ISTITUTO SCOLASTICO “FARINA” - SCUOLA SUPERIORE

APPUNTI DEL CORSO DI

“SISTEMI DI ELABORAZIONE E TRASMISSIONE DATI”

PROF. ENRICO FABRIS

LA CRITTOGRAFIA

1. Introduzione

Crittografia vuol dire scrittura segreta. L'arte di scrivere messaggi segreti che possano essere letti e compresi solo dal destinatario risale alla più remota antichità, anche se già la Bibbia parla di un codice segreto per scrivere il nome di Babele (il codice Atbash).
Per secoli quest'arte è stata appannaggio quasi esclusivo dei militari e dei diplomatici, e i metodi crittografici erano specifici per l'invio di messaggi materiali affidati a corrieri.
Nel XX secolo però prima l'invenzione della radio, poi quella del computer hanno cambiato in modo radicale lo scenario. La necessità di comunicare informazioni in modo riservato si è ampliata notevolmente. Oggi l'utente del Bancomat, di una pay-tv e chi effettua acquisti su Internet con la carta di credito fa uso, spesso senza rendersene conto, di tecniche crittografiche.
Sempre nel XX secolo sono nate nuove tecniche di cifratura, prima macchine cifranti come la celebre macchina Enigma usata dai tedeschi nella II guerra mondiale, poi con l' avvento dei computer che ha di colpo resi inaffidabili e superati quasi tutti i metodi classici, metodi specifici per l'uso informatico come il DES della IBM e il rivoluzionario RSA capostipite dei cifrari a chiave pubblica.
Come detto l'esigenza di garantire la riservatezza dell'informazione non è un aspetto recente nella vita dell'uomo, ma ha caratterizzato la sua storia fin dai tempi greci. I segreti fanno parte della vita umana, così come nascondere le informazioni ed i messaggi in modo che solo il vero
destinatario può accedervi.
Per secoli la crittografia è stata un’arte usata quasi esclusivamente per fini diplomatici e soprattutto militari.
Il bisogno di segretezza ha indotto le nazioni a creare veri dipartimenti di crittografia infatti migliorando i sistemi di crittografici si garantiva la sicurezza di comunicazioni.
La storia della crittologia è la storia dell’antica battaglia intellettuale tra inventori e solutori di codici che hanno lasciato un’impronta profonda nello sviluppo della storia.
Un argomento di cui si tratterà è l’utilizzo di macchine meccaniche strategiche come la famosa Enigma. Questa macchina fu usata dai tedeschi durante la II seconda guerra mondiale. Gli inglesi riuscirono a forzare i messaggi cifrati e, tenendone segreto il successo, poterono continuare a leggere i messaggi del nemico. Per poter forzare i cifrari tedeschi , gli inglesi inventarono varie apparecchiature elettroniche, la più famosa delle quali è il Colossus, il primo computer digitale.

I cifrari storici ci fanno capire come la crittografia si sia sviluppata nel tempo e come siano stati definiti alcuni comuni principi di base anche se, per noi, ora, non hanno più rilevanza pratica con l'avvento dei calcolatori.

Dalla lettura di queste pagine risulterà evidente che la visione da guerra fredda della crittografia è ormai obsoleta, la crittografia non è più solo un arma a disposizione di pochi 007 e potenze militari: con il diffondersi del computer in modo esponenziale in tantissimi i campi ha fatto nascere nuovi bisogni di crittografare lontano dalle sue origini militari, il suo scopo principale è quello di tutelare la propria privacy. Senza saperlo la maggior parte di noi, utilizza quotidianamente la crittografia: pagare con il bancomat o fare una chiamata con un cellulare GSM, guardare la pay tv, inserire semplicemente la password d'accesso in un computer e molte altre operazioni apparentemente normalissime.

Oggi con la grande diffusione della comunicazione elettronica la crittografia è diventata una disciplina molto complessa.

Si potrà parlare così di problemi di protezione delle comunicazioni che nascono dall'impiego delle reti e del sistema crittografico usato su internet (secure socket layer detto SSL) o di smart card elettroniche che potranno avere sempre più sofisticate funzionalità all'interno di esse. Saranno trattati i vari algoritmi che permettono di cifrare i messaggi, si parlerà della firma digitale la quale attraverso speciali tecniche crittografiche rende possibile garantire l'originalità e l'integrità del messaggio.

Gli studi crittografici di oggi costituiscono l'inizio di un lungo viaggio verso applicazioni future sempre più complesse, utili e imprevedibili.

2. Storia della crittografia

2.1. Il cifrario Atbash

Il libro di Geremia nella Bibbia usa un semplicissimo codice monoalfabetico per cifrare la parola Babele; la prima lettera dell'alfabeto ebraico (Aleph) viene cifrata con l'ultima (Taw), la seconda (Beth) viene cifrata con la penultima (Shin) e così via; da queste quattro lettere è derivato il nome di Atbash (A con T, B con SH) per questo codice.
Usando il moderno alfabeto internazionale, l'Atbash può essere riassunto con la seguente tabella di cifratura:

```
CHIARO      a b c d e f g h i j k l m
CIFRATO     Z Y X W V U T S R Q P O N
CHIARO      n o p q r s t u v w x y z
CIFRATO     M L K J I H G F E D C B A
```

Utilizzando la frase *"Il sole brilla"* come frase chiara da cifrare il risultato sarà:

Rohlovyirooz

Il codice Atbash è quindi simile ma meno complesso di quello di Cesare, poiché al contrario di quest'ultimo prevede solo una possibile sostituzione.

2.2. La scacchiera di Polibio

Lo storico greco Polibio (~200-118AC), nelle sue Storie (Libro X) descrive il più antico esempio di codice poligrafico, che attribuisce ai suoi contemporanei Cleoxeno e Democleito; l'idea è quella di cifrare una lettera con una coppia di numeri compresi tra 1 e 5, in base ad una scacchiera 5x5. In tal modo il messaggio può essere trasmesso con due gruppi di cinque torce (p.es. 1,5 = una torcia accesa a destra, cinque a sinistra). In effetti più che di un codice segreto, si tratta di un sistema di telecomunicazione, di fatto un telegrafo ottico. Telegrafi a torce esistevano da molti secoli ed erano stati descritti da Enea il tattico intorno al 350AC, ma erano basati su un limitato elenco di messaggi

possibili; quello di Polibio si basa invece sulla scomposizione del messaggio nelle singole lettere ed è quindi in grado di trasmettere qualsiasi messaggio.

Nell'alfabeto greco ci sono 24 lettere ed avanza quindi un carattere che Polibio proponeva di usare come segnale di sincronizzazione (inizio e fine trasmissione). Nell'esempio seguente si utilizzerà, al posto di quello greco, l'alfabeto internazionale il quale ha viceversa il difetto di essere formato da 26 caratteri; così per poter costruire il quadrato necessario per la cifratura bisognerà "fondere" due lettere rare ma non foneticamente differenti nella stessa casella, in questo caso la k e la q. In questo modo si otterrà la tabella seguente.

#	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

Ogni lettera può viene quindi rappresentata da due numeri, guardando la riga e la colonna in cui la lettera si trova. Per esempio, a=11 e r=42. Quindi la frase “Attenzione agli scogli” dopo la cifratura risulterà:

114444153455243534151122322443133522322 4

La scacchiera di Polibio ha alcune importanti caratteristiche, e cioè la riduzione nel numero di caratteri utilizzati, la conversione in numeri e la riduzione di un simbolo in due parti che sono utilizzabili separatamente. La sua importanza nella storia della crittografia sta nell'essere alla base di altri codici di cifratura come il Playfair Cipher o il cifrario campale germanico usato nella prima guerra mondiale.

2.3. 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 come nella tabella che segue (che fa riferimento all'odierno alfabeto internazionale).

```
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
```

Prendendo come esempio la frase Auguri di buon compleanno si otterrà il seguente messaggio cifrato:

```
Chiaro          auguridibuoncompleanno
Cifrato         dxjxulglexrqfrpsohdqqr
```

Più in generale si dice codice di Cesare un codice nel quale la lettera del messaggio chiaro viene spostata di un numero fisso di posti, non necessariamente tre; un esempio è il codice che sempre secondo Svetonio era usato da Augusto, dove la A era sostituita dalla B, la B dalla C e così via.
Poiché l'alfabeto internazionale è composto da 26 caratteri sono possibili 26 codici di Cesare diversi dei quali uno (quello che comporta uno spostamento di zero posizioni) darà un cifrato uguale al messaggio chiaro iniziale.

2.4. Approfondimento: la teoria dei numeri

La teoria dei numeri è quella parte della matematica che si occupa dei numeri interi; in pratica teoria dei numeri è sinonimo di aritmetica.
Chi ha studiato aritmetica solo alle scuole elementari e medie potrebbe essere indotto a pensare che l'aritmetica sia la parte più semplice e banale della matematica. È vero il contrario: alcuni dei più formidabili problemi matematici sono appunto problemi di teoria dei numeri.
In particolare sappiamo ancora molto poco sui numeri primi. Questa che per il matematico teorico è una grossa spina, è diventata viceversa una fortuna per la crittologia: molti cifrati moderni a

cominciare da RSA si basano proprio sulla estrema complessità di alcuni problemi aritmetici: la fattorizzazione di un numero (RSA), il calcolo del logaritmo discreto e quello della radice discreta.

2.4.1. I numeri primi

In matematica l'aggettivo primo è usato in due accezioni leggermente diverse:

- ✓ numero primo [assoluto]: è un numero naturale (intero positivo) N che ha 2 e 2 soli divisori che sono ovviamente 1 ed N stesso; p.es. 2, 3, 5, 7, 11, 13 ...; il numero 1 viene quindi di norma escluso avendo un solo divisore (se stesso).
- ✓ numero primo relativamente a un altro numero: due numeri M e N si dicono primi tra di loro se hanno come unico divisore comune 1; detto in altri termini deve essere MCD(M, N) = 1. P.es. 25 in assoluto non è primo, 9 in assoluto non è primo ma 25 e 9 sono primi tra di loro avendo MCD(25, 9) = 1.

La teoria dei numeri primi nasce intorno al 300AC ad Alessandria con Euclide che negli Elementi riporta alcuni risultati fondamentali:

- ✓ Esistono infiniti numeri primi.
- ✓ Ogni numero non primo può scomporsi nel prodotto di più numeri primi e questa scomposizione è unica.

Pochi anni dopo, sempre ad Alessandria, Eratostene definisce un metodo per trovare la lista di tutti i numeri primi minori di un dato numero N. Questo metodo, noto come il crivello di Eratostene, è tuttora il più efficiente metodo per generare liste di primi.

Da allora non è che si siano fatti molti progressi nella conoscenza dei numeri primi; i risultati più importanti furono ottenuti da Eulero, circa 2000 anni dopo Euclide, con la dimostrazione del teorema di Eulero-Fermat e l'introduzione della funzione di Eulero.

Eulero diede inoltre una nuova e sorprendente dimostrazione dell'infinità dei numeri primi, dimostrazione che un secolo dopo portò Riemann a formulare quella congettura di Riemann che attende ancora oggi una dimostrazione (o una confutazione).

Negli ultimi anni la disponibilità di computer con elevate capacità di calcolo ha permesso di scoprire numeri primi sempre più grandi, ma non ha fatto fare passi avanti alla teoria!

In definitiva sappiamo ancora molto poco sui numeri primi. In particolare:

- ✓ Non si conosce una formula che permetta di generare i numeri primi, p.es. una funzione che ci permetta di calcolare il 1000º numero primo.

- ✓ La distribuzione dei numeri primi sembra a prima vista casuale; non sappiamo ancora se sia effettivamente così o se vi sia una qualche regolarità rimasta fino ad ora nascosta.
- ✓ Sono frequenti i numeri primi gemelli cioè accoppiati a distanza di 2: p.es. 17 e 19, 29 e 31; non sappiamo se la serie dei primi gemelli sia finita o infinita.
- ✓ Non si conoscono metodi veloci per stabilire se un numero è primo (test di primalità).
- ✓ Non si conoscono metodi veloci per scomporre un numero in fattori primi.

Il fatto di sapere così poco sui numeri primi si è rivelato un vantaggio per i crittologi; oggi quasi tutti i computer usano per comunicare in modo riservato il cifrario RSA basato appunto sulla difficoltà di scomporre in fattori primi numeri molto grandi (centinaia di cifre decimali).
Se un giorno un matematico dovesse scoprire un metodo per fattorizzare velocemente i numeri primi, il cifrario RSA perderebbe di colpo tutta la sua sicurezza!
Alcuni ritengono che una chiave del problema sia la congettura di Riemann; se venisse dimostrata potrebbe aprirsi la strada ad algoritmi veloci per la fattorizzazione dei numeri primi. Ma siamo appunto nel campo delle congetture.

2.4.2. Le aritmetiche finite

L'aritmetica ordinaria tratta di insiemi infiniti di numeri, a partire dall'insieme N dei numeri naturali: {0, 1, 2, 3, 4 ...}.
Nella realtà però si ha spesso a che fare con situazioni nelle quali i numeri possibili sono finiti; l'orologio ha solo 12 o 24 ore; i numeri gestiti da un computer sono sempre limitati ecc.ecc.
Si definisce allora aritmetica finita un'aritmetica che opera su un insieme limitato di numeri. È detta anche aritmetica modulare o circolare, in quanto una volta raggiunto l'ultimo numero si ricomincia dal primo.
Esempio classico quello dell'orologio; le ore si susseguono da 0 a 23, il 24 coincide con il punto di partenza, quindi con lo 0; e con la mezzanotte si ricomincia da 0. L'insieme è {0, 1, 2, 3, ... 22, 23}.
L'aritmetica dell'orologio si dice aritmetica modulo 24.
In generale un'aritmetica finita modulo m si basa sull'insieme {0,1,2...m-1}; questi numeri possono anche vedersi come i possibili resti di una divisione per m.
Le regole di calcolo sono molto semplici, la somma algebrica e il prodotto vengono prima eseguite nell'aritmetica ordinaria; il risultato viene poi diviso per m e si considera il resto come somma.

Molti ambienti e linguaggi informatici prevedono un operatore per il calcolo del resto; il simbolo è mod (linguaggio Pascal) o % (linguaggio C). P.es. 12 mod 7 = 5; 12 % 7 = 5

Esempio: in modulo 24 , 15 + 13 = 4 perchè 15 + 13 = 28 e 28 mod 24 = 4.

Per quanto riguarda le proprietà algebriche delle aritmetiche finite: per la somma valgono tutte le proprietà dell'ordinaria somma fra numeri reali, ovvero è un gruppo finito commutativo.

Per il prodotto si usa lo stesso metodo, ma può cadere la regola di annullamento del prodotto (che dice: un prodotto è nullo se e solo se lo è almeno uno dei due fattori).

Esempio 1 : in modulo 24 , 11*3 = 9 perchè 11*3 = 33 e 33 mod 24 = 9.

Esempio 2 : in modulo 24 , 8*6 = 0 perchè 8*6 = 48 e 48 mod 24 = 0.

Questo inconveniente può evitarsi solo se m è un numero primo; in questo caso si ha un campo finito o di Galois (vedi anche gruppo moltiplicativo).

È anche possibile definire e calcolare l'inverso e la potenza di un numero.

Le aritmetiche finite trovano applicazione in molti metodi della crittografia, tra i quali basta ricordare RSA.

2.4.3. La funzione di Eulero

La funzione di Eulero associa a un numero intero *n* il numero dei numeri interi primi con n e minori di n (compreso l'uno); è una funzione basilare della teoria dei numeri ed interviene in molti teoremi come quello di Fermat-Eulero, oltre ad essere uno degli ingredienti fondamentali del cifrario RSA.

Per esempio per n = 6 la funzione di Eulero vale 2 perché gli interi primi con 6 e minori di 6 sono solo 1 e 5; per n = 7 la funzione vale 6 perché essendo 7 primo tutti i numeri che lo precedono sono primi con 7.

La funzione di Eulero di un numero *n* si indica di solito con $\Phi(n)$

Si dimostra che

$$\Phi(n) = n \cdot \left(1 - \frac{1}{n_1}\right) \cdot \left(1 - \frac{1}{n_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{n_m}\right)$$

dove $n_1, n_2, \ldots, n_m$ sono i fattori primi distinti di *n*.

Se *n* è primo allora ovviamente $\Phi(n) = n - 1$

Se *n* è il prodotto di due numeri primi *p* e *q*, è facile verificare che $\Phi(n)=(p-1)\cdot(q-1)$

Infatti $\Phi(n)=p\cdot q\cdot\left(1-\frac{1}{p}\right)\cdot\left(1-\frac{1}{q}\right)$ e svolgendo i prodotti $p\cdot\left(1-\frac{1}{p}\right)$ e $q\cdot\left(1-\frac{1}{q}\right)$ si ottiene la formula data.

N.B. Su alcuni testi la funzione di Eulero di *N* è chiamata indicatore di *N*.

Esempio

Prendiamo $n=18=3^2\cdot 2$, i fattori primi sono 2 e 3 e la funzione di Eulero vale:

$$\Phi(18)=18\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)=18\cdot\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)=6$$

ed effettivamente sono 6 i numeri primi con 18:

1, 5, 7, 11, 13, 17

Questo esempio ci permette anche di giustificare la formula, come una sorta di setaccio: all'inizio i numeri in gioco sono tutti e 18 (da 1 a 18); poi essendo 18 multiplo del due si escludono tutti i numeri pari, che sono la metà del totale e ne restano 9, come dalla prima parte della formula $18\cdot\left(1-\frac{1}{2}\right)$

1,3,5,7,9,11,13,15,17

A questo punto essendo anche 3 un fattore primo di 18, si escludono tutti i multipli del tre che sono un terzo del totale; ne restano i due terzi, appunto $\left(1-\frac{1}{3}\right)$, dei nove rimasti ovvero i sei già visti:

1,5,7,11,13,17

È evidente che il procedimento resta valido per qualsiasi numero e per qualsiasi numero di fattori e questo giustifica la formula di sopra.

2.4.4. Il calcolo dell'inverso nelle aritmetiche finite

L'inverso di un numero x in un'aritmetica finita modulo *N* è quel numero *y* per il quale risulta. $xy=1 \bmod N$

Un metodo di calcolo è fornito, quando *x* ed *N* sono primi tra di loro, dal teorema di Eulero-Fermat che asserisce:

$x^{\Phi(N)} = 1 \bmod N$

dove $\Phi(N)$ è la funzione di Eulero.

Allora l'inverso è semplicemente il numero

$y = x^{\Phi(N)-1} \bmod N$

Infatti moltiplicando modulo *N* ambo i membri dell'uguaglianza per *x* si ha:

$xy = x \cdot x^{\Phi(N)-1} = x^{\Phi(N)} = 1 \bmod N$

L'utilità di questo metodo di calcolo è ovviamente legata all'esistenza di un algoritmo efficiente per il calcolo della potenza in un'aritmetica finita.

Va inoltre rilevato che il calcolo della funzione di Eulero per numeri elevati ha la stessa complessità della fattorizzazione. Se N è molto grande conviene usare altri metodi; è p.es. possibile estendere a questo problema l'algoritmo di Euclide per il calcolo del MCD.

Esempio

Si prenda il numero 5 in un aritmetica finita di ordine 18; si calcoli la funzione di Eulero $\Phi(18) = 6$, e l'inverso di 5 viene ad essere 55 MOD 18 = 3125 MOD 18 = 11. E in effetti 5 * 11 = 55 = 1 mod 18.

Applicazioni

Supponiamo di avere due numeri d ed e che siano uno l'inverso dell'altro in un'aritmetica finita di ordine $\Phi(N)$, in altre parole sia $de = 1 \bmod \Phi(N)$, o che è lo stesso $de = 1 + k.\Phi(N)$ con k intero positivo qualsiasi. Allora se calcoliamo una potenza con uno dei due numeri come esponente:

$c = m^e \bmod N$

e poi la potenza con l'altro numero:

$\mathbf{m^*} = \mathbf{c}^d \bmod N = \mathbf{m}^{ed} \bmod N = \mathbf{m}^{1 + k.\Phi(N)} \bmod N = \mathbf{m}.m^{k.\Phi(N)} \bmod N$

ma per il teorema di Fermat-Eulero è $m^{\Phi(N)} = 1 \bmod N$, e dunque

$\mathbf{m^*} = \mathbf{m}.1^k \bmod N = \mathbf{m}$

In altre parole con il secondo elevamento a potenza si ritrova il numero di partenza m. Se consideriamo m come un messaggio da trasmettere e c come lo stesso messaggio cifrato abbiamo in pratica un metodo di cifratura che usa il primo esponente (e) come chiave di cifratura e il secondo (d) come chiave di decifratura.
Ed è proprio questo il meccanismo alla base del cifrario RSA.

2.5. Il cifrario di Augusto

Lo scrittore Robert Graves, grande studioso di storia romana e autore di una pseudo-autobiografia dell'imperatore Claudio (nei due romanzi Io Claudio e Il divo Claudio), sostiene che Augusto usava accanto al semplice codice di Cesare un cifrario più sicuro per le comunicazioni più delicate; sarebbe stato lo stesso Claudio a comprenderne il funzionamento dopo aver studiato le carte di Augusto.
La storicità di questo cifrario è dubbia, ma comunque lo descriviamo qui per completezza. Il metodo si basa sul testo greco dell'Iliade; il testo chiaro e un brano dell'Iliade erano scritti in parallelo; ogni lettera del chiaro era confrontata con la corrispondente dell'Iliade, si calcolava la differenza tra i due caratteri e la sequenza dei numeri così calcolati costituiva il messaggio cifrato.
Per decifrare era sufficiente sommare al carattere dell'Iliade il numero del messaggio.
Il procedimento è quello della somma e della differenza nelle aritmetiche finite.
Ecco un esempio usando come testo chiaro "Le nostre truppe in Polonia sono in rotta" crittografato usando come chiave i primi versi dell'Inferno di Dante Alighieri:

```
chiaro:    l  e  n  o  s  t  r  e  t  r  u  p  p  e  i  n  p
chiave:    n  e  l  m  e  z  z  o  d  e  l  c  a  m  m  i  n
sposta:   14  5 12 13  5 26 26 15  4  5 12  3  1 13 13  9 14
cifrato    z  j  z  b  x  p  o  t  x  w  g  s  q  r  v  w  d

chiaro:    o  l  o  n  i  a  s  o  n  o  i  n  r  o  t  t  a
chiave:    d  i  n  o  s  t  r  a  v  i  t  a  m  i  r  i  t
sposta:    4  9 14 15 19 20 18  1 22  9 20  1 13  9 18  9 20
cifrato:   s  u  c  c  a  u  k  p  j  x  c  o  e  x  l  c  u
```

Il messaggio crittato sarà quindi:

zjzbxpotxwgsqrvwdsuccaukpjxcoexlcu

Per decifrare il testo basterà compiere il processo inverso (sottrarre invece di sommare).

2.6. Il disco cifrante di Leon Battista Alberti

Nel corso del `400 il matematico Leon Battista Alberti (1404-1472), introduce una sostituzione polialfabetica facile da eseguire e che rende estremamente più difficili da cogliere i cicli che avvengono nella cifratura e quindi le periodicità del cifrario. Questa idea rimarrà in funzione, sostanzialmente inalterata, fino all'epoca moderna.

Il nuovo metodo di cifratura ha bisogno di un dispositivo meccanico, il disco cifrante, che l'Alberti chiama "Modine". Di questo modello devono esistere due copie, il primo a disposizione del mittente, il secondo presso il destinatario.

Si costruiscono due lamine a forma di cerchio con diametro diverso e si divide la circonferenza di ciascuna in 24 parti uguali o Case

Sulle case dei due cerchi si riportano i caratteri dell'alfabeto, inserendo solo nel più grande i numeri da 1 a 4 e togliendo le lettere "inutili" come H e K, quindi i due dischi si sovrappongono e si fissano in modo che possano ruotare intorno al loro centro. A questo punto siamo pronti per cifrare ogni messaggio.

Le due parti scelgono una chiave cifrante, chiave che serve esclusivamente per iniziare la cifratura "*… come quasi per una chiave per aprirci l'entrata…*", e che deve essere composta di una coppia di caratteri che determinano la corrispondenza iniziale fra i caratteri del disco più grande e caratteri del disco più piccolo. Così, scegliendo la chiave (A,r), i dischi devono avere inizialmente la disposizione illustrata in Figura 1.

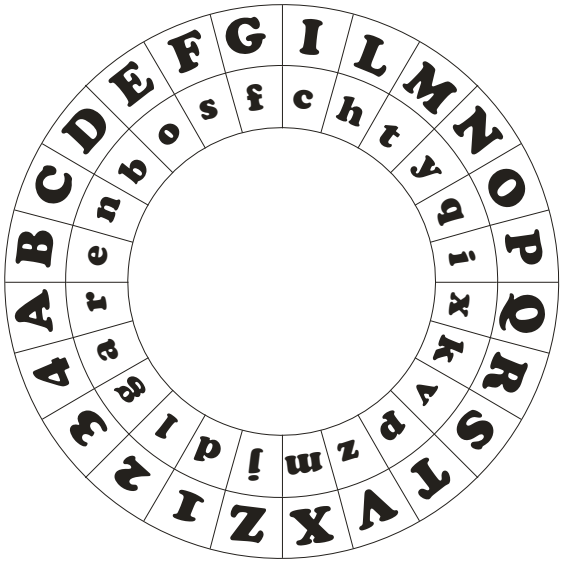


Figura 1

Supponiamo che le due parti vogliano scambiarsi il seguente messaggio:

`IL PROFESSOR MERCANTI HA ORGANIZZATO BENE QUESTO CONVEGNO`

Il mittente elimina gli spazi ed inserisce, a caso, numeri da 1 a 4 nel mezzo del testo, ad esempio:

`ILP1ROFE2SSORME4RCANTI2HAORG3ANIZZATOBE4NEQUES3TOCONVEG1NO`

A questo punto il mittente, ad ogni lettera del messaggio in chiaro, lettera che va letta sul disco più grande, associa la lettera corrispondente nel disco più piccolo fino a che non si incontra uno dei numeri: a quel punto la lettera corrispondente al numero determina una nuova disposizione: alla lettera A (la prima lettera della chiave) si fa corrispondere proprio questa lettera. Nell'esempio che stiamo considerando la nuova disposizione si ha in corrispondenza del numero 1: questo individua la lettera "d" per cui si ruota il disco più piccolo fino a portare la "d" in corrispondenza della "A" (vedi Figura 2).

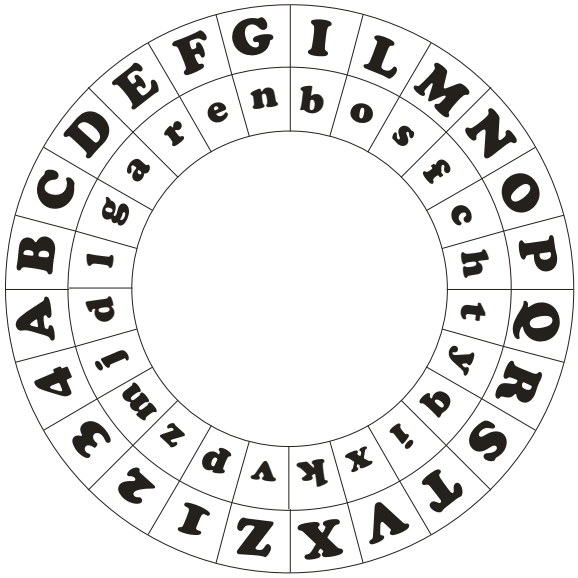


Figura 2

Procedendo in questo modo la traduzione del messaggio avviene nel seguente modo:

I L P 1 R O F E 2 S S O R M E 4 R C A N T I 2 H A …

c h i d y c e r z h o c n l p f m p n h a x x …

ottenendo la seguente cifratura:

chidycerzhocnlpfmpnhaxxrbjqalmfqbgivydkakehrjyjmeikokv.

E' utile e simpatico esercizio per il lettore operare ora a rovescio. Supponiamo di ricevere, come messaggio, la sequenza sopra indicata e naturalmente di essere in presenza della macchina di Alberti azzerata con la coppia (A, r). Allora in corrispondenza di "chi" avrò "ILP" ma in corrispondenza di "d" ho il numero "1" dunque ruoterò la macchina al contrario portando il carattere "d" in corrispondenza di "A" e ricomincerò a decifrare.

2.7. Il cifrario di Vigenère

Blaise de Vigenère pubblicò nel 1586 un trattato di cifre nel quale proponeva tra gli altri un codice che ebbe grande fortuna e che è ricordato con il suo nome. Si tratta del più semplice codice di sostituzione polialfabetica, e proprio per la sua semplicità ha goduto per secoli di una fama immeritata, essendo molto più debole di altri codici polialfabetici precedenti come il disco

dell'Alberti, o le cifre del Bellaso. Tale fortuna è durata fino a molti decenni dopo che era stato pubblicato un primo metodo di decrittazione: quello del Kasiski; e altri metodi di crittanalisi sono possibili.
Dal cifrario di Vigenère deriva peraltro il cifrario di Vernam, considerato il cifrario teoricamente perfetto.
Il metodo si può considerare una generalizzazione del codice 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 in base ad una parola chiave, da concordarsi tra mittente e destinatario, e da scriversi sotto il messaggio, carattere per carattere; la parola è detta verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo, come nel seguente esempio:

```
Testo chiaro  - ARRIVANOIRINFORZI
Verme         - VERMEVERMEVERMEVE
Testo cifrato - VVIUZVRFUVDRWAVUM
```

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

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

Figura 3

Per semplificare questa operazione il Vigénère propose l'uso della seguente tavola quadrata, composta da alfabeti ordinati spostati. Volendo ad esempio cifrare la prima R di ARRIVANO si individuerà la colonna della R, quindi si scenderà lungo la colonna fino alla riga corrispondente della corrispondente lettera del verme (qui E); la lettera trovata all'incrocio è la lettera cifrata (qui V); la seconda R invece sarà cifrata con la lettera trovata sulla riga della R di VERME, e cioé con la I

Il vantaggio rispetto ai codici mono-alfabetici è evidente: la stessa lettera del testo chiaro non è sempre cifrata con la stessa lettera; e questo rende più difficile l'analisi statistica del testo cifrato e la decrittazione.

Chi riceve il messaggio per decifrarlo deve semplicemente usare il metodo inverso (sottrarre invece che sommare); riferendosi all'esempio di sopra si avrà:

```
Testo cifrato - VVIUZVRFUVDRWAVUM
Verme         - VERMEVERMEVERMEVE
Testo chiaro  - ARRIVANOIRINFORZI
```

si potrà decifrare la seconda V ricercandola nella riga della corrispondente lettera del verme, la E; la colonna dove si trova la V ha al primo posto in alto la lettera chiara, la R.

2.8. Il cifrario di Vernam

Il cifrario di Vigenere ha il suo tallone d'Achille nel fatto di essere un insieme di cifrari di Cesare intercalati a distanza fissa, cosa che ne rende possibile e anzi molto facile la crittanalisi, tanto più se la chiave è breve.
Ben diversa sarebbe però la situazione se la chiave avesse lunghezza infinita o, che in fondo è lo stesso, fosse lunga come il testo chiaro (o meglio come la somma di tutti i testi chiari).
È questa l'idea proposta da G.S.Vernam nel 1926 per il cifrario che porta il suo nome; viene generata una chiave del tutto casuale, e dunque imprevedibile, lunga come il testo; a questo punto il chiaro e la chiave vengono "sommati" proprio come nel cifrario di Vigenere. L'unica differenza è che nel Vernam si sommano non tanto gli ordinali delle lettere da cifrare ma i singoli bit che codificano la lettera nei codici usati nelle telecomunicazioni (allora il codice Baudot, oggi il codice ASCII) con l'operazione logica XOR. Questa è simile all'addizione, ma ha il vantaggio di essere reversibile, e quindi verrà usata anche per decifrare.

ADDIZIONE DI CARATTERI CON IL CODICE BAUDOT

chiaro **c**	A 11000	T 00001	T 00001	E 10000	N 00110	Z 10001	I 01100	O 00011	N 00110	E 10000
verme **v**	W 11001	I 01100	A 11000	P 01101	F 10110	I 01100	L 01001	K 11110	M 00111	S 10100
cifrato **c XOR v**	00001 T	01101 P	11001 W	11101 Q	10000 E	11101 Q	00101 H	11101 Q	00001 T	00100 {sp}

In tal modo la debolezza del Vigenere è superata e anzi Claude Shannon, il padre della Teoria dell'Informazione, ha dimostrato nel 1949 che ogni cifrario "teoricamente sicuro" è un cifrario di Vernam (e viceversa). Infatti se la chiave è totalmente casuale e lunga come il testo allora il testo

cifrato non contiene alcuna informazione sul testo chiaro, ed è del tutto al sicuro dagli attacchi della crittanalisi statistica.
Per avere una sicurezza assoluta non si dovrebbe mai riutilizzare la stessa chiave; se si utilizza più volte la stessa chiave infatti questa torna ad essere più breve del messaggio, o meglio della somma di tutti i messaggi e il cifrario non è più perfetto. Per questo motivo questo tipo di cifrario viene detto a chiave non riutilizzabile.
Perché allora non usiamo tutti questo cifrario? Il problema è che la chiave lunga come il testo deve essere preventivamente comunicata al destinatario in modo sicuro e ... qui il gatto si morde la coda, visto che non sempre è disponibile un canale sicuro di comunicazione.
I due corrispondenti dovrebbero incontrarsi periodicamente in luogo sicuro e generare una sequenza casuale lunghissima, sufficiente per un gran numero di messaggi, da utilizzare un po' alla volta. Una volta esaurita la chiave dovranno incontrarsi di nuovo, rigenerare la chiave etc.etc.
Per semplificare le cose si potrebbe pensare di generare la chiave in modo pseudo-casuale, secondo una qualche regola nota e riproducibile dal destinatario; questa idea diede luogo nel periodo tra le due guerre mondiali a una generazione di macchine cifranti, tra le quali la macchina Lorenz usata dai tedeschi nella II guerra mondiale. Ma così il cifrario non è più assolutamente sicuro, perché la chiave non è più realmente lunga come il testo, la vera chiave è la regola generatrice!. Tanto è vero che la macchina Lorenz fu forzata dagli inglesi sin dal 1941.
Nonostante queste difficoltà il cifrario di Vernam sembra sia stato usato effettivamente negli anni della guerra fredda dai servizi segreti dell'Est e per il telefono rosso tra Washington e Mosca. Un cifrario di Vernam era anche quello trovato addosso al Che Guevara dopo la sua uccisione nel 1967.

2.9. Il cilindro di Jefferson

Il cifrario di Jefferson prende il nome dal suo inventore Thomas Jefferson (1743-1826), uno degli autori della Dichiarazione d'Indipendenza e Presidente degli USA nel 1801-1804. Il codice è di facile utilizzo e può ancor oggi essere considerato abbastanza sicuro. Stranamente però Jefferson non lo mise mai in uso e il suo cifrario fu dimenticato fino al 1922, quando fu riscoperto e

utilizzato, fino agli anni '50, dall'esercito statunitense. E nel 1890 Etienne Bazeries un crittologo francese propose l'Indecifrabile, un cifrario del tutto equivalente a quello di Jefferson.

Il codice di Jefferson è un metodo di cifratura meccanico basato su un cilindro di circa 15 cm di lunghezza e 4 cm di larghezza montato su un asse e sezionato in 36 dischi uguali (25 nella versione poi utilizzata dagli Americani, 20 nel cilindro di Bazeries). Sull'esterno di ciascuna ruota sono scritte le 26 lettere dell'alfabeto, equidistanti l'una dall'altra. L'ordine in cui sono disposte le varie lettere non corrisponde a quello naturale e varia da ruota a ruota.

Il messaggio in chiaro deve essere cifrato a blocchi di 36 lettere ciascuno (qualora l'ultimo blocco presenti meno di 36 lettere, esso deve essere completato con lettere nulle); la chiave di cifra è un numero che va da 1 a 25. Supponendo che il testo chiaro sia *"La missione in Polinesia è fallita"* e la chiave sia il numero 5, in una certa riga, non importa quale, si comporrà il messaggio in chiaro (omettendo naturalmente gli spazi); il crittogramma corrispondente andrà letto sulla quinta riga sopra quella che contiene il blocco in chiaro.

```
cifrato ->5  GKRPXAFYEQYFUUAXYYEPSQYFTAELCIXVFCKZ
          4  HJQOWBHXDPXETRZYAZDORPXESZDMBHWUEBHX
          3  IBPNVCQWBOWDSQYZPACNQPWDRYCNZGVTDAGW
          2  JNOMUDLTHNVCRPXAIBBMPNVCQWBOYFUSAZFU
          1  KONLTHNVCABVNTHNVCALNVCLHXDPXETRZYDP
chiaro ->    LAMISSIONEINPOLINESIAEFALLITAXXXXXXX
```

La decifratura avviene con il procedimento inverso; si compone il messaggio e si legge il testo chiaro nella quinta riga sotto.

In pratica la chiave di questo metodo è duplice: 1) un numero segreto compreso tra 1 e 25 e 2) la struttura del cilindro. Considerato che ogni ruota ha una permutazione di 26 caratteri e le permutazioni sono 26! (circa 4x1026) il numero di chiavi possibili è dell'ordine di 10 26xN, dove N è il numero di ruote, che è un numero enorme. Il livello di sicurezza è quindi molto elevato, ma con un grosso rischio: se il cilindro cade nelle mani del nemico, restano solo 25 chiavi possibili e il crittogramma può essere facilmente forzato come un cifrario di Cesare.

2.10. La macchina Enigma

Nella prima metà del XX secolo cominciarono a diffondersi macchine cifranti a rotori, sul modello del cilindro di Jefferson reinventato da Beziers.
La più celebre di queste macchine è l'Enigma inventata nel 1918 dal tedesco Arthur Scherbius e adottata dall'esercito e dalla marina tedesca fino alla seconda guerra mondiale.
L'Enigma è una macchina simmetrica, nel senso che se la lettera A è cifrata con la G in una certa posizione del testo allora nella stessa posizione la G sarà cifrata con la A. La stessa macchina serve quindi per cifrare e decifrare; una grossa comodità operativa che è però anche una debolezza crittografica.
La macchina ha al suo interno un certo numero di rotori (nella prima versione erano 3) collegati elettricamente e liberi di ruotare; quando l'operatore preme un tasto p.es. la A un segnale elettrico passa da rotore a rotore fino al rotore finale detto il riflettore e quindi torna indietro fino a mostrare una lettera illuminata che è il carattere cifrato. Non esiste possibilità di stampa, dunque l'operatore deve copiare a mano, carattere per carattere il messaggio cifrato da trasmettere.
La chiave dell'Enigma è la disposizione iniziale dei rotori; questa chiave veniva cambiata ogni 24 ore secondo una regola prefissata; in definitiva la vera chiave segreta era questa regola. Anche i collegamenti interni dei rotori sono segreti.
Inoltre i tre (o più) rotori possono essere scambiati tra di loro, e quindi vi sono n! (3! = 6 nella Enigma originale) disposizioni possibili, cosa che aumenta il numero di posizioni iniziali possibili. Era anche consigliato di tenere una scorta di rotori con cablaggi diversi, in modo da poter aumentare ancora il numero di combinazioni possibili.
I tedeschi erano convinti che l'Enigma fosse inattaccabile, ma questa fiducia era assai mal riposta. Già nei primi anni '30 un gruppo di matematici polacchi guidato da Marian Rejewski era riuscito a ricostruire la struttura dei rotori e a decrittarne i messaggi.
E il servizio crittografico inglese al quale partecipava anche il famoso matematico Alan Turing riuscì a sua volta a forzare l'Enigma sin dall'inizio della guerra, sfruttando le debolezze intrinseche di questa macchina e alcune ingenuità dei cifratori tedeschi.

Vediamo più in dettaglio il percorso storico e il funzionamento della macchina.
La macchina Enigma fu sviluppata da Arthur Scherbius in varie versioni a partire dal 1918 quando ottenne il brevetto, ispirandosi al disco cifrante di Leon Battista Alberti. La prima versione misurava appena 34 x 28 x 15 cm ma aveva un peso vicino ai 12 kg.

Egli creò una società, la Scherbious & Ritter, a Berlino per produrre tale macchina e mise in vendita la prima versione commerciale nel 1923. A causa dell'alto costo della macchina, sebbene i crittogrammi prodotti fossero effettivamente indecifrabili per l'epoca, molti commercianti e uomini d'affari pensarono che l'alto costo della macchina non giustificasse la possibilità di avere messaggi sicuri.

A causa della scoperta da parte dei tedeschi del fatto che le comunicazioni navali della Prima Guerra Mondiale erano state decrittate dalla Gran Bretagna anche tramite dei codici scoperti dopo l'affondamento di un incrociatore tedesco, il governo tedesco pensò che fosse arrivata l'ora di affidarsi ad un sistema sicuro per crittare i propri messaggi importanti.

Scherbius realizzò quindi una versione diversa dalla precedente, con i circuiti degli scambiatori modificati per impedire che le macchine già vendute fino a quel momento potessero cadere in mani nemiche, permettendo così la decodifica dei messaggi tedeschi.

Diversi esemplari furono acquistati dalla Marina Militare tedesca nel 1926, poi nel 1929 il dispositivo venne acquisito dall'Esercito, e da allora in poi praticamente da ogni organizzazione militare tedesca e dalla maggior parte della gerarchia nazista.

Versioni di Enigma furono usate per quasi tutte le comunicazioni radio tedesche, spesso anche per quelle telegrafiche, durante la guerra (perfino i bollettini meteorologici vennero cifrati con Enigma). Si dice che gli spagnoli (durante la Guerra civile) e gli italiani (nella Seconda Guerra Mondiale) usassero la versione commerciale, non modificata, per le comunicazioni militari. Questo però era sconsigliabile, dato che si trattava della prima versione di Enigma, meno sofisticata e già decifrabile grazie al metodo scoperto da Marian Rejewski.

Nel novembre del 1931 Hans-Thilo Schmidt, impiegato tedesco che poteva accedere alla macchina Enigma militare, aveva fornito ai francesi due documenti, chiamati Gebrauchsanweisung für die Chiffriermaschine Enigma e Schlüsselanleitung für die Chiffriermaschine Enigma che erano una specie di manuali di istruzioni della macchina tramite i quali ed altre informazioni recuperate dall'intelligence francese, permisero di ricostruire Enigma.

La Francia, visti gli schemi e cosa avrebbero dovuto decifrare, decise che il meccanismo era troppo complesso per essere decifrato dai propri crittoanalisti e non si preoccupò neanche di finire la realizzazione di un prototipo della macchina. La Polonia invece, che sapeva che, se la Germania avesse iniziato una guerra, sarebbe stata la prima ad essere attaccata, chiese alla Francia i progetti e tutto ciò che era stato recuperato per la realizzazione di un prototipo e per provare a violare il codice. Vista la natura tecnologica di Enigma, il Buro Polacco decise di interpellare gli accademici

della vicina Università Poznań, sottoponendoli ad un test per trovare le persone più adatte a decrittare Enigma.
I servizi segreti polacchi riuscirono così a decifrare Enigma, grazie all'unica debolezza del sistema cifrante, e cioè che nessuna lettera poteva mai comparire nel testo cifrato come sé stessa: l'intelligence polacco, guidato dal matematico Marian Rejewski progettò una macchina apposita chiamata Bomba, per estrarre da un messaggio enigma le chiavi di regolazione della macchina che lo aveva cifrato e quindi poterlo decifrare a loro volta. I tedeschi però cambiarono il funzionamento di Enigma introducendo un set di cinque rotori, di cui ne venivano usati tre diversi ogni giorno: questo moltiplicava per sessanta le combinazioni possibili e la bomba polacca non poteva affrontare un tale incremento di complessità.

Dopo l'invasione della Polonia, nel 1939, il progetto venne passato agli inglesi, i quali organizzarono un'attività di intercettazione e decifrazione su vasta scala delle comunicazioni radio tedesche a Bletchley Park e con l'aiuto di grandi matematici come Alan Turing, riprogettarono la Bomba e idearono diversi metodi per forzare le chiavi di codifica tedesche, che davano come prodotto il testo in chiaro noto con il nome in codice Ultra. Nel 1944, un'ulteriore evoluzione della bomba portò all'introduzione del calcolatore Colossus.
Ecco spiegato in modo più preciso il funzionamento della macchina.
La macchina Enigma aveva l'aspetto di una macchina per scrivere con due tastiere: una vera inferiore, e la seconda fatta di lettere luminose che si accendevano ad ogni tasto premuto sulla tastiera: la sequenza delle lettere che si illuminavano dava il messaggio cifrato (o quello in chiaro, se si batteva il testo cifrato).
Il suo funzionamento si basava su tre dischi cablati, detti rotori, che avevano 26 contatti per lato (uno per ogni lettera dell'alfabeto tedesco): i cablaggi dei dischi mettevano in comunicazione ciascuna lettera su un lato con una lettera a caso sull'altro lato. I dischi erano collegati insieme da un meccanismo simile ad un odometro: il primo disco ruotava di una lettera ad ogni pressione di tasto, il secondo ruotava di una lettera ogni volta che il primo compiva un giro e il terzo ruotava di una lettera quando il secondo finiva un giro. Il terzo e ultimo rotore era collegato a un riflettore che, cablato come un rotore, scambiava a caso il contatto della lettera del terzo rotore e rispediva indietro il contatto attraverso tutti e tre i rotori: quindi la tensione applicata al contatto della lettera premuta dall'operatore sulla tastiera veniva applicata sul contatto corrispondente del primo rotore e usciva dallo stesso rotore attraverso un altro contatto, diretta stavolta verso una delle lampadine del display di Enigma.

Oltre a questo, Enigma poteva essere regolata con degli spinotti per scambiare fra loro dieci lettere con altre dieci a scelta, per maggior sicurezza; inoltre i contatti di ogni rotore da una faccia all'altra potevano venire sfalsati a piacere.

Prima di usare la macchina un operatore doveva:

- ✓ Prendere i tre rotori da usare per quel dato giorno;
- ✓ Regolare gli anelli di ogni rotore perché fossero sulle corrispondenze indicate;
- ✓ Inserirli nella macchina nell'ordine indicato;
- ✓ Regolare i rotori sulla tripletta di lettere indicate nella chiave enigma di quel giorno;
- ✓ Configurare le spine di scambio lettere come stabilito dalla chiave enigma di quel giorno.

A questo punto la macchina era pronta a cifrare o decifrare un messaggio.

3. Crittografia simmetrica

I cifrari tradizionali sono tutti caratterizzati da una chiave segreta; mittente e destinatario dei messaggi segreti devono preventivamente concordare una qualche chiave da mantenere segreta: una parola segreta (oggi la si direbbe una password) o una griglia o una qualche tabella di codifica.
Questa necessità di comunicarsi la chiave segreta è un grosso punto debole: o ci si vede di persona e in luogo riservato, o si deve usare un canale di comunicazione assolutamente sicuro, cosa molto difficile da ottenersi (e se si dispone di un tale canale ... la crittografia diviene inutile); e la scoperta della chiave da parte del nemico sarebbe fatale alla segretezza del messaggio.
Questi cifrari sono detti anche simmetrici: infatti cifratura e decifratura fanno uso della stessa chiave; p.es. in un cifrario di Vigenere la parola segreta usata per cifrare viene usata anche per la decifratura.
Tra i cifrari a chiave segreta contemporanei va ricordato prima di tutti il DES della IBM.

3.1. Il DES

Il D.E.S. (Data Encryption Standard) è un cifrario composto che prevede 16 cifrature successive (trasposizioni e sostituzioni di bit).
Presentato nel 1975 dall'IBM allora leader incontrastato del mondo dell'Informatica è tuttora il cifrario a chiave segreta più usato negli ambienti informatici.
Certificato per la sua affidabilità da NIST (*National Institute of Standards and Technology*)[1] ogni 5 anni, fino al 1993, il D.E.S. è divenuto il sistema ufficiale di cifratura del Governo degli Stati Uniti già dal 1977.

[1] Il National Institute of Standards and Technology (NIST), è una divisione del Dipartimento del Commercio degli Stati Uniti. Precedentemente conosciuto come National Bureau of Standards, (NBS), da molto tempo sprona lo sviluppo delle attività economiche basate sull'informatica.
Il Computer Security Act, approvato dal Congresso nel 1987, autorizza NIST a sviluppare degli standards che rendano più sicure le informazioni del sistema informatico governativo, cui nessuno che non ne sia autorizzato deve accedere.
Ciò incoraggiò NIST a lavorare in collaborazione con altre agenzie governative ed industrie private, valutando le varie proposte avanzate e certificando gli standards che ritiene sicuri. Tra questi il DES è stato certificato ogni 5 anni fino al 1993, ma NIST, in seguito ai numerosi tentativi di forzatura, ed

In pratica il testo chiaro viene suddiviso in blocchi da 64 bit (equivalenti a 8 caratteri); ogni blocco è sottoposto a una trasposizione data in base ad una chiave di 64 bit; si applica quindi per 16 volte una funzione cifrante e alla fine la trasposizione inversa di quella iniziale.
Viene definito un sistema simmetrico perchè sia l'emittente del messaggio, sia il ricevente devono conoscere la stessa chiave segreta. Se usato singolarmente, il D.E.S. può essere un ottimo sistema per inserire files in un disco fisso, nella forma cifrata.
Il DES è stato presentato come un cifrario assolutamente sicuro, ma su questa presunta inattaccabilità si sono accese molte polemiche e certo anche molte leggende. La critica più fondata è quella di Hellman della Stanford University, che sostiene che la chiave è troppo corta e che il codice potrebbe essere forzato con una crittoanalisi di tipo esaustivo[2].
In effetti le chiavi possibili sono 256 (8 dei 64 bit sono usati come bit di controllo e ne restano quindi solo 56 per la chiave), un numero molto elevato ma non più fuori della portata dei moderni supercomputer. E' stata avanzata perfino l'ipotesi che un nemico sufficientemente ricco e potente potrebbe far costruire un computer capace di forzare il D.E.S. con una brutale ricerca esaustiva dello spazio chiave (che richiederebbe 3,5 ore). Tale computer è stato estimato per 1 milione di dollari; sono stati fatti tanti progetti ed altrettante polemiche, ma il computer non è ancora stato realizzato.
Gli studiosi Biham e Shamir idearono una nuova tecnica di forzatura detta crittanalisi differenziale Tale tecnica richiederebbe la cifratura di 247 testi in chiaro scelti in base a specifici criteri, ed il confronto dei risultati.
Più recentemente Matsui ha sviluppato un'altro tipo di attacco, conosciuto come crittanalisi lineare. Secondo Matsui la chiave del D.E.S. può essere riconosciuta tramite l'analisi di 243 testi in chiaro noti. Il suo primo esperimento ebbe successo, ma fu archiviato perchè richiese 9735 stazioni di lavoro operanti per 50 giorni e 12 ore, un tempo troppo lungo, considerando che la chiave del D.E.S. può essere frequentemente cambiata proprio per impedire forzature.
Il 17 luglio 1998 la Electronic Frontier Foundation diffonde un comunicato stampa con il quale annuncia la definitiva sconfitta del DES. Per dimostrare i gravi rischi di sicurezza a cui si sottopone chi utilizza il DES, la EFF costruisce il primo apparecchio Hardware non coperto dal segreto di

al parziale successo ottenuto da Matsui adottando la crittanalisi lineare ha dichiarato che non lo avrebbe più fatto.

[2] Si dice esaustiva una ricerca che prova una per una tutte le possibili soluzioni del problema dato; p.es. se si deve cercare una parola chiave di cinque caratteri alfabetici, si devono provare 26^5= 11881376 parole possibili.
I metodi esaustivi sono ovviamente praticabili solo con l'aiuto del computer.

stato per decodificare i messaggi crittografati utilizzando il Data Encryption Standard. In meno di un anno viene costruito un calcolatore costato 250.000 dollari che in meno di sessanta ore era capace di forzare un messaggio cifrato con DES. Tutte le specifiche utilizzate sono documentate in un libro realizzato dalla EFF dal titolo "Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design". Con le informazioni contenute nel libro è possibile realizzabile, a partire da un normale personal computer domestico, il così detto DES cracker. Il testo è disponibile unicamente in versione cartacea perché secondo le leggi USA in materia di esportazioni è reato pubblicare e quindi esportare questo tipo di informazioni su Internet.

Di seguito sarà descritto l'algoritmo DES che, nonostante abbia più di vent'anni, è stato utilizzato diffusamente fino ai nostri giorni. Come mostra la Figura 3a il testo chiaro viene cifrato in blocchi di 64 bit, che producono 64 bit di testo cifrato. L'algoritmo, che è parametrizzato da una chiave di 56 bit, ha 18 stadi distinti.
Il primo stadio è la trasposizione indipendente dalla chiave sul testo in chiaro, mentre l'ultimo svolge esattamente l'operazione inversa di tale trasposizione. È tuttavia evidente che queste due trasposizioni non aggiungono niente alla sicurezza dell'algoritmo.
I rimanenti 16 stadi sono funzionalmente identici, ma sono parametrizzati da differenti funzioni della chiave. L'algoritmo è stato progettato per consentire la decifrazione utilizzando la medesima chiave adoperata per la cifratura, solo che i passi sono effettuati nell'ordine inverso.

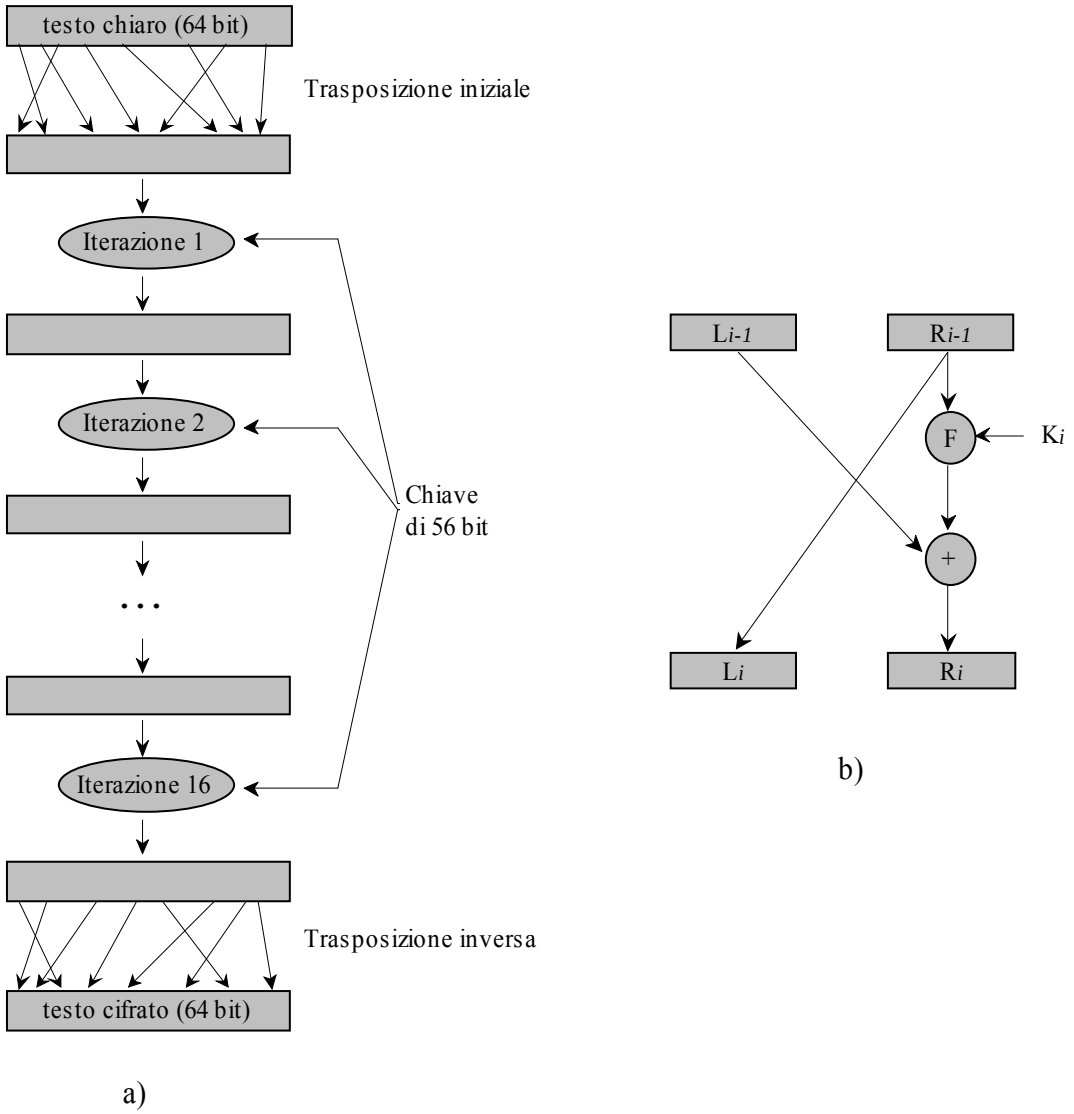


Figura 3 Lo standard di cifratura dei dati (DES). a) Schema generale. b) Dettagli di un'iterazione.

L'operazione di uno degli stadi intermedi è illustrata in Figura 3b. Il blocco di 64 bit viene smezzato in due parti di 32 bit e viene ricavata una chiave di 48 bit da quella di 56. Se indichiamo la metà sinistra e la metà destra all'iterazione i-esima rispettivamente con L_i e R_i e la chiave di 48 bit con K_i, allora i tre blocchi vengono combinati assieme seguendo le seguenti regole:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

in cui il simbolo $\oplus$ indica l'operatore OR esclusivo (XOR). Resta da definire la funzione F e da mostrare come venga ricavato ogni K_i dalla chiave di 65 bit.

La funzione consiste di quattro passi eseguiti in sequenza. Prima la funzione F espande R_{i-1} da 32 a 48 bit in modo tale che possa essere combinata con K_i. Per ottenere questo effetto R_{i-1} viene suddiviso in 8 parti di 4 bit e ogni parte viene espansa a 6 bit duplicando i bit alle estremità di

ognuna. Secondo, ai 48 bit risultanti viene applicato l'OR esclusivo con K_i. Questo output viene poi suddiviso in otto gruppi di 6 bit ciascuno e ogni gruppo viene poi assegnato ad un particolare circuito detto S-box (substitution box, è un circuito in grado di eseguire, in questo caso, la mappatura da 6 a 4 bit). Il risultato è una sequenza di 32 bit.

In ciascuna delle iterazioni si impiega una chiave diversa. Prima che l'algoritmo inizi, una trasposizione di 56 bit è applicata alla chiave. Appena prima di ciascuna iterazione, la chiave viene ripartita in due unità di 28 bit, ciascuna delle quali viene ruotata a sinistra di un certo numero di bit che dipende dal numero di iterazione. K_i è ricavata da questa chiave ruotata applicando ad essa un'altra trasposizione di 56 bit.

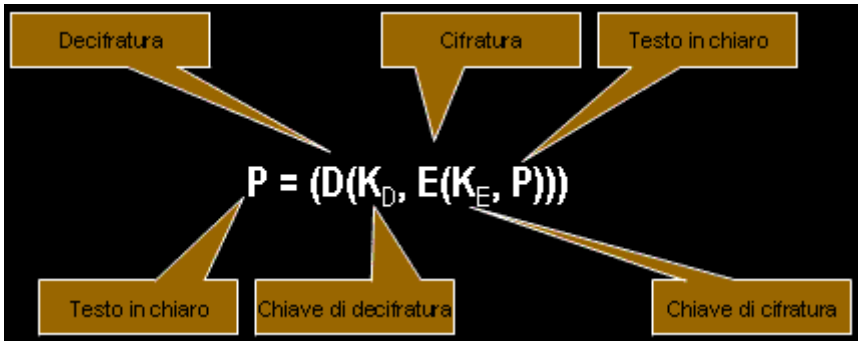
3.2. Introduzione ai crittosistemi asimmetrici

"La crittografia a chiave pubblica nacque nel maggio del 1975, come conseguenza di due problemi… il problema della distribuzione delle chiavi e quello delle firme elettroniche… La scoperta non consisteva in una soluzione, ma nel capire che i due problemi, ognuno dei quali sembrava irresolubile per definizione, poteva essere risolto e che la soluzione di entrambi scaturiva da un solo metodo".

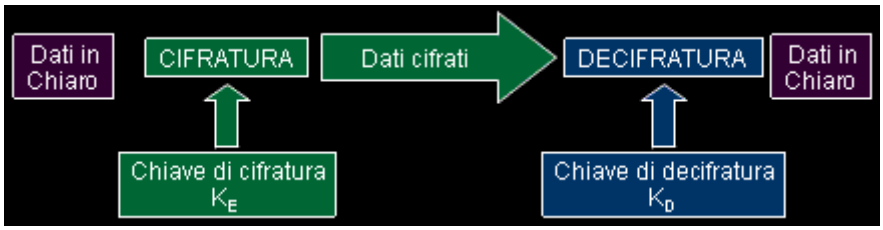
Whitfield DIFFIE

Modello utilizzato

In questo modello le chiavi di cifratura e decifratura sono utilizzate in coppia. In pratica una chiave di decifratura, KD, inverte la cifratura della chiave KE, così da avere:



Gli algoritmi di cifratura di questo tipo vengono detti asimmetrici, perché per convertire il dato dalla forma cifrata a quella in chiaro non basta invertire i passi di E.
Lo schema del modello è il seguente:



Vantaggi

La chiave pubblica può essere trasmessa tramite un canale insicuro, in quanto la sua conoscenza da parte di terzi non è sufficiente a mettere in pericolo la sicurezza dei dati crittografati con essa. Ciascuna chiave segreta resta sotto la responsabilità del solo utente proprietario.
In un sistema a chiave segreta per ogni possibile coppia di utenti deve esistere una chiave, per cui per n utenti occorrono:

$$\frac{n*(n-1)}{2}$$

chiavi; in un sistema a chiave pubblica deve esistere una coppia di chiavi per ogni possibile utente, ovvero per n utenti occorrono 2*n chiavi.
Esempio di combinazioni possibili:

Numero di utenti	Numero di chiavi in un sistema a chiave pubblica	Numero di chiavi in un sistema a chiave privata
10	20	45
100	200	4.950
1.000	2.000	499.500
10.000	20.000	49.995.000
100.000	200.000	4.999.950.000
1.000.000	2.000.000	499.999.500.000

Gli algoritmi simmetrici e quelli asimmetrici necessitano di chiavi di lunghezze differenti per raggiungere il medesimo grado di sicurezza teorica.

Simmetrica	Asimmetrica
56	384
64	512
80	768
112	1792
128	2304

La lunghezza raccomandata per la chiave è:

Anno	Privato	Azienda	Governo
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

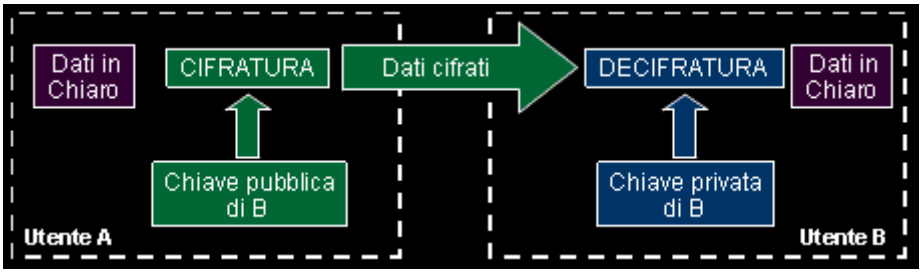
Svantaggi

Generalmente gli algoritmi asimmetrici sono molto più lenti da eseguire, rispetto a quelli simmetrici, per cui risulta poco agevole il loro uso per crittografare lunghi messaggi.

Caratteristiche

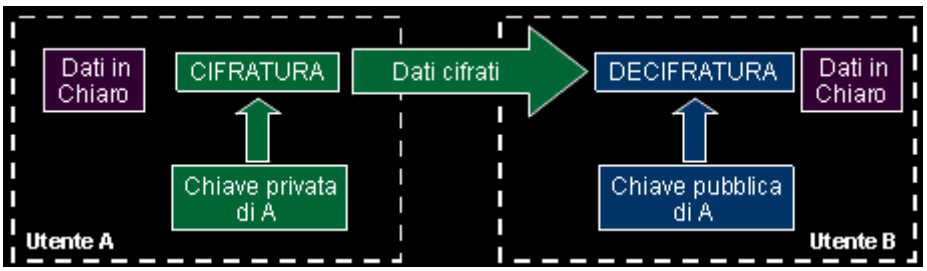
Riservatezza

L'utente A vuole inviare un messaggio all'utente B e lo cifra utilizzando la chiave pubblica di quest'ultimo. Solo il legittimo destinatario, l'utente B, utilizzando la propria chiave privata sarà in grado di decifrare il messaggio.



Autenticazione del mittente

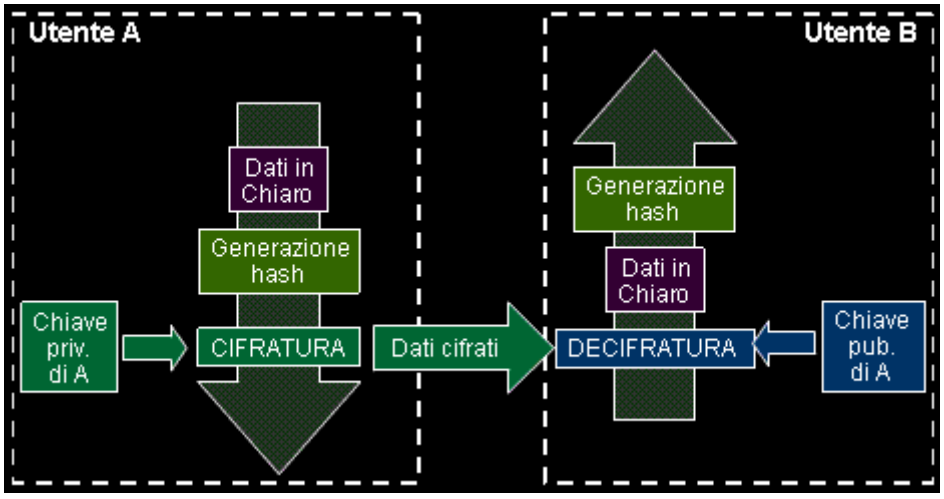
L'utente A cifra il suo messaggio con la propria chiave privata. Chiunque, avendo accesso alla chiave pubblica di A, può decifrare quel messaggio. Se la procedura riesce, si è allora sicuri che esso è stato scritto dall'utente A, l'unico a possedere la corrispondente chiave segreta. L'utente A ha quindi posto la sua firma elettronica sul messaggio.



E' possibile autenticare oltre al mittente anche il contenuto del messaggio, generando un "hashing" dello stesso. Se il messaggio viene alterato, l'hash, aggiunto in fondo al messaggio, non corrisponde più.

Autenticazione del mittente e del messaggio

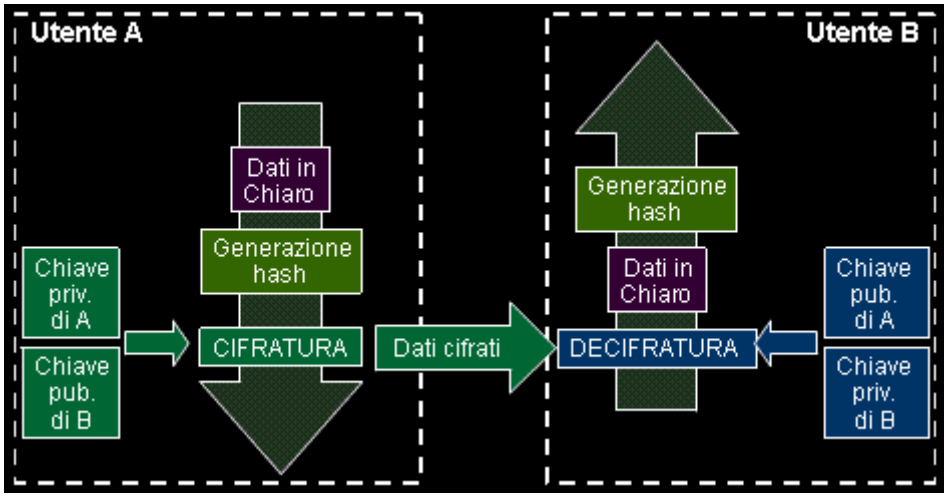
Il mittente può firmare con la propria chiave privata tutto l'insieme, oppure lasciare il messaggio vero e proprio in chiaro e firmare solo l'hash. Chiunque può decifrare l'insieme ricevuto o il solo hash con la chiave pubblica del mittente e così è sicuro dell'origine del messaggio.
Se inoltre, una volta effettuata la procedura, messaggio ed hash corrispondono, si è sicuri che nessuno dei due è stato alterato in qualche maniera.



Riservatezza ed autenticazione

E' possibile utilizzare contemporaneamente le due coppie di chiavi in modo da ottenere sia la riservatezza della comunicazione che l'autenticazione: L'utente A vuole inviare un messaggio all'utente B, e cifra il messaggio usando la chiave pubblica di quest'ultimo. Solo l'utente B, che ha la corrispondente chiave segreta, è in grado di decifrare e leggere il messaggio.

L'utente A cifra inoltre il suo messaggio con la propria chiave privata. Se l'utente B, che possiede la chiave pubblica dell'utente A, riesce nella decifrazione, è allora sicuro che esso è stato scritto dall'utente A, l'unico a possedere la corrispondente chiave segreta. L'utente A ha quindi posto la sua firma elettronica sul messaggio.



4. RSA

4.1. Storia

L'algoritmo RSA è stato descritto nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman al MIT; le lettere RSA vengono proprio dalle iniziali dei cognomi.

Clifford Cocks, un matematico britannico che lavorava per un dipartimento di spionaggio, il GCHQ, descrisse un sistema equivalente in un documento interno nel 1973. I documenti furono posti sotto segreto e, visto il costo relativamente alto delle macchine necessario a quel tempo per implementarlo, non ci furono ulteriori indagini né prove pratiche e la cosa fu considerata come una curiosità, per quanto se ne sa. La scoperta di Cocks fu resa pubblica solo nel 1997.

Nel 1983 l'algoritmo fu brevettato negli Stati Uniti dal MIT (brevetto 4.405.829). Il brevetto è scaduto il 21 settembre 2000.

Nel 2005 un gruppo di ricerca riuscì a scomporre un numero di 640 bit (193 decimali) in due numeri primi da 320 bit, impiegando per cinque mesi un cluster Opteron con 80 processori da 2,2 GHz, potenzialmente decifrando un messaggio codificato con RSA-640.

Fatto abbastanza rilevante è che RSA è computazionalmente impegnativo, soprattutto per quanto riguarda una eventuale realizzazione hardware. Di conseguenza un attuale buon utilizzo è quello di sfruttare RSA per codificare un unico messaggio contentene una chiave segreta, tale chiave verrà poi utilizzata per scambiarsi messaggi tramite un algoritmo a chiave segreta (ad esempio AES).

Oggi, insieme a DSS, RSA è uno degli algoritmi più usati per la cifratura di firme digitali.

4.2. Funzionamento

Per semplificare il funzionamento immaginiamo che A debba spedire un messaggio segreto a B. Occorrono i seguenti passaggi:

1. B sceglie due numeri primi molto grandi (per esempio da 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
2. B invia il numero che ha ottenuto ad A. Chiunque può vedere questo numero.
3. A usa questo numero per crittografare il messaggio
4. A manda il messaggio a B, che chiunque può vedere ma non leggere
5. B riceve il messaggio e utilizzando i due fattori primi, che solo lui conosceva decifra il messaggio.

A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe milioni di anni per scoprire i due fattori primi, con cui si può decifrare il messaggio.

In realtà questo sistema non è così semplice, come si può notare dai calcoli descritti nel paragrafo successivo, e per trasmettere grandi quantità di dati occorre tanto tempo, quindi A e B si scambieranno con questo sistema una chiave segreta (che non occupa molto spazio), che poi useranno per comunicare tra loro usando un sistema a crittografia simmetrica, più semplice, sicuro e veloce.

4.3. Operazioni

RSA è basato sul problema complesso della fattorizzazione in numeri primi. Il suo funzionamento base è il seguente:

1. si scelgono a caso due numeri primi, p e q, l'uno indipendentemente dall'altro, abbastanza grandi da garantire la sicurezza dell'algoritmo
2. si calcola il loro prodotto $n = pq$, chiamato *modulo* (dato che tutta l'aritmetica seguente è modulo n) e la funzione di Eulero Φ(n) = (p - 1)(q - 1) dopo di che i due primi p, q vengono eliminati;
3. si sceglie poi un numero e (chiamato *esponente pubblico*), più piccolo e coprimo con Φ(n)
4. si calcola il numero d (chiamato *esponente privato*) tale che $e * d \equiv 1 \pmod{(p-1)(q-1)}$

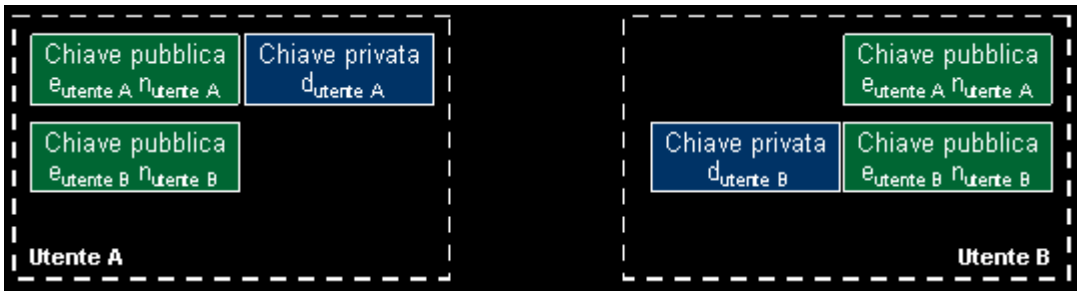
La chiave pubblica è (n, e), mentre la chiave privata è (n, d). I fattori p e q possono essere distrutti, anche se spesso vengono mantenuti all'interno della chiave privata.

La forza dell'algoritmo è che per calcolare d da e (così come il contrario) non basta la conoscenza di n, ma serve il numero $(p-1)(q-1)$, infatti fattorizzare (cioè scomporre un numero nei suoi divisori) è un'operazione molto lenta, soprattutto se n è un numero grande a sufficienza, poiché non si conoscono algoritmi efficienti.

Un messaggio m viene cifrato attraverso l'operazione $m^e \pmod{n}$, mentre il messaggio c viene decifrato con $c^d = m^{ed} = m^1 \pmod{n}$. Il procedimento funziona solo se la chiave e utilizzata per cifrare e la chiave d utilizzata per decifrare sono legate tra loro dalla relazione $e * d \equiv 1 \pmod{(p-1)(q-1)}$, e quindi quando un messaggio viene cifrato con una delle due chiavi può essere decifrato solo utilizzando l'altra. Tuttavia proprio qui si vede la debolezza dell'algoritmo: si basa sull'assunzione mai dimostrata (nota come assunzione RSA, o RSA assumption in inglese) che il problema di calcolare $\sqrt[e]{c} \mod n$ con n numero composto di cui non si conoscono i fattori sia computazionalmente non trattabile.

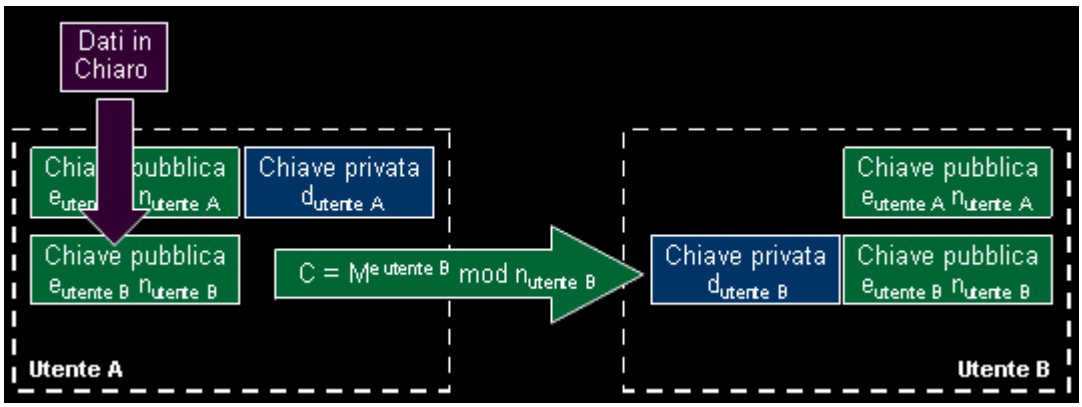
La firma digitale non è altro che l'inverso: il messaggio viene crittato con la chiave privata, in modo che chiunque possa, utilizzando la chiave pubblica conosciuta da tutti, decifrarlo e, oltre a poterlo leggere in chiaro, essere certo che il messaggio è stato mandato dal possessore della chiave privata corrispondente a quella pubblica utilizzata per leggerlo.

Una volta generata la coppia di chiavi, vediamo insieme le operazioni effettuabili, immaginando di avere due utenti, l'Utente A e l'Utente B, entrambi con la propria coppia di chiavi, pubblica e privata, più la chiave pubblica della controparte:



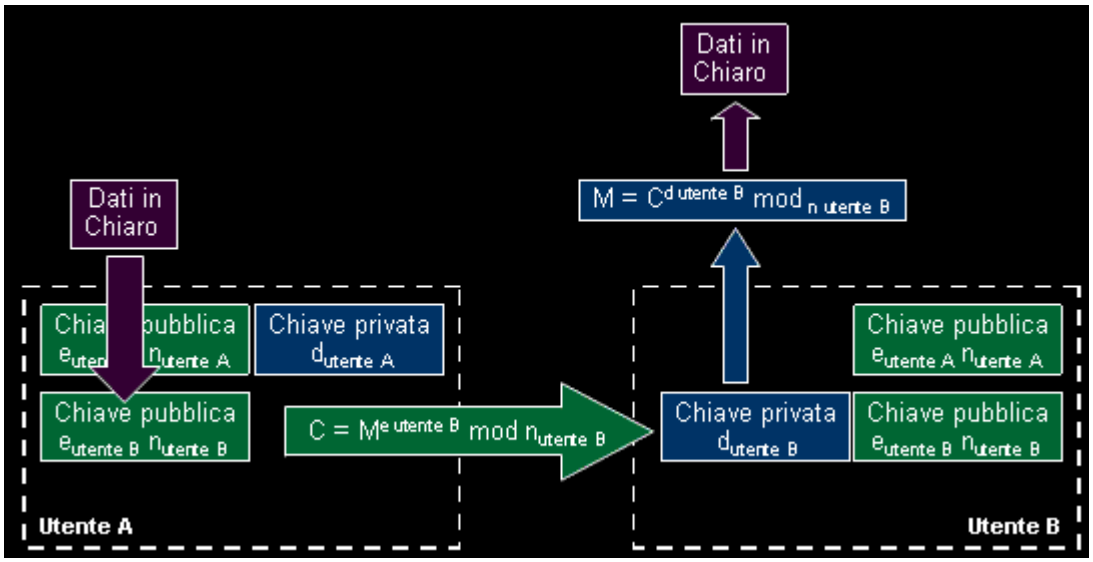
Cifratura

L'Utente A deve inviare del materiale cifrato all'Utente B. Per fare questo utilizzerà la chiave pubblica dell'Utente B effettuando queste operazioni:



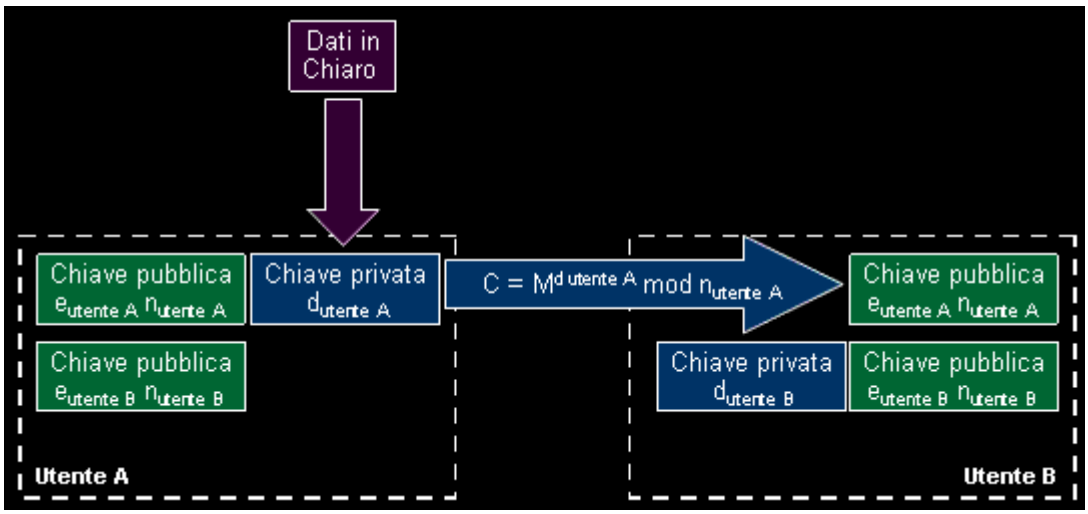
Decifratura

Ricevuto i dati cifrati, l'Utente B utilizzerà la sua chiave privata per eseguire l'operazione opposta di decifratura.



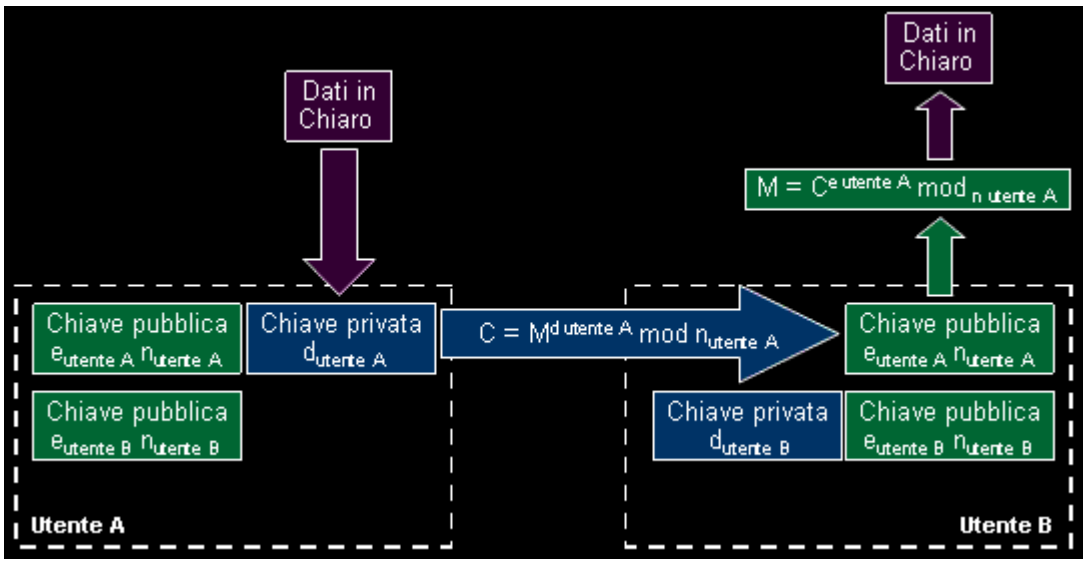
Firma

L'operazione di firma prevede l'utilizzo della chiave privata dell'Utente A sui dati, come riportato di seguito:



Verifica

Per verificare i dati ricevuti, l'Utente B utilizzerà la chiave pubblica dell'utente A:



Per motivi di efficienza e comodità normalmente viene inviato il messaggio in chiaro con allegata la firma digitale di un hash del messaggio stesso; in questo modo il ricevente può direttamente leggere il messaggio (che è in chiaro) e può comunque utilizzare la chiave pubblica per verificare che l'hash ricevuto sia uguale a quello calcolato localmente sul messaggio ricevuto. Se i due hash corrispondono anche il messaggio completo corrisponde (questo, ovviamente, solo se l'hash utilizzato è crittograficamente sicuro).

4.4. Esempio

Ecco un esempio di cifratura e decifratura RSA. I numeri scelti sono volutamente primi piccoli, ma nella realtà sono usati numeri dell'ordine di 10^{100}.

Generazione delle chiavi

1. $p = 61$ e $q = 53$, $(p-1)(q-1) = 3120$
2. $n = p * q = 61 * 53 = 3233$
3. $e = 17, e < n$ ed è coprimo per 3120 (in questo caso è primo, ma in generale non è necessario)
4. $d = 2753$ infatti
   $e * d = 2753 * 17 = 46801 \equiv 1 \pmod{(p-1)(q-1)} \equiv 1 \pmod{3120}$
   poiché $46801/3120 = 15$ con resto 1

Quindi abbiamo la chiave pubblica $(3233, 17)$ e la chiave privata $(3233, 2753)$.

Cifratura e decifratura

Prendiamo ora in considerazione il messaggio $m = 123$e cifriamolo per ottenere il messaggio cifrato c, ovviamente possiamo usare i 3233 e 17, ma non 2753 che fa parte della chiave privata.

$$c = m^e \pmod{n} = 123^{17} \pmod{3233} = 855$$

E ora decifriamo $c = 855$per ottenere m; qui utilizzeremo 2753, componente essenziale della chiave privata.

$$m = c^d \pmod{n} = 855^{2753} \pmod{3233} = 123$$