit che codificano la lettera nei codici usati nelle telecomunicazioni (allora codice Baudot oggi codice ASCII).

Il cifrario di Vernam utilizza il codice Baudot e l'operatore XOR, che è simile all'addizione ed è reversibile.

0	0			24	11000	A	-
19	10011	B	?	14	1110	C	:
18	10010	D	\$	16	10000	E	3
22	10110	F	!	11	1011	G	&
5	101	H	#	12	1100	I	8
26	11010	J	'	30	11110	K	(
9	1001	L)	7	111	M	.
6	110	N	,	3	11	O	9
13	1101	P	0	29	11101	Q	1
10	1010	R	4	20	10100	S	{bel}
1	1	T	5	28	11100	U	7
15	1111	V	;	25	11001	W	2
23	10111	X	/	21	10101	Y	6
17	10001	Z	"	27	11011	{cifr}	{cifr}
2	10	{cr}	{cr}	31	11111	{lett}	{lett}
8	1000	{lf}	{lf}	4	100	{sp}	{sp}

Codice Baudot

Facciamo un esempio:

Testo in chiaro

A	T	T	E	N	Z	I	O	N	E
11000	00001	00001	10000	00110	10001	01100	00011	00110	10000

Chiave

W	I	A	P	F	I	L	K	M	S
11001	01100	11000	01101	10110	01100	01001	11110	00111	10100

Testo cifrato

00001	01101	11001	11101	10000	11101	00101	11101	00001	00100
T	P	W	Q	E	Q	H	Q	T	Sp

XOR ha il vantaggio di essere reversibile quindi verrà usata anche per decifrare.



La macchina di Lorenz (1926-1939)

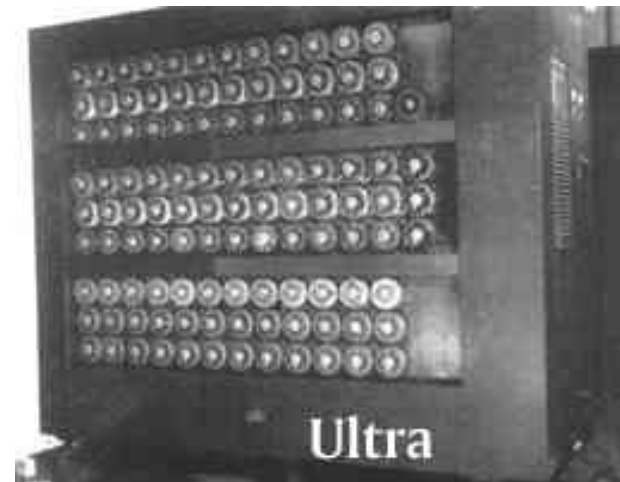
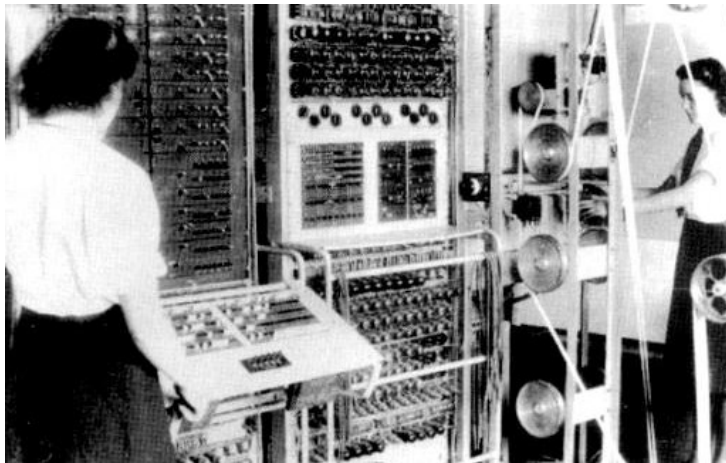
Durante la II guerra mondiale, i tedeschi usarono anche altri cifrari; in particolare gli alti comandi tedeschi usarono una macchina telescrivente realizzata dalla ditta Lorenz che a differenza dell' Enigma usava 32 caratteri codificati con il codice Baudot. La cifratura Lorenz si ispirava direttamente al cifrario di Vernam secondo cui la chiave dovrebbe essere indefinitamente lunga ma sostituì la chiave casuale con una chiave pseudo-casuale generata da un dispositivo meccanico di 12 rotori.



MACCHINA DI LORENZ

Fu proprio la componente non casuale a far sì che la macchina Lorenz fosse forzata dai crittoanalisti inglesi del progetto Ultra, (grazie anche a una grossa ingenuità di un cifratore tedesco).

Per decrittare più velocemente i cifrati Lorenz, nel 1943 nacquero i Colossi ricordati non tanto perchè possedevano un'elevata velocità, ma perchè erano macchine programmabili.





DH (cif rario asimmet r ico) (1976)

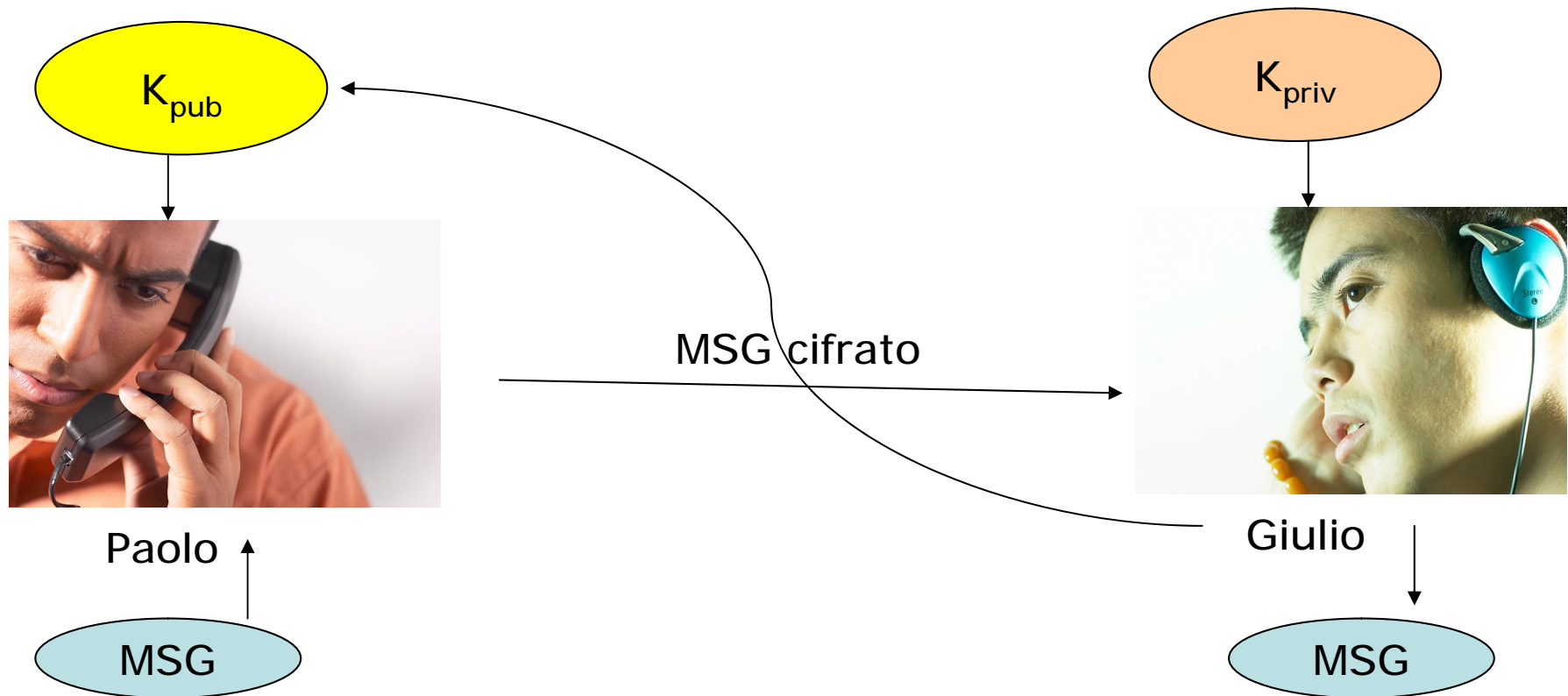
Nel 1976, gli americani Whitfield Diffie e Martin Hellman danno vita ad una nuova generazione di sistemi crittografici: sistemi asimmetrici detti a chiave pubblica e chiave privata.

Il meccanismo ideato da Diffie ed Helmann superava d'un tratto l'intero problema di distribuzione delle chiavi: non era più necessario comunicare nella massima segretezza la chiave prima di poter effettuare una comunicazione sicura. Con questo metodo la chiave per cifrare non è la stessa di quella per decifrare; la prima può allora essere resa pubblica mentre solo la seconda resta segreta.

La sicurezza di questi sistemi si fonda quasi sempre su funzioni relativamente facili da calcolare ma molto difficili da invertire (problemi ardui).

Paolo ha la necessità di mandare a Giulio un messaggio segretissimo tramite un canale non sicuro (ad esempio telefono) :

1. Giulio genera due chiavi: una pubblica (K_{pub} che serve per cifrare) ed una privata (K_{priv} che serve per decifrare)
2. Giulio manda a Paolo solo la sua chiave pubblica (la può dire al telefono, spedire via email, la può pubblicare in internet)
3. Paolo codifica il messaggio da inviare usando la K_{pub} e spedisce il messaggio così ottenuto a Giulio
4. Giulio una volta ricevuto il messaggio da Paolo lo decifra usando la sua chiave privata K_{priv}



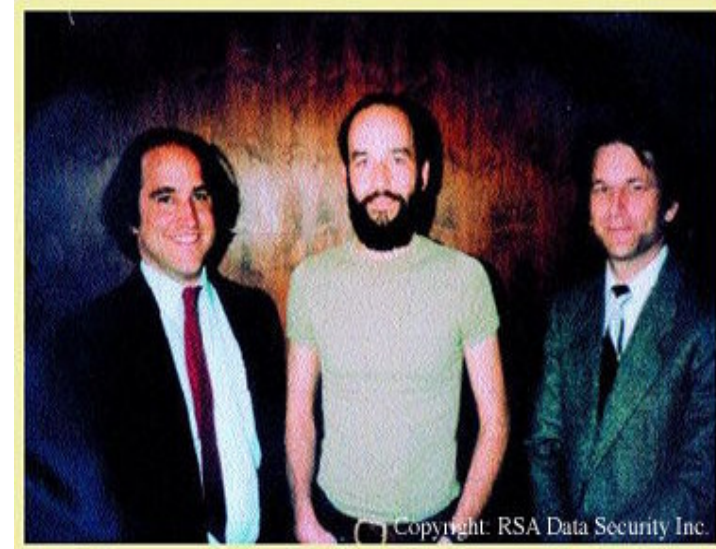


Il cifrario RSA (1977)

Nel 1977, R. Rivest, A. Shamir, L. Adleman, pubblicarono l'articolo "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", nel quale indicavano funzioni matematiche atte ad implementare lo schema concettuale di Diffie ed Hellman. L'algoritmo battezzato con le iniziali dei loro cognomi, RSA, è ancora oggi l'algoritmo a chiave pubblica più diffuso.

L'idea alla base del RSA è quella di sfruttare la **complessità computazionale del calcolo della fattorizzazione un numero.**

Cioè trovare il prodotto di due numeri primi molto grandi è facilissimo, ma dato il prodotto sarà estremamente difficoltoso trovarne i 2 fattori primi



La scelta delle chiavi



- ❑ Scegli due numeri primi grandi p, q .
- ❑ Calcola $n = pq$, $z = (p-1)(q-1)$
- ❑ Scegli e minore di n , dispari e primo con $(p-1)(q-1)$.
- ❑ scegli d tale che $(ed-1)$ sia esattamente divisibile per z .
- ❑ La Chiave Pubblica è (n,e) , quella Privata è (n,d) .



II DES (1977)

- 5 maggio 1973: 15 Maggio 1973, il National Bureau of Standards (NBS) pubblicò un invito, nel Registro Federale, per l'emissione di un crittosistema standard
⇒ nasce DES — Data Encryption Standard, che è divenuto il crittosistema più usato nel mondo
- 1975: DES fu sviluppato alla IBM come evoluzione di un crittosistema più antico, LUCIFER, e fu pubblicato sul Registro Federale il 17 Marzo 1975
- 15 gennaio 1977: La definizione di DES è riportata nel Federal Information Processing Standards Publication 46 del 15 Gennaio 1977
- 1983, 1987, 1992: Riaffermato per successivi 5 anni
- giugno 1997, luglio 1998, gennaio 1999 DES challenges
- 2000 Advanced Encryption Standard (AES)



Crittografia recente

- **1989-RC2:** di derivazione DES, si differenzia da questo per la particolarità di poter variare la lunghezza della chiave.

Si è diffuso essenzialmente grazie al fatto che il governo USA ne ha permesso l'esportazione sebbene limitando la lunghezza massima della chiave a soli 40 bit. Questa limitazione lo rende praticamente inefficace per la protezione di informazioni importanti: i tentativi di brute-force per la ricerca della possibile chiave scendono dal massimo di 72 milioni di miliardi del DES ad un massimo di soli 1000 miliardi rendendo possibile la decrittazione, con una modica spesa in hardware, a poche ore di attesa (parliamo sempre di hardware noti!).

- **1991-IDEA:** è stato proposto quando si è intuito che il sistema DES non avrebbe resistito per molto agli attacchi degli analisti. IDEA (**International Data Encryption Algorithm**) è nato nel 1991 sotto il nome di IPES (Improved Proposed Encryption Standard), ed è stato progettato da due famosi ricercatori in Svizzera: **Xuejia Lai e James L. Massey**. Come il DES è un codice cifrato a blocchi di 64 bit, la differenza sta nel fatto che questa volta però la chiave è di 128 bit e questo dovrebbe impedire di trovare la chiave procedendo per tentativi poiché le chiavi possibili sono infatti 2^{128} .



Crittografia recente

- **1993-BlowFish:** Questo algoritmo utilizza varie tecniche tra le quali la rete Feistel, le S-box dipendenti da chiavi e funzioni F non invertibili che lo rendono, forse, l'algoritmo più sicuro attualmente disponibile.

Le chiavi utilizzate sono di dimensioni variabili fino ad un max. di 448 bit e i blocchi utilizzati per la cifratura sono di 64 bit.

Non si conoscono al momento tecniche di attacco valide nei suoi confronti. E' considerato uno degli algoritmi di cifratura a blocchi più veloce (risulta più veloce del DES e dell'IDEA).

- **1994-RC5:** Proprietà della RSA Data Security Inc., basato su DES ed evoluzione di RC2.

Si differenzia dall' RC2 per la notevole flessibilità operativa.



Crittografia recente

- **1997-CAST:** L'algoritmo CAST, progettato da **Carlisle Adams** e **Stafford Taveres**, è ottimo e molto stabile. E' molto simile al Blowfish come struttura poiché utilizza più o meno le stesse tecniche crittografiche (con l'eccezione della rete Feistel rimpiazzata da un sistema chiamato di "permutazioni-sostituzioni").

David Wagner, John Kelsey e Bruce Schneier hanno scoperto un attacco sulle chiavi a 64 bit del CAST mediante 2^{17} testi cifrati, con 2^{48} computazioni dell'algoritmo. Naturalmente l'attacco non è efficace al 100 per cento. L'algoritmo CAST è registrato dalla **Entrust Technologies**, che lo ha rilasciato per un uso libero e gratuito.

- **2000-AES:** Il 2 ottobre del 2000 il **NIST (National Institute of Standard and Technology** - Istituto Nazionale degli Standard e delle Tecnologie) ha annunciato la scelta di adottare un nuovo standard di cifratura tra 15 possibili candidati. Questo nuovo standard nasce con lo scopo di sostituire il desueto DES la cui dimensione delle chiavi di cifratura inizia ad essere troppo piccola.

Rijndael - lo strano nome nasce dall'unione dei nomi dei suoi inventori, ovvero Rijmen e Daemen - è stato scelto come il futuro AES ed è diventato lo standard per la cifratura del XXI secolo.

Fino al Novembre 2002 non sono stati riscontrati punti deboli.

Fonti In Rete

<http://www.liceofoscarini.it/studenti/crittografia/index.html>

<http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/crittografiaclassica/>

www.riksoft.com

<http://telemat.det.unifi.it/book/1997/cryptography/>

<http://www.liceofoscarini.it/studenti/crittografia/critto/>

www.sancese.com

This document was created with Win2PDF available at <http://www.win2pdf.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.