# La crittografia e la sicurezza dei dati

*M.Moro* - Dip. di Elettronica e Informatica - Univ. di Padova - Gennaio 2001

# 1 Introduzione

La sicurezza nella archiviazione e nella trasmissione dei dati richiede di adottare adeguate misure per proteggere i dati da intrusioni o da una loro utilizzazione diversa da quella prevista dai legittimi possessori e/o operatori. Questo problema, già affrontato nei secoli passati relativamente ai messaggi scritti, ha acquisito una connotazione particolare grazie all'uso dei *computer* e delle reti di trasmissione, e si è esteso alla protezione di dati di qualsiasi natura. La tecnica di base adottata a tale scopo viene denotata con il termine generale di **crittografia**. Attualmente le due forme più diffuse di crittografia sono dette **crittografia simmetrica** e **crittografia asimmetrica**, cui sono strettamente legati argomenti quali la firma **digitale** e la **certificazione**. Il problema ha di recente assunto maggior peso con riferimento ai **sistemi di pagamento in rete**.

Quando si parla della sicurezza nella trasmissione delle informazioni su supporto elettronico si intende quel complesso di accorgimenti che evitano che una unità informativa che viene in qualche modo trasmessa (un messaggio, nel caso più semplice, oppure un file o un archivio) venga intercettata da entità diverse dal o dai destinatari, e il contenuto informativo da questi consultato e/o copiato. Va detto subito che non esiste una soluzione che garantisca la sicurezza al 100% ma esistono metodi diversi con diversi gradi di sicurezza, a cui corrispondono diverse tipologie di costo: sta all'utilizzatore stabilire un adeguato livello di sicurezza valutando il rapporto tra il costo da sopportare e il valore delle informazioni protette.

Per esempio, a livello aziendale a tutt'oggi il telefono su rete pubblica e, conseguentemente, il fax possono essere ritenuti sufficientemente sicuri per le normali operazioni, anche quando si tratta di informazioni parzialmente o totalmente riservate, nonostante tecnicamente la sicurezza in quei casi sia in linea di principio modesta (basti pensare alle intercettazioni e al fatto che si può facilmente collegare un apparecchio fax (quasi) direttamente sulla linea d'uscita dell'inviante, cosicché la trasmissione può essere tranquillamente letta senza che l'inviante se ne accorga). In alcuni casi l'azienda decide di ricorrere a mezzi più costosi e ritenuti più affidabili (messo personale, corriere privato, o altro).

Con lo svilupparsi dell'informatica, e soprattutto della telematica, sorgono nuove istanze per la trasmissione sicura delle informazioni. Mentre in alcuni settori come quelli dell'industria strategica e militare, questi problemi sono stati sempre presenti, con lo sviluppo della rete *Internet*, che ha natura 'aperta', e del commercio elettronico, queste problematiche si sono moltiplicate e hanno assunto importanza via via crescente anche per utenti normali.

Ricomprenderemo nel termine generale di *crittografia* le diverse e sempre più sofisticate tecniche atte ad un invio sicuro dell'informazione. Per *crittoloanalisi* si intenderà lo studio dei metodi di attacco atti a ricavare le chiavi di decifratura dai messaggi cifrati; crittografia e crittoanalisi formano insieme la cosiddetta *crittologia*. Nelle note che seguono si parlerà sempre genericamente di 'messaggio' per indicare l'unità informativa da proteggere.

# 2 La crittografia

Da secoli la protezione sulla trasmissione dei dati viene ottenuta con il metodo della *crittografia*, consistente nel trasformare il messaggio originario in una forma reversibile ma inintelligibile ai più salvo che al destinatario. Ai primordi di applicazione di questo metodo, la sicurezza era basata sull'assunto che solo mittente e destinatario conoscessero la **regola di trasformazione** e quella inversa: si pensi ad esempio al famoso codice di Cesare che traslitterava le lettere alfabetiche (**sostituzione**) che formavano in sequenza il messaggio, spostandole di una quantità fissa rispetto all'alfabeto, o un'altra classe di trasformazioni che collocavano in posizione diversa i caratteri all'interno del messaggio (**trasposizione**).

Nella moderna crittografia il metodo di trasformazione è ricondotto ad un *algoritmo* eseguito da uno o più elaboratori, che trasforma il messaggio sfruttando le caratteristiche di precisione e rapidità degli elaboratori e la praticità del supporto elettronico. Un algoritmo di crittografia è generalmente costituito da una regola di trasformazione che viene fatta dipendere da un parametro detto *chiave*. Questo significa che l'applicazione del medesimo algoritmo di crittografia su un determinato messaggio con due chiavi distinte produce sempre risultati diversi nei due casi, ed inoltre il messaggio *criptato* può essere *decriptato* solo applicando la chiave giusta. In questo modo, la sicurezza non è più basata sulla segretezza dell'algoritmo (che anzi è bene sia mantenuto pubblico, così al suo perfezionamento, in termini di qualità ed efficienza di calcolo, possono contribuire esperti diversi sparsi per il mondo) bensì su quella della chiave: questo principio generale è stato enunciato da Kerckhoffs nel 1883 (***principio di Kerckhoffs***). Il metodo è tanto più sicuro quanto più difficile è scoprire, disponendo al più della conoscenza dell'algoritmo utilizzato, del messaggio *criptato*, ed eventualmente di qualche altra informazione accessoria quale la tipologia del contenuto, la chiave necessaria per *decriptarlo*.

### 2.1.1 Il Cifrario di Vernam e l'importanza della chiave

Come brevemente accennato sopra, un cifrario si basa su due presupposti: un **algoritmo** che definisce le regole per l'operazione di cifratura e per quella di decifratura, e una **chiave** che rende il risultato dell'applicazione dell'algoritmo parametricamente dipendente dalla chiave stessa. Ad esempio, nel codice di Cesare l'algoritmo è la regola di trasposizione letterale e la chiave è il fattore di trasposizione (1..25).

Si è presto verificato che la sicurezza di un cifrario dipende dalla lunghezza della chiave poiché da questa dipende il numero di varianti dell'applicazione dell'algoritmo che si possono ottenere. Più varianti sono possibili e più è difficile che si riesca in tempi ragionevoli a identificare la chiave, provando tutte le combinazioni dell'algoritmo di decifratura sul messaggio cifrato (attacco esaustivo).

L'idea proposta da G.S.Vernam nel 1926, per il cifrario che porta il suo nome, conduce ad un cifrario intrinsecamente sicuro; viene generata una chiave del tutto casuale, e dunque imprevedibile, lunga come il testo in chiaro, che viene "sommato" alla chiave per dare il messaggio cifrato. Il noto teorico dell'informazione Claude Shannon 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 in chiaro, ed è del tutto al sicuro dagli attacchi della crittoanalisi 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. Dovendo la chiave lunga come il testo essere preventivamente comunicata al destinatario in modo sicuro, il mittente deve generare periodicamente una chiave casuale lunghissima, passarla in modo sicuro al destinatario ed usarla a pezzetti, in base alla lunghezza dei messaggi trasmessi, fino ad esaurimento. Questi limiti rendono difficilmente utilizzabile questo metodo generale. Nonostante ciò sembra che questo cifrario 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.

# 3 L'avvento dei computer

La nascita della moderna informatica ha fatto fare un salto di qualità anche al settore crittografico: in particolare è stato possibile studiare nuove metodologie di trasformazione crittografica non più legate ai simboli del testo da trasmettere, ma riferentesi direttamente alla loro codifica binaria. Ciò ha consentito, da un lato, di poter spezzare le correlazioni intrasimbolo (i bit della codifica di un simbolo) e intersimbolo (parole e frasi) rendenso più difficile l'applicazione di crittoanalisi statistica, e dall'altro, di poter cifrare informazioni di qualsiasi natura (non strettamente testuale).

Per esemplificare il tipo di trasformazione che un computer può agevolmente eseguire su un messaggio da cifrare, si consideri una chiave costituita da una sequenza di bit di lunghezza pari al messaggio, egualmente considerato come sequenza di bit, e si esegua l'operazione di OR esclusivo (può essere vista come somma di due bit modulo 2) su ciascuna coppia di bit corrispondenti (1 bit dal messaggio, 1 bit dalla chiave nella stessa posizione relativa). La sequenza che si ottiene è il messaggio cifrato, che si può ricostruire nella sua versione in chiaro non appena si ripeta, presso il destinatario, l'operazione di OR esclusivo con la medesima chiave usata per cifrare.

## *3.1 La crittografia a chiave simmetrica (segreta)*

Quando sia l'algoritmo di cifratura che quello di decifratura usano la medesima chiave, si parla di *crittografia a chiave simmetrica* o *a chiave segreta*. In questo caso si ha (fig. 1):

M' = C(M, K) C algoritmo di cifratura M messaggio in chiaro M' messaggio cifrato K Chiave segreta
M = D(M', K) D algoritmo di decifratura

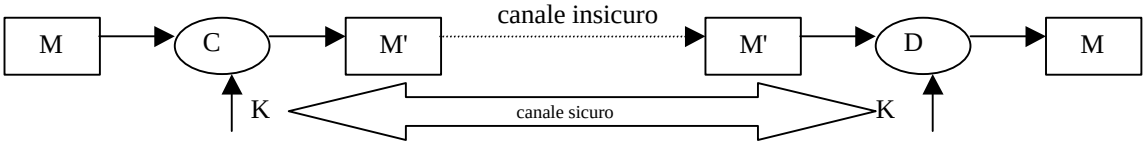



**Figura 1**

La necessità che entrambi gli interlocutori dispongano della chiave segreta comporta due aspetti negetivi:

- obbliga quello dei due che la genera a trasmetterla all'altro attraverso un canale sicuro (incontro 'ravvicinato', corriere fidato, altro sistema di cifratura già attivo, ecc.);
- ai fini della sicurezza, è necessario che venga generata e scambiata una chiave segreta per ogni coppia di interlocutori, fatto questo che provoca la proliferazione delle chiavi e aumenta ulteriormente il problema del loro scambio in forma sicura.

Anche la possibilità di rinnovare periodicamente le chiavi, per ridurre il rischio che vengano a conoscenza di intrusi, si scontra con lo stesso problema di invio sicuro.

Come già detto in precedenza, la sicurezza è basata sulla segretezza della chiave e sulla pratica impossibilità di ricavare la chiave dal messaggio *criptato*, pur conoscendo l'algoritmo utilizzato. Tanto per dare una misura di quest'ultimo aspetto, supponendo che la chiave sia costituita da un numero intero rappresentabile nel calcolatore con 256 bit (32 byte) e pensando di provare ad applicare esaustivamente l'algoritmo D sul messaggio *criptato* con tutte le possibili chiavi (assumendo di poter riconoscere quando il testo decriptato corrisponde all'originale; si noti che, nel caso peggiore, il risultato positivo potrebbe arrivare con l'ultima chiave provata, mediamente dopo aver esaminato metà chiavi), disponendo di un elaboratore in grado di provare 1 miliardo di chiavi al secondo, sarebbero necessari nel caso peggiore:
$T = 2^{256} / 10^9$ s ~= $10^{77} / 10^9 = 10^{68}$ s ~= $10^{68} / (31*10^6)$ anni = $3*10^{60}$ anni

## *3.2 L'algoritmo DES (Data Encryption Standard) e altri algoritmi a chiave simmetrica*

Si tratta di un algoritmo a chiave simmetrica proposto da IBM nel 1975 e accettato come *standard* nel 1977 e da allora, e fino a tempi recenti, è stato utilizzato dagli enti governativi americani (e da altri) per cifrare dati sensibili. Si tratta di un algoritmo piuttosto

efficiente e lavora con una chiave di 64 bit, di cui 56 generati casualmente (quindi questa è la vera lunghezza della chiave) e 8 calcolati come bit di parità per ciascun gruppo di 7 bit dei 56 generati. Il numero di combinazioni della chiave ($2^{56} \approx 7.2 * 10^{16}$) ha fatto ritenere sufficientemente sicuro almeno fino alla comparsa dei veloci calcolatori degli anni '90.

In grande sintesi l'algoritmo funziona nel modo seguente. Il messaggio viene scomposto in blocchi di 64 bit, con un riempimento dell'ultimo blocco se inferiore a 64 bit.. Ogni blocco subisce la seguente sequenza di trasformazioni:

1. Si permutano i 64 bit secondo una mappa prefissata (IP);
2. Detti L e R rispettivamente i 32 bit della prima metà e della seconda metà del blocco (LR costituisce l'intero blocco), si esegue 16 volte di seguito la seguente coppia di operazioni, dalla quale si ottiene una nuova combinazione di 64 bit L'R':
   L' = R
   R' = L $\oplus$ f(R, K)
   K è un blocco di 48 bit prelevati, secondo una mappa prefissata, diversa ad ogni ciclo di ripetizione, dai 64 bit della chiave; f(R,K) è una funzione di trasformazione (qui per semplicità non descritta in dettaglio) che opera su un blocco di 32 bit e uno di 48 bit producendo un blocco di 32 bit, e $\oplus$ è l'operatore di OR esclusivo bit-a-bit.
3. Si permutano i 64 bit ottenuti con la mappa inversa della permutazione iniziale ($IP^{-1}$)

Le caratteristiche di simmetria dell'algoritmo, compresa la permutazione iniziale e quella inversa finale, fanno sì che algoritmo di decifratura sia del tutto identico a quello di cifratura salvo l'applicazione in ordine inverso della sequenza di blocchi K ricavata dalla chiave.

Nel 1998 la Cryptography Research assieme a Advanced Wireless Technologies e EFF hanno progettato e prodotto un multi-computer costituito da 27 schede montanti un totale di più di 1800 processori specializzati, ciascuno dotato di 24 unità di ricerca in grado di provare separatamente un *range* di chiavi secondo un fornito criterio di identificazione del messaggio corretto. Questo processo di identificazione selezionava un sottoinsieme ristretto di chiavi che, applicate, forniscono un messaggio decifrato verosimilmente corretto, e che vengono valutate con criteri più selettivi da un computer di architettura tradizionale. Il grado di parallelismo ottenuto consentiva, con le sue 37000 e più unità di ricerca, di poter provare più di 92 miliardi di chiavi al secondo; il costo del progetto e dell'apparecchiatura è rimasto sotto i $250.000. La macchina è stata utilizzata per effettuare l'attacco esaustivo su un messaggio cifrato con DES e fornito da RSA come banco di prova per un concorso. La prova è stata superata il 15/7/1998 e il concorso vinto: la chiave è stata trovata dopo 56 ore di lavoro.

Una volta dimostrato che il DES con chiave a 64 bit non poteva più considerarsi sicuro con la tecnologia disponibile negli anni '90, sono stati proposti altri algoritmi a chiave simmetrica. Il triplo-DES è in pratica l'applicazione in serie di 3 DES con due chiavi diverse (una usata due volte) o con 3 chiavi diverse, allungando corrispondentemente la chiave effettiva. IDEA (International Data Encryption Algorithm) è un algoritmo realizzabile sia in *hardware* che in *software*, veloce quanto DES e con chiavi da 128 bit.

## *3.3 L'algoritmo di Diffie-Hellman*

Nel 1976 Diffie e Hellman hanno proposto un metodo particolare per generare e trasmettere su un canale insicuro una chiave segreta, da utilizzare successivamente per un algoritmo di cifratura simmetrico. Poiché le caratteristiche dell'algoritmo sono state più tardi utilizzate come base per lo sviluppo degli algoritmi a chiavi asimmetriche, l'interesse per questo metodo va oltre il suo principale obiettivo appena ricordato..

Detti X e Y i due interlocutori, il procedimento si divide nei seguenti passi:

1. X e Y scelgono pubblicamente un valore naturale N (grande) e un altro valore s appartenente all'intervallo di valori G=[0,N-1].
2. X sceglie in modo casuale e privato un valore a nell'intervallo G; calcola poi il valore $x = s^a \bmod N$, e invia x a Y.
3. Analogamente Y sceglie in modo casuale e privato un valore b nell'intervallo G; calcola poi il valore $y = s^b \bmod N$, e invia y a X.
4. A questo punto entrambi gli interlocutori possono calcolare la stessa chiave privatamente, X nella forma $Kx=y^a \bmod N$, Y nella forma $Ky=x^b \bmod N$.

Che la chiave calcolata separatamente sia la stessa si verifica facilmente poiché risulta:

$Kx = y^a \bmod N = (s^b \bmod N)^a \bmod N = (s^b)^a \bmod N$

$Ky = x^b \bmod N = (s^a \bmod N)^b \bmod N = (s^a)^b \bmod N = (s^b)^a \bmod N = Kx$

Attraverso il canale insicuro sono transitati N, s, x e y ma non a e b, necessari per il calcolo della chiave: la sicurezza è basata sulla elevata difficoltà computazionale di ricavare l'esponente a della formula $x = s^a \bmod N$ (logaritmo intero) noti N, s e x, e analogamente per b e y.

Esempio:

$N=1000 \quad s= 9 \quad X$ sceglie $a=4$ e calcola $x= 9^4 \bmod 1000 = 6561 \bmod 1000 = 561$
Y sceglie $b = 6$ e calcola $y= 9^6 \bmod 1000 = 531441 = 441$
$Kx = 441^4 \bmod 1000 = 37822859361 \bmod 1000 = 361$
$Ky = 561^6 \bmod 1000 = 31172897213027361 \bmod 1000 = 361$

# 4 La moderna crittografia a chiave asimmetrica

Più di recente è stato proposto un approccio alternativo che risolve brillantemente i limiti della crittografia a chiave segreta. Esso si basa sull'uso non di una singola chiave, bensì di coppie di chiavi: ciascuna coppia è costituita da una **chiave pubblica** ($K_p$), normalmente utilizzata per cifrare, e da una **chiave privata o segreta** ($K_s$) normalmente utilizzata per decifrare. Le due chiavi della coppia sono fra loro strettamente correlate e vengono generate di norma da un potenziale destinatario. Infatti, quando un utente Y desidera ricevere un messaggio sicuro, genera una coppia di chiavi pubblica/privata ($Ky_p$/$Ky_s$) e comunica la propria chiave pubblica $Ky_p$ al mittente X: come dice l'attributo, questa chiave può essere tranquillamente trasmessa attraverso canali non sicuri, addirittura può essere pubblicata su un sito associato ad Y e/o su rubriche di chiavi pubbliche mantenute da terzi su siti raccolta. Questa possibilità discende dal fatto che la sicurezza è legata alla sola segretezza della chiave privata: Y dovrà conservare con cura in segreto la chiave $Ky_s$ in quanto solo attraverso quest'ultima è possibile decifrare un messaggio criptato con $Ky_p$. Formalmente si ha che (fig.2):

$M' = C(M, Ky_p)$ C algoritmo di cifratura M messaggio in chiaro M' messaggio cifrato $Ky_p$ Chiave pubblica del destinatario

$M = D(M', Ky_s)$ D algoritmo di decifratura $Ky_s$ Chiave privata del destinatario

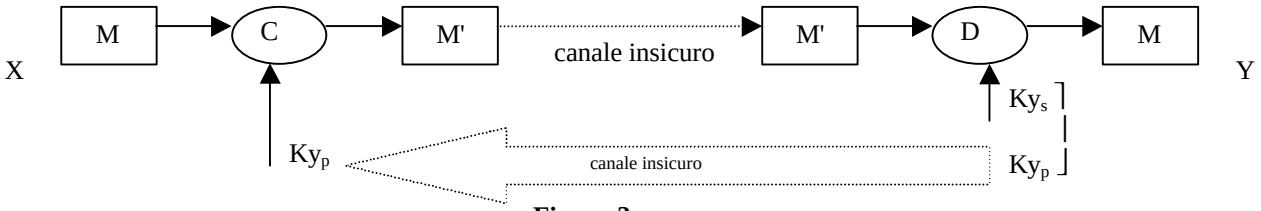



**Figura 2**

Quindi, una volta cifrato il messaggio con una determinata chiave pubblica, non può essere decifrato se non con la corrispondente chiave privata; la chiave pubblica usata per cifrare non consente di decifrare, nemmeno alla persona che effettuato la cifratura. Da un punto di vista pratico, un inviante deve procurarsi la chiave pubblica del ricevente se vuol essere sicuro che un messaggio possa essere letto solo da quest'ultimo.

Si noti che ciascun ricevente può disporre di una sola coppia valida di chiavi pubblica/privata in un certo momento, visto che la chiave pubblica può essere senza problemi conosciuta e condivisa da tutti i potenziali invianti, e quindi ogni utente deve conservare 'gelosamente' solo una chiave 'segreta', quella privata. Questo elimina il problema della proliferazione delle chiavi che affliggeva le chiavi simmetriche. Come in quel caso sarà comunque buona norma rinnovare periodicamente la coppia ed è per questo che risultano molto utili siti che mantengono aggiornata la raccolta delle chiavi pubbliche valide degli utenti registrati.

## *4.1 L'algoritmo RSA e altri algoritmi*

Il più conosciuto e utilizzato algoritmo a chiavi asimmetriche è stato proposto da Rivest, Shamir e Andleman nel 1978 e porta come nome la sigla dei cognomi dei suoi inventori. L'algoritmo sfrutta l'approccio di Diffie/Hellman e si basa sulla fattorizzazione di numeri interi grandi.

Un destinatario Y di messaggi sicuri, per poter generare la propria coppia di chiavi, effettua i seguenti passaggi:

1. Sceglie due grandi numeri interi p e q, entrambi numeri primi; il valore N = p*q verrà utilizzato per le operazioni di modulo durante la cifratura.
2. Sceglie un intero e<N che sia primo rispetto al valore b = (p-1)*(q-1) (cioè e non ha fattori comuni diversi da 1 sia con (p-1) che con (q-1)).
3. Trova il più piccolo intero d per il quale il valore (e*d-1) è divisibile per b, cioè (e*d) mod b = 1
4. La chiave pubblica è pari a $Ky_p$ = [N, e], la chiave privata $Ky_s$ = [N, d]; i fattori p e q possono essere distrutti o mantenuti segreti assieme alla chiave privata.

L'algoritmo di cifratura richiede che il messaggio venga suddiviso in blocchi di m bit con $m \leq \log_2 N$ (cioè il valore numerico espresso da ciascun blocco deve essere ≤ N); detto $m_i$ un generico di questi blocchi, la versione cifrata $m_i$' è ottenuta come:

$m_i' = m_i^e \bmod N$

Per la decifratura, si applica un calcolo analogo, ma con l'altro esponente, a ciascun blocco cifrato per riottenere quello in chiaro:

$m_i = m_i'^d \bmod N$

Esempio (con numeri piccoli):

p=5, q=11  N = p*q = 55  b = 4*10 = 40
(poiché p e q sono sempre dispari, b è sempre divisibile per 4)
e = 13  (13*d) mod 40 = 1  il più piccolo intero d che soddisfa l'eguaglianza è d = 37
$Ky_p$ = [55, 13]  $Ky_s$ = [55, 37]

se M = $3A90256C  ($ sta per esadecimale) si può decidere di cifrare blocchi di 4 bit, corrispondenti a 1 cifra esadecimale (infatti 4 < $\log_2$ 55 = 5.7; si poteva arrivare fino a

5 bit, mentre il cifrato ha necessariamente blocchi di 6 bit per rappresentare valori nell'intervallo [0,54])

$m_0' = (\$C)^{13} \bmod 55 = (12)^{13} \bmod 55 = 12 = \$0C$ $\quad$ $m_1' = (6)^{13} \bmod 55 = 51 = \$33$
$m_2' = (5)^{13} \bmod 55 = 15 = \$0F$ $\quad$ $m_3' = (2)^{13} \bmod 55 = 52 = \$34$
$m_4' = (0)^{13} \bmod 55 = 0$ $\quad$ $m_5' = (9)^{13} \bmod 55 = 14 = \$0E$
$m_6' = (\$A)^{13} \bmod 55 = (10)^{13} \bmod 55 = 10 = \$0A$ $\quad$ $m_7' = (3)^{13} \bmod 55 = 38 = \$26$

Il valore cifrato che si ottiene è una sequenza di 6*8=48 bit ottenuti giustapponendo i blocchi di 6 bit cifrati:

M' = $26 | $0A | $0E | 0 | $34 | $0F | $33 | $0C = (binario) %100110 001010 001110 000000 110100 001111 110011 001100 =
= $98A380D0FCCC

Per la decifratura si ottiene:

$m_0 = (\$0C)^{37} \bmod 55 = (12)^{37} \bmod 55 = 12 = \$C$ $\quad$ $m_1 = (\$33)^{37} \bmod 55 = (51)^{37} \bmod 55 = 6$
$m_2 = (\$0F)^{37} \bmod 55 = (15)^{37} \bmod 55 = 5$ $\quad$ $m_3 = (\$34)^{37} \bmod 55 = (52)^{37} \bmod 55 = 2$
$m_4 = (0)^{37} \bmod 55 = 0$ $\quad$ $m_5 = (\$0E)^{37} \bmod 55 = (14)^{37} \bmod 55 = 9$
$m_6 = (\$A)^{37} \bmod 55 = (10)^{37} \bmod 55 = 10 = \$A$ $\quad$ $m_7 = (\$26)^{37} \bmod 55 = (38)^{37} \bmod 55 = 3$

La sicurezza dell'algoritmo è basata sulla elevata difficoltà computazionale a ricavare i fattori p e q da un valore N grande, essendo quest'ultimo noto perché parte della chiave pubblica: il problema della fattorizzazione di un valore grande in due fattori primi, in particolare se questi sono grossomodo della stessa grandezza ma non così prossimi l'un l'altro, è ritenuto un problema difficile. In base a recenti ricerche che, in merito al problema della fattorizzazione con chiavi di 512 bit, hanno ottenuto risultati di quest'ordine: hardware del costo inferiore a 1 M$, 7-8 mesi di calcolo, oggi si può affermare che chiavi di 1024 o più bit sono ragionevolmente sicure per la maggior parte delle esigenze. Occorre tener però presente, come si evince dalla formula per la cifratura e decifratura, che più grandi sono le chiavi in gioco, maggiore è il tempo necessario per queste operazioni a parità di messaggio.

Sono stati proposti anche altri algoritmi come quello di ElGamal (1985) ancor più vicino rispetto a RSA al metodo di Deffie/Hellman, e quello delle curve ellittiche (il corpo numerico di base è in questo caso rappresentato dai punti di una curva ellittica definita su un campo finito) che ha un livello di sicurezza superiore a quello basato sulla fattorizzazione intera.

# 5 La firma digitale

La crittografia a chiavi asimmetriche risolve le limitazioni che, nell'invio sicuro, presentavano i metodi con chiave simmetrica (proliferazione delle chiavi e necessità di invio sicuro della chiave segreta). Connessi al problema della sicurezza nell'invio delle informazioni, vi sono alcuni problemi aggiuntivi che si possono così riassumere:

1. Garanzia di integrità del messaggio inviato (si vuole evitare il rischio che, per errori di trasmissione o per intrusione, un messaggio pervenga al destinatario corrotto rispetto all'originale)
2. Autenticazione dell'invio (il mittente deve essere riconoscibile come autore del messaggio)
3. Impossibilità di ripudio (il mittente non deve poter negare la produzione del messaggio che è avvenuta per sua volontà in un certo istante)
4. Identificazione del destinatario (il mittente deve essere sicuro dell'associazione chiave pubblica/destinatario)

I primi due problemi aggiuntivi vengono risolti con la tecnica della **firma digitale** mentre tutti e 4 sono legati al ruolo della cosiddetta **Autorità di Certificazione**.

La firma digitale, nella sua forma più semplice, non è altro che il messaggio cifrato con la chiave **privata** del mittente: in questo modo il destinatario può verificare, riuscendo a decifrare la firma con la chiave pubblica del mittente, e rilevando l'eguaglianza del messaggio effettivo e di quello 'contenuto' nella firma, sia l'identità del mittente che l'associazione tra firma e messaggio (ovvero la firma è pertinente a quel messaggio e non ad altri). Poiché cifrare ai soli fini di firma un intero messaggio è un'operazione onerosa in termini di calcolo, sono stati proposti metodi alternativi tra cui quello principale, legato all'algoritmo di cifratura RSA, prevede di cifrare con la chiave privata del mittente un 'riassunto' del messaggio, che è quindi un'informazione intimamente legata al messaggio stesso ma meno onerosa da cifrare. Sono stati proposti anche altri metodi, ad esempio quello legato all'algoritmo di ElGamal, quello di Schnorr e il DSS (Digital Signature Standard) proposto dall'americano NIST (National Institute of Standard and Technology) nel 1991. In queste note si tratterrà per semplicità solo il metodo RSA.

La firma può essere spedita assieme al messaggio a cui fa riferimento o anche separatamente (essendo il legame tra i due discendente dai rispettivi contenuti e non dalla compresenza nell'invio). Firma e messaggio, se spediti assieme, possono essere inviati in chiaro se interessa solo la sottoscrizione del messaggio, oppure in forma sicura cifrando il tutto con la chiave pubblica del destinatario.

## *5.1 Impronta hash*

Il riassunto del messaggio, che costituisce il contenuto della firma, è detto **impronta** del messaggio (in inglese ***fingerprint*** o anche ***digest***) ed è un'informazione ricavata dal messaggio ma di lunghezza prefissata, tipicamente un valore numerico di 128 o 160 bit. L'impronta viene usualmente calcolata applicando al messaggio una particolare funzione H non reversibile detta *funzione **hash***:

$$I = H(M)$$

Ad esempio, detto $m_i$ l'i-esimo byte di un messaggio di lunghezza L byte arbitraria, una funzione di questo tipo è la funzione che esegue il seguente calcolo:

$$I = (\Sigma i\ m_i) \bmod 2^k \qquad i:1..L$$

Nella funzione dell'esempio vengono sommati gli L byte e della somma si prendono i k bit meno significativi; l'impronta è in questo caso di k bit (lunghezza fissa, contro una lunghezza arbitraria del messaggio di L byte = L*8 bit).

Il fatto che la funzione hash sia non reversibile garantisce che, pur essendo applicabile a qualsiasi messaggio di qualsivoglia lunghezza (quindi di qualsiasi messaggio si può calcolare l'impronta), dall'impronta non è ricavabile il messaggio da cui è stata calcolata e quindi, di per sé, l'impronta non è una informazione da proteggere perché non lede la riservatezza del messaggio, e ha significato solo in quanto associata al messaggio che l'ha generata. La funzione hash deve anche garantire un'altra importante proprietà: deve essere molto bassa, quasi trascurabile, la probabilità che due messaggi diversi, in particolare se hanno la stessa lunghezza, generino la stessa impronta, ovvero si assume praticamente che:

$$I_1=H(M_1) \quad I_2=H(M_2) \quad M_1 \neq M_2 \ \Rightarrow \ I_1 \neq I_2$$

Questo garantisce che l'impronta di un messaggio sia un riassunto distintivo del messaggio stesso, una 'immagine fedele' ancorché ridotta, come lo può essere per un individuo l'impronta digitale. La bontà di un algoritmo di *hashing* sta quindi nella difficoltà crittoanalitica di trovare un messaggio diverso dall'originale ma che produce la stessa impronta: alcuni algoritmi di *hashing* sono in tal senso già stati violati.

Sono stati proposti svariati algoritmi che realizzano funzioni hash diverse (i primi tre dell'elenco in ambito RSA):

- MD2 (*message digest* 2): produce un'impronta a 128 bit, con il messaggio diviso in blocchi da 16 byte. È già stato violato.
- MD4: impronta da 128 bit, più veloce del precedente, opera su blocchi da 512 bit ed esegue il riempimento dell'ultimo blocco non completato anche un valore (sempre presente) di 64 bit che rappresenta la lunghezza effettiva del messaggio, cosa che rende molto più sicuro l'algoritmo; ciò nondimeno è stato violato.
- MD5: più sicuro del precedente, è basato su operazioni logiche e di OR esclusivo, ma rispetto a MD4 è più lento.
- SHA-1 (Secure Hash Algorithm): utilizzato nel protocollo S/MIME, derivato da MD4 e impronta da 160 bit.
- RIPE-MD: derivato da MD4 e SHA-1, ha varie versioni (impronta da 128, 160, 256 e 320 bit).

### *5.2 Integrità e autenticazione*

Quando un mittente X fa pervenire al destinatario Y sia il messaggio che la firma digitale (il tutto inviato in chiaro oppure cifrato), il destinatario Y può verificare l'integrità dell'invio. Infatti Y può decifrare l'impronta I del messaggio M applicando la chiave pubblica di X ($Kx_p$), ricalcolare l'impronta dal messaggio con lo stesso algoritmo applicato dal mittente (I*), e confrontare impronta ricalcolata (I*) e impronta ricevuta decifrata (I) per verificare che siano eguali (fig. 3). In caso affermativo, Y è praticamente certo che il messaggio pervenuto è nella sua forma originale: infatti in caso di corruzione del messaggio (per intrusione o per errore del canale di comunicazione) le due impronte (I e I*) sono quasi certamente diverse, grazie alle proprietà della funzione *hash*.

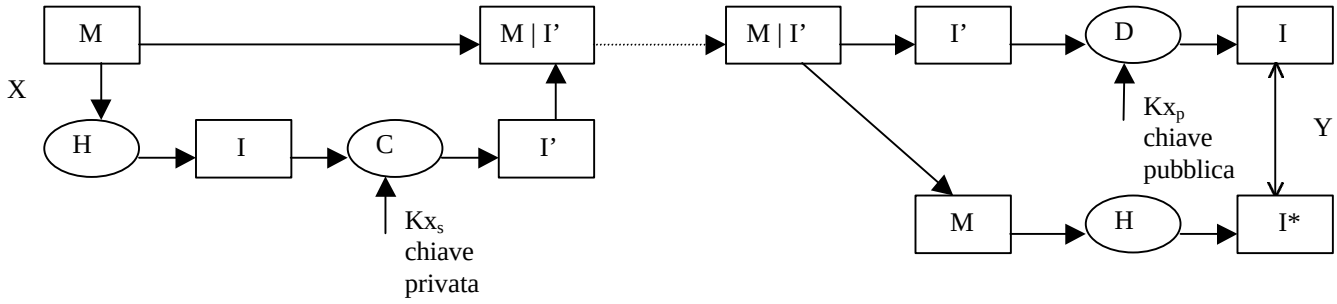



**Figura 3**

Inoltre, se Y è sicuro che la chiave pubblica $Kx_p$ 'appartiene' a X (cioè X è il depositario della corrispondente chiave privata $Kx_s$), allora l'eguaglianza delle due impronte garantisce anche che quel messaggio è stato spedito da X in quanto l'ha certamente sottoscritto con la sua chiave privata.

Assunto che la chiave privata venga gelosamente conservata dal legittimo possessore, che per altro può in ogni momento sostituirla, assieme a quella pubblica, con una nuova coppia di chiavi pubblica/privata, revocando la precedente chiave pubblica, rimangono aperte le questioni relative alla fidatezza delle chiavi pubbliche e al non ripudio, che vengono affrontate mediante l'istituzione delle autorità di certificazione.

# 6 Le Autorità di Certificazione

Se un mittente X non può ottenere direttamente da Y la chiave pubblica di quest'ultimo $Ky_p$, deve cercare di ottenerla da un terzo fidato W che faccia da garante. Questo dipende dalla fondamentale differenza che distingue la firma autografa da quella di tipo elettronico: la prima è direttamente riconducibile all'identità di chi l'ha prodotta, mentre la seconda non possiede questa proprietà

(anche se ne ha, come abbiamo visto, altre). Un modo pratico per superare il problema è richiedere che il garante sottoscriva la chiave $Ky_p$ con la propria firma, assunto naturalmente che X disponga della chiave pubblica di W $Kw_p$ ottenuta in modo fidato. Se anche questo non è vero, il problema si sposta coinvolgendo un altro come garante, e così via fino ad arrivare ad un garante fidato (cioè di cui si dispone di una chiave pubblica affidabile). Per svolgere questa funzione di garanzia in modo controllato e ad uso generale, sono state istituite le cosiddette **Autorità di Certificazione (AC)**. La loro responsabilità è di verificare l'identità degli utenti che registrano la propria chiave pubblica, generare, per il legittimo possessore e per chiunque ne faccia richiesta, documenti elettronici detti **certificati** che contengono la chiave pubblica sottoscritta dalla AC, mantenere aggiornate le liste degli utenti registrati per facilitarne la ricerca nonché la lista dei certificati revocati. All'estero talvolta le autorità coinvolte sono due, quella che registra l'utente (*Registration Authority*) verificandone l'identità, e quella che mantiene il *data base* delle chiavi e certificati (AC): il legislatore italiano ha rifiutato questo sdoppiamento di ruoli.

## *6.1 Registrazione di un utente ed emissione dei certificati*

La registrazione di un utente ha lo scopo di verificarne l'identità e di istituire tra utente e AC una connessione sicura per la trasmissione delle chiavi pubbliche da parte dell'utente. Questo secondo aspetto non deve stupire perché, pur essendo le chiavi pubbliche liberamente trasmissibili, la AC deve però assicurarsi che la chiave da inserire nelle liste provenga effettivamente dall'utente registrato, e ciò è ottenuto mediante l'invio su un canale sicuro 'personalizzato', ad esempio utilizzando un algoritmo di cifratura simmetrica con una chiave specifica per le comunicazioni AC/utente registrato. La registrazione avviene pertanto attraverso i seguenti passi:

1. l'utente fornisce, ai fini della sua identificazione, tutta la documentazione richiesta dalla AC;
2. la AC attribuisce all'utente 'validato' un identificatore univoco che faciliterà le successive operazioni di ricerca;
3. la AC inserisce l'utente nel *data base* degli utenti registrati;
4. la AC fornisce all'utente attraverso un canale sicuro la chiave che l'utente utilizzerà per la richiesta di certificazione delle sue chiavi pubbliche.

Ogni volta che l'utente genera una coppia chiave pubblica/chiave privata, le fasi da attuare per ottenerne la certificazione sono le seguenti:

1. l'utente invia in forma 'autenticata' la chiave pubblica in precedenza da lui generata, sottoscritta dalla firma ottenuta con la corrispondente chiave privata (questo dà garanzia che l'utente possieda effettivamente quest'ultima ma in più, essendo una sottoscrizione, difende l'utente da possibili modifiche della chiave pubblica presso la AC), effettuando l'invio cifrato con la chiave fornita dalla AC;
2. la AC genera il certificato che include: i dati dell'utente, compreso il suo identificativo, la sua chiave pubblica, la sua firma e la firma di autenticazione della AC, altre informazioni relative all'uso del certificato nonché il suo periodo di validità (fig. 4);
3. il certificato viene inviato all'utente;
4. l'inclusione del nuovo certificato nel o nei cataloghi gestiti dalla AC per un accesso di prelievo pubblico.

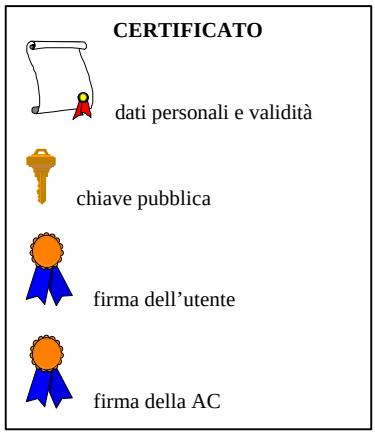



**Figura 4**

La firma della AC apposta al certificato deve essere naturalmente fidata: per questo anche le AC hanno un certificato pubblico che può essere autofirmato o firmato da una AC di livello superiore. Nel primo caso, il certificato deve essere stato ottenuto attraverso un canale sicuro; è prassi, ad esempio, includere nei programmi che fanno uso di queste tecnologie (ad esempio i *browser*) i certificati pubblici delle principali AC mondiali, mediante i quali eventualmente verificare certificati di AC secondarie e/o di utenti finali. Per l'Italia il ruolo principale è svolto dall'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) che pubblica documentazione tecnica e normative sull'argomento , e mantiene anche il registro pubblico dei certificatori italiani.

Il periodo di validità del certificato garantisce, ai fini della sicurezza, che una coppia chiave pubblica/privata 'scada' trascorso un certo tempo dalla sua generazione. Quando ciò accade, il certificato viene revocato, costringendo a quel punto l'utente a generare una nuova coppia di chiavi, e rendendo in questo modo meno probabili attacchi da parte di intrusi grazie al periodico rinnovo delle chiavi. Poiché la sicurezza è però strettamente legata anche al grado di segretezza con cui l'utente conserva la sua chiave privata valida, qualora egli per qualsiasi ragione ritenga non più sicuro l'utilizzo di questa chiave (per esempio ha dimenticato il supporto su cui era memorizzata in luogo accessibile e non sorvegliato per un certo tempo, oppure lo ha smarrito), può darne segnalazione alla AC che immediatamente provvede a dichiarare revocato il certificato anche se non scaduto.

Un certificato revocato dichiara non più autorizzato l'uso della corrispondente chiave pubblica da parte di potenziali mittenti, né di quella privata da parte del possessore ai fini di firma. Per rendere consapevoli tutti della revoca, la AC mantiene un catalogo dei certificati revocati: è responsabilità di un mittente verificare che, qualora sia in possesso della chiave pubblica del destinatario, questa non sia stata invalidata, controllando prima di usarla che il relativo certificato non sia stato nel frattempo revocato. Resta comunque valido, ai fini della verifica a posteriori della sottoscrizione, un certificato che, al momento della firma, fosse valido ma successivamente revocato. Per questo è conveniente mantenere collegati un messaggio firmato e il certificato del mittente valido al momento della firma.

Quando un mittente deve inviare un messaggio cifrato, si procura il certificato del destinatario da cui ricavare la chiave pubblica con cui cifrare il messaggio; se vi acclude la propria firma, conviene che il mittente vi aggiunga anche il proprio certificato per facilitare le operazioni di riconoscimento della firma da parte del destinatario.

Per garantire che varie applicazioni possano far uso agevolmente dei servizi di certificazione è stato sviluppato uno standard denominato **X.509**: grazie alla standardizzazione le informazioni vengono prodotte in formati riconoscibili e facilmente estensibili.

### *6.2 Servizio di marcatura temporale*

La garanzia del non ripudio da parte del mittente di un messaggio prodotto ed inviato al destinatario, non è ottenibile con la sola sottoscrizione del documento da parte del mittente, anche assumendo la validità del certificato che contiene la chiave pubblica del mittente e la sottoscrizione con la corrispondente chiave privata, perché manca la qualificazione temporale in forma fidata che, ovviamente, può essere fornita solo da una autorità terza. Per questo le AC svolgono solitamente anche un servizio di '**marcatura temporale**'. Esso consiste nei seguenti passi:

1. l'utente invia al servizio l'impronta del documento da marcare: questo non inficia la riservatezza del messaggio grazie alle proprietà dell'impronta, da cui non è possibile ricavare il messaggio stesso ma al quale è intimamente legata;
2. la marcatura dell'impronta consiste nell'aggiungere ad essa, da parte del servizio, data e ora;
3. l'impronta marcata viene cifrata con una chiave privata del servizio; il mittente e quello che sarà il destinatario del messaggio possono ricavare impronta e marcatura temporale decifrando con la chiave pubblica del servizio;
4. l'impronta marcata viene reinviata all'utente che la allega al messaggio.

Una volta inviati, in chiaro o cifrati, il messaggio, la firma del mittente e la corrispondente marcatura temporale, il mittente non potrà in alcun modo ripudiare tale invio (nemmeno parzialmente, dicendo che è avvenuto ma in altro momento) o sostituire messaggio e firma con altri in un momento successivo. Di norma, la AC usa chiavi diverse per la autenticazione e per la marcatura temporale.

## 7 La normativa italiana sulla firma digitale

L'Italia è stato uno dei primi paesi a dotarsi di un complesso normativo per la regolamentazione della firma digitale, prima ancora che si sviluppasse il commercio elettronico, col fine principale di semplificare le procedure burocratiche nei rapporti con la pubblica amministrazione e nella contrattistica. Le norme principali sono:

- Legge 15/3/1997 n.59 ("Bassanini")
  dà validità agli atti su supporto elettronico
- DPR 10/11/1997
  dà attuazione pratica alla legge 15/3/97 stabilendo in particolare il ruolo e la validità a fini legali della firma digitale
- Circolare AIPA 24/7/1998
  contiene regole tecniche per la validità degli atti su supporto ottico
- DPCM 8/2/1999
  contiene, nel suo allegato tecnico, le specifiche più importanti per la certificazione e la validazione temporale (algoritmi di generazione delle firme, tipologia delle chiavi, certificati, funzione delle AC, dispositivi di firma, criteri per la sicurezza, validazione temporale)
- Circolare AIPA 26/7/1999
  contiene requisiti degli aspiranti certificatori

Purtroppo in questa occasione il legislatore italiano ha preceduto quello europeo impostando la normativa con tutta una serie di precauzioni, adeguate probabilmente all'obiettivo di sostituire a tutti gli effetti atti cartacei con analoghi su supporto elettronico, ma secondo una impostazione eccessivamente restrittiva nell'ambito del commercio elettronico. Inoltre la normativa europea di riferimento, cioè la direttiva n. 99/93/CE, è alquanto diversa da quella italiana: per esempio, parla di **firma elettronica** e **firma elettronica avanzata,** la prima non generata con un sistema di 'firma sicura' (si pensi alla semplice sottoscrizione di un email) per la quale ogni legislazione nazionale può stabilire, caso per caso, il grado di validità in caso di controversia o giudizio; la seconda invece è più simile alla nostra firma digitale e viene assimilata alla firma autografa. Un'altra differenza riguarda i certificati, che per la direttiva europea sono pure di due tipi, 'semplici' e 'qualificati', questi secondi dotati di particolari caratteristiche e certificati da entità dotate di particolari requisiti. Ma questi requisiti sono di gran lunga meno restrittivi di quelli fissati dalla normativa italiana, che per i certificatori vuole società per azioni i cui amministratori devono avere un'onorabilità paragonabile a quella richiesta ai dirigenti bancari. Queste disuniformità dovranno essere in qualche modo sanate entro il 2001 e possono essere attualmente causa di freno nell'ampia adozione di queste metodiche e nel loro effettivo valore legale in Italia.

# 8 Protocolli di trasmissione sicuri

Il dialogo tra applicazioni in Internet richiede l'uso di protocolli standard che possono essere visti in forma stratificata (fig. 5). Ogni strato utilizza le funzioni degli strati sottostanti e fornisce funzioni a quelli soprastanti.

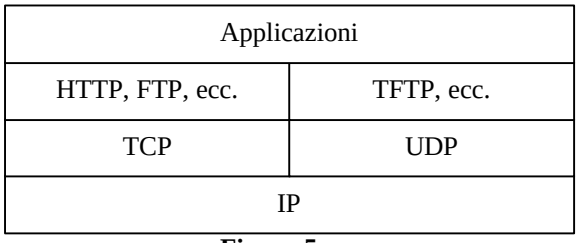



**Figura 5**

Quando due applicazioni o protocolli superiori vogliono comunicare via TCP (*Transmission Control Protocol*) devono aprire una connessione attraverso una porta denominata ***socket*** (questo temine traduce l'italiano 'presa'): una porta è univocamente identificata da un numero di IP (*Internet Protocol*) e da un numero di porta. Un numero di IP è a sua volta un identificativo da 32 bit, solitamente espresso come sequenza di 4 numeri compresi tra 0 e 255 (un numero per byte), ad esempio 147.162.2.100, mentre il numero di porta è un valore da 16 bit espresso come un singolo numero intero. I numeri di IP si possono ottenere anche indirettamente attraverso le funzioni di un DNS (*Domain Name Server*) che effettua la traduzione da nome simbolico di dominio (ad esempio www.dei.unipd.it) e numero di IP. Applicazioni standard lavorano su porte corrispondenti a numeri di norma predefiniti: ad esempio un web server su porta 80, un server telnet o SSH su porta 23, un server news su porta 119, ecc..

Per estendere questi protocolli a forme sicure che consentano alle applicazioni di comunicare in modo cifrato sicuro, si può agire a livello IP, a livello TCP o direttamente a livello delle applicazioni. Un interessante esempio della seconda categoria è **SSL (*Secure Socket Layer*)** e la sua versione Internet standardizzata **TLS (*Transport Layer Security*)**. SSL utilizza l'interfaccia dei *socket* per creare porte attraverso le quali la comunicazione avviene in forma cifrata. La variante di protocollo HTTP che fa uso di questi servizi per consentire una navigazione in forma sicura è chiamata HTTPS (fig. 6). Altre volte la sicurezza è inglobata direttamente all'interno delle applicazioni come nel caso di PGP e dei protocolli **SET (*Secure Electronic Transaction*)** e **S/MIME (*Secure Multipurpose Mail Extension*)**.

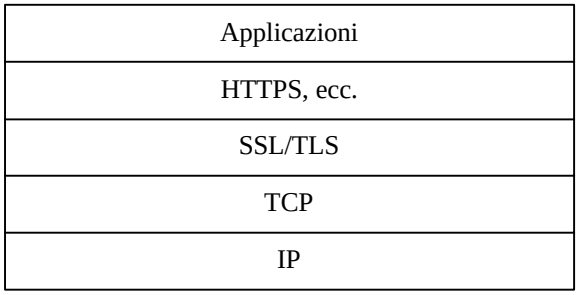



**Figura 6**

## *8.1 SSL (Secure Socket Layer)*

Si tratta di un protocollo creato da Netscape Communications Corporation per ottenere lo scambio sicuro di informazioni attraverso Internet. Esso garantisce:

- **Riservatezza**
  dopo la fase di contrattazione iniziale (*handshake*), i dati vengono trasmessi cifrati con algoritmi simmetrici (DES, RC4, 3DES, IDEA, FORTEZZA);
- **Autenticazione**
  l'identità dei soggetti può essere autenticata con l'uso di certificati e di algoritmi asimmetrici (RSA, DH);
- **Integrità**
  sono previsti controlli d'integrità dei dati via via trasmessi, controlli basati su MAC (*Message Authentication Code*) ottenuto con funzioni *hash* sicure quali SHA e MD5.

Nella fase di *handshake* viene stabilita una connessione con l'interlocutore e vengono concordati alcuni parametri che regoleranno il successivo scambio sicuro di informazioni durante tutta la sessione. Tra questi parametri vi sono: un identificatore di sessione, l'algoritmo da utilizzare per la cifratura di dati, quello per l'eventuale compressione dei dati, gli eventuali certificati. Terminata questa fase, ciascuno degli interlocutori disporrà di un *master secret* che è una chiave segreta da 48 byte da cui verranno ricavate le chiavi per la cifratura e per il calcolo del MAC; notare che, per ridurre alcune possibilità di attacco, la chiave usata per cifrare in un verso è diversa da quella usata per l'altro verso. Avviata la connessione, i dati da trasmettere vengono suddivisi in blocchi (max $2^{14}$ byte), ogni blocco viene prima compresso (se richiesto), viene calcolato il MAC del blocco e il tutto viene cifrato per essere passato al protocollo sottostante (TCP). Quando il blocco viene ricevuto, si procede alla verifica del MAC e successivamente alla sua decompressione.

## 8.2 S/MIME (Secure Multipurpose Mail Extension)

La specifica S/MIME, nata nel 1995 ad opera di RSA Data Security è finalizzata alla sicurezza della posta elettronica relativamente ai servizi di trasmissione, memorizzazione, autenticazione e trasferimento (*forwarding*). È stata successivamente rivista a fine di standardizzazione (1999). Trattandosi di un'estensione di MIME, può essere integrata nei diffusi programmi di posta e può garantire che il messaggio rimanga nella forma cifrata anche quando viene scaricato dal server di posta e memorizzato su disco locale. Prevede anche la possibilità della firma digitale del messaggio.

## 8.3 Telepay Light

È la naturale evoluzione di ***Telepay Classic***, una soluzione tecnologica proposta da **SSB (Società per i servizi bancari)** fin dal 1977 per i pagamenti elettronici sicuri con carta di credito. Gli attori coinvolti nel processo di pagamento sono:

- **Acquirente (*Cardholder*)**
  il possessore della carta di credito che vuole acquistare;
- **Emettitore della carta (*Issuer*)**
  l'istituto finanziario che emette la carta di credito e che garantisce il pagamento della transazione in accordo con le regole fissate dal circuito (es. VISA) a cui aderisce;
- **Venditore (*Merchant*)**
  mette a disposizione la merce del negozio virtuale;
- **Banca d'appoggio (*Acquirer)***
  istituto finanziario, con il quale è convenzionato il *Merchant*, che provvede alla ricezione, verifica ed effettuazione degli ordini di pagamento con carte di credito, eventualmente di vari circuiti;
- **Banca convenzionante *Telepay***
  istituto finanziario, collegato ad SSB, che accetta l'adesione del venditore al servizio *Telepay*.

*Telepay Light*, rispetto al *Classic*, non richiede né l'installazione di un *plug-in* (*wallet* - borsellino) sul sistema dell'acquirente (*Telepay Classic*, soluzione proprietaria basata su RSA a 1024 bit) né la registrazione di quest'ultimo; il sistema del venditore (sito di e-commerce e software collegato) non è obbligato a disporre di un POS virtuale per la richiesta di autorizzazione allo *Issuer*, in quanto questa è a carico di SSB. Il sistema dà egualmente una sicurezza sufficiente in quanto l'invio dei dati sensibili, in particolare i dati della carta, avviene con protocollo SSL a chiave segreta da 128 bit, e i dati della carta vengono impostati su un *form* che è presso il sistema SSB e a questo quindi inviati per la richiesta di autorizzazione: il venditore non riceve direttamente le informazioni sulla carta e quindi il suo sistema è concentrato sulla gestione dell'ordine (carrello, fidelizzazione del cliente registrato, offerte speciali, ecc.), mentre SSB garantisce come terzo l'autorizzazione al pagamento e, usualmente, funge anche da AC per i certificati di protezione. Attualmente *Telepay Light* supporta solo carte di credito ma è aperto ad altre forme automatiche di pagamento.

Il venditore può scegliere, all'atto della sottoscrizione con SSB, due diverse modalità per la autorizzazione (*on-line* o differita) e per la contabilizzazione (immediata o differita). Con la autorizzazione *on-line*, adeguata per un venditore che non deve fare verifiche di magazzino perché ha un magazzino ampio oppure fornisce servizi senza magazzino, SSB innesca immediatamente il processo di richiesta di autorizzazione allo *Issuer* e restituisce immediatamente l'esito; con la modalità differita, tale richiesta avviene previo consenso del venditore, che deve arrivare entro un tempo prestabilito all'atto della sottoscrizione (tipicamente qualche giorno), pena l'automatico annullamento dell'ordine: questo consenso viene inviato dal venditore tramite il SW di *Back-office* a cui egli ha accesso da remoto presso il sistema SSB. Nella contabilizzazione immediata, al termine della giornata in cui è avvenuta l'operazione autorizzata, SSB inoltra le informazioni per il regolamento contabile dell'operazione alla banca convenzionante e all'*Acquirer*; in quella differita, tale inoltro attende il consenso via *Back-office* dal venditore, entro il limite di tempo concordato, pena l'automatico annullamento. Nella fase di adesione, attraverso la banca convenzionante, SSB fornisce al venditore una chiave per l'autenticazione dell'esito nonché l'identificativo e il *password* per l'accesso al *Back-office*.

Le ti piche fasi di una transazione con *Telepay* si possono così riassumere:

1. l'acquirente accede al negozio virtuale e riempie il carrello della merce da acquistare, totalizzando la cifra da versare;
2. una volta verificati gli estremi d'ordine, l'acquirente lo conferma (di solito con la pressione di un apposito tasto dell'interfaccia Web);
3. il *browser* dell'acquirente viene ridirezionato dalla pagina del venditore verso una apposita pagina, protetta da SSL, del Web server SSB: questa pagina include alcuni dati riassuntivi dell'ordine, spediti in questa fase dal *server* del venditore, e deve essere riempita dall'acquirente con i dati della carta di credito;
4. se l'acquirente conferma i dati impostati, SSB li elabora, e se si opera in modalità di autorizzazione *on-line*, effettua la richiesta di autorizzazione al circuito della carta e ne dà l'esito all'acquirente; inoltre, a seconda della modalità scelta dal venditore, invia in modo contestuale, o meno, l'esito dell'operazione anche al *server* di quest'ultimo, in modo protetto dalla chiave fornita in fase di adesione; per l'autorizzazione differita, SSB si limita ad avvisare l'acquirente che ha preso in carico la richiesta e che questa sarà completata successivamente, cosa che all'acquirente sarà resa nota mediante email;
5. se la risposta è positiva, il *browser* dell'acquirente viene redirezionato, con un bottone di conferma, al sito del venditore per la conclusione della transazione, se nagativa, ritorna alla sezione del carrello.

Anche Banca Sella ha un servizio analogo indipedente.

## *8.4 SET (Secure Electronic Transaction)*

Formalizzato nel 1997, il protocollo SET è dovuto alla collaborazione di varie aziende del settore (Microsoft, IBM, Netscape, RSA, GTE, VISA, Mastercard, e altre) con l'obiettivo di rendere sicuri al massimo i pagamenti in rete con carte di credito. Gli obiettivi che il protocollo si prefigge sono:

- **Riservatezza**
  ottenuta mediante cifratura simmetrica dei dati sensibili ed in particolare del numero di carta di credito;
- **Integrità**
  ottenuta mediante firma digitale;
- **Autenticazione dell'acquirente**
  firma e certificato garantiscono il venditore dell'identità dell'acquirente e della validità della carta di credito in suo possesso;
- **Autenticazione del venditore**
  firma e certificato garantiscono l'acquirente dell'identità del venditore e della sua affidabilità;

Oltre agli attori già elencati nel caso di *Telepay Light*, è coinvolto nel processo di pagamento anche il **Servizio di Pagamento (*Payment Gateway*)** che è un dispositivo HW/SW che elabora le istruzioni di pagamento inviate dall'*Acquirer*. Tra i certificati coinvolti, quello dell'acquirente è emesso e firmato da un istituto finanziario (che funge quindi da AC) di cui l'acquirente è cliente; non contiene in chiaro i dati della carta di credito ma solo una impronta di questi, in modo che i dati stessi non siano ricavabili dal certificato, ma a chiunque vengano esplicitamente forniti dall'acquirente, questi possono essere collegati al certificato mediante confronto delle impronte. Esiste una forma ridotta di SET che non richiede questo certificato. Il certificato del venditore è solitamente emesso e firmato dall'*Acquirer* che in questo modo garantisce sull'identità del venditore e sulla possibilità di gestire correttamente le istruzioni di pagamento.

Si prevede che ogni partecipante disponga di due coppie di chiavi pubblica/privata, una riservata a firmare i dati (chiavi di firma), l'altra a proteggere lo scambio delle chiavi per gli algoritmi simmetrici di cifratura (chiavi di scambio), cui corrispondono i relativi certificati. Un pagamento si svolge attraverso due fasi: la richiesta di acquisto e l'autorizzazione di pagamento, gestite dai software utilizzati dai diversi attori in gioco.

Fasi della **richiesta di acquisto**:

1. L'acquirente invia al venditore l'informazione relativa al tipo di carta che intende usare.
2. In risposta a questa prima richiesta, il venditore invia all'acquirente un identificatore univoco assegnato alla transazione (TI), il proprio certificato per le chiavi di firma e quello del *Payment Gateway* per le chiavi di scambio, entrambi corrispondenti al tipo di carta comunicato.
3. Dopo aver verificato i certificati ricevuti, l'acquirente crea, aggiungendovi in entrambi il TI, gli estremi d'ordine (*order information* – OI), e gli ordini di pagamento (*Payment Instruction* – PI), questi secondi contenenti i dati della carta di credito. Le impronte degli OI e dei PI vengono concatenate, dalla concatenazione viene poi ricavata un'unica impronta, quest'ultima cifrata con la chiave privata dell'acquirente (quella di firma) a costituire una specie di 'firma doppia'. Viene quindi generata una chiave simmetrica casuale che viene usata per cifrare PI, l'impronta di OI e la firma complessiva prima calcolata. PI firmati e cifrati, e chiave simmetrica vengono cifrati con la chiave pubblica del *Payment Gateway* (quella di scambio). L'acquirente invia al venditore quest'ultima informazione cifrata assieme agli OI, all'impronta dei PI, alla sua firma 'doppia' e al suo certificato di firma.
4. Il venditore, verificato il certificato dell'acquirente, può verificare l'integrità del messaggio: calcola l'impronta di OI, la concatena con l'impronta di PI (che non deve e non può calcolare) ricevuta, calcola l'impronta di questa concatenazione e la confronta con quella ricevuta in modo cifrato come firma 'doppia' (la decifrazione è possibile grazie alla chiave pubblica dell'acquirente contenuta nel suo certificato ricevuto). Se quest'ultimo confronto dà esito positivo, il messaggio è integro. Allora il venditore elabora gli OI e, fatto questo, invia all'acquirente un messaggio firmato e cifrato con la propria chiave privata di firma a conferma dell'avvenuta ricezione della richiesta di acquisto.
5. L'acquirente, verificata l'integrità del messaggio di conferma ricevuto, verificandone la firma, lo salva opportunamente.

Fasi della **autorizzazione di pagamento**:

1. Al punto 4 del protocollo precedente il venditore provvede anche a generare e firmare una richiesta di autorizzazione che include l'ammontare della transazione e il suo TI. La richiesta viene cifrata con una chiave simmetrica casuale a sua volta cifrata con la chiave pubblica di scambio del *Payment Gateway*. La richiesta, assieme ai PI cifrati ricevuti dall'acquirente, vengono inviati al *Payment Gateway* assieme ad entrambi i certificati del venditore e a quello di firma dell'acquirente.
2. Quando il *Payment Gateway* riceve il messaggio, ne ricava la chiave simmetrica di cifratura decifrandola con la propria chiave privata di scambio. Decifra quindi la richiesta, controlla la validità del certificato di firma del venditore e, grazie a questo, verifica la validità della firma con cui il venditore a sottoscritto la richiesta. Quindi decifra con la propria chiave privata di scambio la chiave simmetrica con cui sono stati cifrati i PI e con questa decifra i PI stessi. Provvede poi a controllarne l'integrità confrontando la firma 'doppia' decifrata con il valore *hash* calcolato sulla concatenazione dell'impronta dei PI (da calcolare) e di quella degli OI (già disponibile). Quindi verifica che il TI ricevuto dal *Merchant* sia identico a quello contenuto nelle PI: se il

controllo dà esito positivo, invia una richiesta di autorizzazione allo *issuer* specificando i dati della carta (questa parte non è qui descritta, può essere gestita da un terminale virtuale POS). Ricevuta la risposta dallo *issuer*, il *Payment Gateway* genera e firma un messaggio di risposta all'autorizzazione che comprende il suo certificato di firma e la risposta dello *issuer*. Questo messaggio viene cifrato con una chiave simmetrica casuale e questa chiave viene cifrata con la chiave pubblica di scambio del *Merchant*. Il messaggio cifrato e chiave simmetrica cifrata vengono inviati al *Merchant*.

3. Il *Merchant* decifra la chiave simmetrica con la propria chiave privata e con la prima il messaggio ricevuto. Controlla quindi la validità del certificato di firma del *Payment Gateway* e, se tutto è ok, salva opportunamente la risposta ricevuta e provvede alla consegna della merce richiesta.

Si può notare come con il protocollo SET si sia realizzato un notevole salto di qualità nella sicurezza dei pagamenti con carta di credito, anche se la sua complessità ne limita al momento la diffusione e fa prevalere altre soluzioni più limitate (Telepay Light o addirittura il semplice invio via SSL del numero di carta al *Merchant*). V'è anche da notare il ruolo centrale svolto in questo protocollo dai certificati emessi in questo caso dagli istituti finanziari che svolgono quindi funzione di AC. In futuro, con le nuove versioni del protocollo, è previsto anche l'utilizzo di tecnologie più avanzate quali *smartcard* per aumentare il profilo di sicurezza di SET.

### *8.5 Altre forme di pagamento*

Sono state ideate anche altre forme di pagamento elettronico, basate sul concetto di **moneta virtuale**, alternative all'uso della carta di credito, che tra l'altro possono risolvere il problema che nasce quando la consistenza economica della transazione è paragonabile al costo 'finanziario' della stessa (ovvero nel caso di piccoli acquisti): si dispone infatti, in questo caso, di un **borsellino virtuale** paragonabile ad una carta a debito, da cui prelevare 'moneta' nella misura che serve di volta in volta fino ad esaurimento, cui fa seguito una ricarica. Un esempio di questo è **E-Cash** della DigiCash.

## APPENDICE

# 9 Cenni storici

### 9.1.1 Il primo cifrario

La più antica forma conosciuta di crittografia è la *scitala lacedemonica*, data da Plutarco come in uso dai tempi di Licurgo (IX sec a.C.) ma più sicuramente usata ai tempi di Lisandro (verso il 400 a.C.). Consisteva in un bastone su cui si avvolgeva ad elica un nastro di cuoio; sul nastro si scriveva per colonne parallele all'asse del bastone, lettera per lettera, il testo da rendere segreto. Tolto il nastro dal bastone, il testo vi risultava trasposto in modo regolare ma sufficiente per evitare la lettura senza un secondo bastone uguale al primo. Si tratta di una forma elementare di crittografia a **trasposizione**.

### 9.1.2 Cifrario di trasposizione

Come ulteriore esempio di cifrario basato sulla trasposizione dei caratteri di un testo si consideri il seguente.

Si sceglie una parola chiave di n caratteri (possibilmente senza doppie); si divide il testo in chiaro in gruppi di n caratteri, riempiendo eventualmente di x l'ultimo gruppo se incompleto, e si scrive il messaggio mettendo un gruppo per riga e incolonnando il tutto su n colonne. Si riordinano le colonne con gli stessi spostamenti che sarebbero necessari per ordinare alfabeticamente le lettere della parola chiave e si ottiene il messaggio cifrato leggendo le colonne così riordinate.

Esempio: `vieni subito`

Parola chiave: `rame`

```
r a m e
v i e n
i s u b
i t o x
```

Riordinamento:

```
a e m r
i n e v
s b u i
t x o i
```

Messaggio cifrato:

```
aistenbxmeuorvii
```

### 9.1.3 Cifrario basato su macchinario

Il primo esempio di cifratura basata su un 'macchinario' si può far risalire ad una testimonianza tra il 360 e il 390 dovuta ad Enea il tattico, generale della lega arcadica, in un trattato di cifre il cui XXI capitolo tratta appunto di messaggi segreti. In questo viene descritto un disco sulla zona esterna del quale erano contenuti 24 fori, ciascuno corrispondente ad una lettera dell'alfabeto. Un filo, partendo da un foro centrale, si avvolgeva passando per i fori delle successive lettere del testo: all'arrivo, riportate le lettere sul disco, si svolgeva il filo segnando le lettere da esso indicate; il testo si doveva poi leggere a rovescio. Le vocali spesso erano sostituite da gruppi di puntini.

### 9.1.4 Il Cifrario di Atbash

Un primo esempio di cifratura per **sostituzione** è il codice scriba ATBASH, utilizzato per cifrare il libro biblico di Geremia, codice per il quale ogni occorrenza nella frase di ciascuna lettera dell'alfabeto viene trasformata in altra lettera secondo una regola fissa. Nel codice Atbash la regola è molto semplice: la prima lettera viene sostituita dall'ultima dell'ordine alfabetico, la seconda dalla penultima e così via. Per il moderno alfabeto, questa regola è riassunta dalla tab. 1.

| **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** | 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 |

**Tabella 1**

### 9.1.5 La Scacchiera di Polibio

Il più antico codice poligrafico (sostituzione di tipo multiplo) è probabilmente la *scacchiera di Polibio*. Lo storico greco Polibio (~200-118AC), nelle sue Storie (Libro X) descrive un cifrario 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, secondo la descrizione di una scacchiera 5x5. Il messaggio veniva in tal modo trasmesso con due gruppi di cinque torce (p.es. 1,5 = una torcia accesa a destra, cinque a sinistra) e poteva essere qualsiasi e di qualsiasi lunghezza. Una scacchiera per l'alfabeto moderno (fondendo insieme i due caratteri poco frequenti k e q per ottenere in tutto 25 codici) è quella della tab. 2.

| # | 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 |

**Tabella 2**

Esempio:

```
v i e n i s u b i t o
5124153424434513244435
```

La scacchiera di Polibio ha alcune importanti caratteristiche, e cioè la riduzione nel numero di caratteri utilizzati nel messaggio cifrato, 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.

### 9.1.6 Il Codice di Cesare

Il famoso *codice di Cesare* è un classico esempio di codice a sostituzione mediante **trasposizione di lettera**: ciascuna lettera viene sostituita con quella ottenuta spostandola di un certo numero di posti (circolarmente) nella sequenza alfabetica. In origine il fattore di trasposizione era 3, ma una forma generalizzata può prevedere un fattore compreso tra 1 e 25 (per il moderno alfabeto di 26 lettere). Per il codice di Cesare di fattore 3 la codifica è quella di tab. 3.

| **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 |

**Tabella 3**

La frase dell'esempio precedente verrebbe codificata:

```
vienisubito
YLHQLVXELWR
```

### 9.1.7 Codici medioevali e il disco cifrante

Nel medioevo i cifrari sono soprattutto *monografici*: nomi e frasi convenzionali vengono sostituiti da simboli speciali.

Un altro noto cifrario basato su un macchinario fu il disco cifrante dovuto al famoso architetto L.B.Alberti: il disco era composto di due cerchi cifranti concentrici, uno esterno fisso con 24 caselle contenenti 20 lettere latine maiuscole (inclusa la Z, con U=V ed escluse H J K W Y) ed i numeri 1 2 3 4 per il testo in chiaro; ed uno interno mobile, con le 24 lettere latine minuscole per il testo cifrato. Le 20 lettere maiuscole erano messe in ordine alfabetico, mentre le 24 maiuscole erano in disordine, ciò costituendo un passo in avanti rispetto al codice di Cesare. Fissata una lettera maiuscola come indice (ad es. B), si doveva spostare il disco mobile interno e scrivere, come prima lettera del crittogramma, la lettera minuscola (nel nostro caso j) che corrispondeva alla B; quindi cifrare alcune parole con la lista risultante. I numeri 1 2 3 4 servivano da caratteri nulli. Quando si decideva di cambiare la lista cifrante, si scriveva la nuova lettera chiave in maiuscolo, in modo da indicare chiaramente al corrispondente il cambio di lista. Ciò fatto, si portava quella lettera ad affacciare l'indice B ed in questa nuova posizione si cifravano le altre parole secondo la nuova lista. Per aumentare la segretezza (le lettere maiuscole costituivano un aiuto non solo per il corrispondente ma anche per il "nemico"), l'Alberti suggeriva di usare uno dei quattro numeri per segnalare il cambio di alfabeto.

### 9.1.8 Il Cifrario bifido di Delastelle

Il *cifrario bifido di Delastelle* è un altro esempio di cifrario poligrafico e, come quello di Polibio, è basato su una matrice 5x5. Il metodo si articola in 3 passi:

1 Il messaggio in chiaro viene spezzato in blocchi di cinque caratteri ciascuno; se l'ultimo blocco non è esattamente di cinque, gli ultimi posti sono riempiti di X.

2 Ogni lettera del blocco viene cifrata con due cifre e cioè con l'indice di riga e l'indice di colonna, che vengono scritti in verticale.

3 Le cifre vengono ora riscritte in orizzontale, riga dopo riga, ottenendo un messaggio con un numero di cifre doppio dell'originale. A questo punto ogni coppia di numeri viene ritrasformata in lettera sempre secondo la matrice. Ne risulta il messaggio cifrato da trasmettere.

La matrice può essere quella semplice con le lettere dell'alfabeto ordinate (senza la W che può cifrarsi con una doppia V), oppure può essere ottenuta inserendo dapprima una parola chiave, depurata delle eventuali doppie, seguita da tutte le altre lettere dell'alfabeto in ordine.

Esempio: parola chiave COMPUTER

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

**Tabella 4**

```
v i e n i   s u b i t   o x x x x
5 3 2 4 3   5 1 2 3 2   1 5 5 5 5
2 5 2 4 5   1 5 5 5 1   2 3 3 3 3


53 24 32 52 45   51 23 21 55 51   15 55 52 33 33
X  A  F  V  Q    S  R  T  Z  S    U  Z  V  G  G
```

La decifratura avviene applicando il procedimento inverso con la medesima tabella che, come nei casi simili precedenti, deve quindi essere già nota al destinatario (in pratica, la chiave è proprio la parola chiave).

```
X A F V Q   S R T Z S   U Z V G G
5324325245  5123215551  1555523333

5 3 2 4 3   5 1 2 3 2   1 5 5 5 5
2 5 2 4 5   1 5 5 5 1   2 3 3 3 3

5235224435  5115253521  1253535353
v i e n i   s u b i t   o x x x x
```

### 9.1.9 Dal secolo XIX alla Grande Guerra

Dalla metà del XIX secolo l'uso della crittografia assume un ruolo determinante nella trasmissione di messaggi di carattere logistico e strategico. Con l'invenzione della radio i messaggi sono trasmessi anche via etere e quindi esposti molto più di prima all'intercettazione da parte del nemico; il ricorso alla crittografia diventa inevitabile, come la necessità di cifrari sempre più sofisticati. Una necessità che è ignorata in Italia dove si dovrà attendere l'entrata in Guerra nel 1915 per rendersi conto del ritardo accumulato in campo crittografico, e porvi rimedio.

Tra i metodi usati nella Grande Guerra si possono citare:

- Playfair cipher (1854)

- Cifra campale germanica (1918)

- Il cifrario bifido di Delastelle

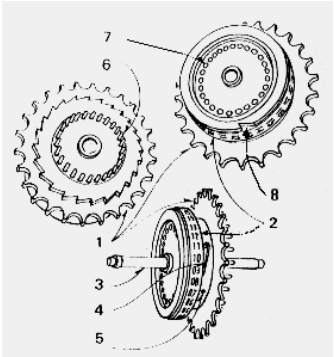
### 9.1.10 La macchina Enigma

Nel 1918 Arthur Scherbius inventò a Berlino una macchina di cifratura che applicava ripetutamente sostituzioni e trasposizioni dei singoli caratteri di un messaggio. Con l'aggiunta di alcune parti (il riflettore e di un'ulteriore trasposizione ottenuta con connessioni manuali sul frontale), la macchina è stata utilizzata anche per le operazioni militari della seconda guerra mondiale.

Ogni sostituzione era ottenuta con l'uso di un insieme di connessioni elettriche che collegavano una coppia di contatti: ogni contatto corrisponde ad una lettera e ciascuna connessione era interpretabile come la trasformazione di una lettera in chiaro nella corrispondente lettera cifrata. Le connessioni erano collocate all'interno di un dispositivo rotante detto rotore (fig. 7). Nel corso degli anni sono stati costruiti 10 tipi di rotori (I..VIII, Beta, Gamma), ciascuno con la propria specifica mappa di sostituzione.

Una sostituzione può essere descritta dalla fig. 8, ove compare solo una parte delle 26 connessioni: in figura la lettera Q viene sostituita con M e M con R.

1 anello per la rotazione manuale
2 l'alfabeto (in numeri da 1 a 26)
3 asta di supporto
4 blocco dell'anello d'alfabeto rispetto al corpo delle le connessioni
5 corpo con le connessioni elettriche
6 contatti mobili verso il rotore precedente
7 contatti verso il rotore successivo
8 aggancio solidale all'anello per l'avanzamento da imprimere al rotore successivo



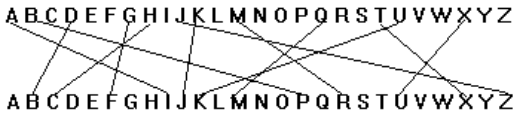
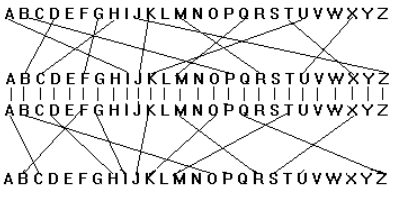




**Figura 7** **Figura 8**

La macchina era dotata di una tastiera con le 26 lettere e di una batteria di 26 lampadine, ciascuna illuminante una lettera diversa. Se si fosse collegato un capo dell'interruttore di ciascun tasto con una batteria e l'altro con il corrispondente contatto della riga superiore del dispositivo di sostituzione di fig. 8, una volta collegati i contatti della riga inferiore alle corrispondenti lampadine, il cui secondo contatto era in comune collegato all'altro polo della batteria, la pressione del tasto Q avrebbe fatto accendere la lampadina M.

La macchina, per aumentare il numero di combinazioni possibili, includeva una serie di ulteriori complicazioni. Intanto, faceva uso della serie di più rotori, basati su una mappa di sostituzione tra loro diversa, in modo da ottenere una sostituzione composta. Ad esempio (fig. 9) con due dispositivi si otteneva una trasformazione complessiva per la quale Q si trasformava in R passando per M. Per evitare che la serie dei due dispositivi avesse lo stesso effetto di un unico dispositivo realizzante la sostituzione complessiva, la connessione tra due rotori adiacenti poteva subire uno scorrimento circolare, corrispondente ad una trasposizione di un certo numero di caratteri, nell'intervallo 0..25 (fig. 10). In questo modo la serie dei due dispositivi produceva una trasformazione complessiva costituita da due trasposizioni, una in avanti e una indietro dello stesso fattore, dipendente dalla posizione mutua regolabile, e due sostituzioni indotte dalle mappe dei rotori..



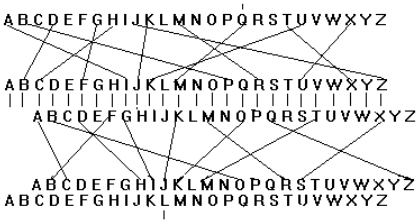




**Figura 9** **Figura 10**

Per l'esempio di fig. 10, il carattere Q si trasformava in L passando per M (sost.), K (trasp. indietro di 2), J (sost.) e infine L (trasp. in avanti di 2, opposta alla precedente). La macchina utilizzata nella seconda guerra mondiale disponeva di 3 di questi dispositivi rotativi (rotori) messi in serie, il primo dei quali poteva ruotare rispetto ai contatti di ingresso che erano montati su un disco d'ingresso fisso (fig. 11), cosa che realizzava una ulteriore trasposizione.

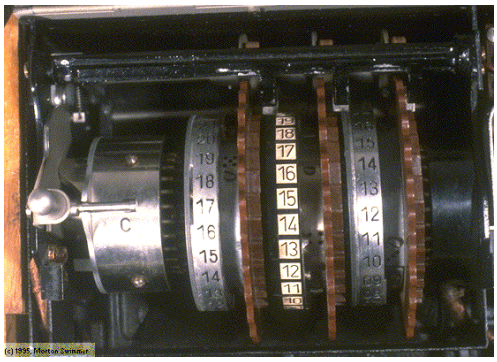


**Figura 11**

L'uscita dell'ultimo rotore, anziché costituire la versione cifrata della lettera iniziale, veniva fatta pervenire ad un altro componente (il 'riflettore', di cui esistevano 4 tipi, B, C, B Dünn, C Dünn) che provvedeva semplicemente ad uno scambio tra le lettere di 13 coppie prefissate (del tipo A↔Y cioè A→Y e Y→A): il risultato di questa ulteriore sostituzione a regola fissa veniva sottomesso in verso contrario alla sequenza dei 3 rotori (si può facilmente verificare che, grazie allo scambio, in questo percorso all'indietro venivano interessate connessioni elettriche diverse da quelle attraversate dalla corrente nel primo tratto diretto dal tasto al riflettore) e la corrente catturata dal primo rotore (cioè l'ultimo percorso all'inverso). Ciò che si ottiene, grazie a questa 'riflessione', è un principio di reciprocità.

Ad esempio, facendo riferimento alla tab. 5, che descrive la trasformazione indotta da ciascun tipo di rotore impostando l'allineamento dell'anello d'alfabeto ad A e il fattore di trasposizione a 0 (cioè A o 1 nella specifica della macchina), la trasformazione del riflettore e la posizione dell'aggancio di avanzamento, e scegliendo una della combinazioni possibili (stesso allineamento A degli anelli per i 3 rotori, destra rotore III con fattore trasposizione 0; centro rotore II fattore trasp. 2, sinistra rotore I fattore trasp. 4, riflettore B, nessuna connessione esterna), la sequenza di trasformazioni per due lettere A battute di seguito è la seguente (→si→ sostituzione rotore i, →sir→ sostituzione rotore i inversa, →ti→ trasposizione rotore i in ingresso, →tir→ trasposizione rotore i in uscita, →r→ riflessione):

A →t3→ B →s3→ D →t3r→ C →t2→ E →s2→ S →t2r→ Q →t1→ U →s1→ A →t1r→ W →r→ V →t1→ Z →s1r→ J →t1r→ F →t2→ H →s2r→ L →t2r→ J →t3→ K →s3r→ U →t3r→ T

A →t3→ C →s3→ F →t3r→ D →t2→ F →s2→ I →t2r→ G →t1→ K →s1→ N →t1r→ J →r→ X →t1→ B →s1r→ W →t1r→ S →t2→ U →s2r→ H →t2r→ F →t3→ H →s3r→ D →t3r→ B

Si noti che, prima di ciascuna trasformazione, il rotore a destra viene avanzato di una posizione, incrementando conseguentemente il fattore di trasposizione, e che, dopo la riflessione, occorre applicare la mappa inversa. La posizione dell'aggancio di avanzamento dei 3 rotori e la trasposizione iniziale sono tali da non far avanzare il rotore centrale e quello a sinistra durante la cifratura dei due caratteri.

Applicando la macchina a partire dalla stessa configurazione iniziale per decifrare, si ottiene:

T →t3→ U →s3→ K →t3r→ J →t2→ L →s2→ H →t2r→ F →t1→ J →s1→ Z →t1r→ V →r→ W →t1→ A →s1r→ U →t1r→ Q →t2→ S →s2r→ E →t2r→ C →t3→ D →s3r→ B →t3r→ A

B →t3→ D →s3→ H →t3r→ F →t2→ H →s2→ U →t2r→ S →t1→ W →s1→ B →t1r→ X →r→ J →t1→ N →s1r→ K →t1r→ G →t2→ I →s2r→ F →t2r→ D →t3→ F →s3r→ C →t3r→ A

| **INPUT** | **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** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Rotore I | E | K | M | F | L | G | D | Q | V | Z | N | T | O | W | Y | H | X | U | S | P | A | I | B | R | C | J |
| Rotore II | A | J | D | K | S | I | R | U | X | B | L | H | W | T | M | C | Q | G | Z | N | P | Y | F | V | O | E |
| Rotore III | B | D | F | H | J | L | C | P | R | T | X | V | Z | N | Y | E | I | W | G | A | K | M | U | S | Q | O |
| Rotore IV | E | S | O | V | P | Z | J | A | Y | Q | U | I | R | H | X | L | N | F | T | G | K | D | C | M | W | B |
| Rotore V | V | Z | B | R | G | I | T | Y | U | P | S | D | N | H | L | X | A | W | M | J | Q | O | F | E | C | K |
| Rotore VI | J | P | G | V | O | U | M | F | Y | Q | B | E | N | H | Z | R | D | K | A | S | X | L | I | C | T | W |
| Rotore VII | N | Z | J | H | G | R | C | X | M | Y | S | W | B | O | U | F | A | I | V | L | P | E | K | Q | D | T |
| Rotore VIII | F | K | Q | H | T | L | X | O | C | B | J | S | P | D | Z | R | A | M | E | W | N | I | U | Y | G | V |
| Rotore Beta | L | E | Y | J | V | C | N | I | X | W | P | B | Q | M | D | R | T | A | K | Z | G | F | U | H | O | S |
| Rotore Gamma | F | S | O | K | A | N | U | E | R | H | M | B | T | I | Y | C | W | L | Q | P | Z | X | V | G | J | D |

| | |
|---|---|
| riflettore B | (AY) (BR) (CU) (DH) (EQ) (FS) (GL) (IP) (JX) (KN) (MO) (TZ) (VW) |
| riflettore C | (AF) (BV) (CP) (DJ) (EI) (GO) (HY) (KR) (LZ) (MX) (NW) (TQ) (SU) |
| riflettore B Dünn | (AE) (BN) (CK) (DQ) (FU) (GY) (HW) (IJ) (LO) (MP) (RX) (SZ) (TV) |
| riflettore C Dünn | (AR) (BD) (CO) (EJ) (FN) (GT) (HK) (IV) (LM) (PW) (QZ) (RX) (UY) |

| | |
|---|---|
| Rotore I | avanzamento del successivo su R |
| Rotore II | avanzamento del successivo su F |
| Rotore III | avanzamento del successivo su W |
| Rotore IV | avanzamento del successivo su K |
| Rotore V | avanzamento del successivo su A |
| Rotori VI, VII and VIII | avanzamento del successivo su A and su N |

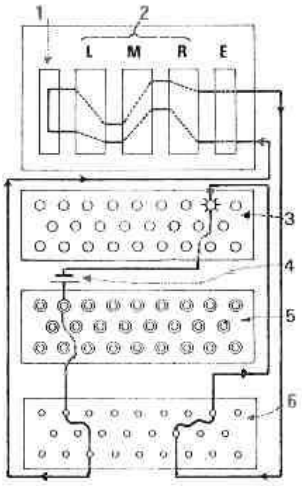
(i rotori beta e gamma, collocabili solo come 4 e ultimo rotore, non provocano avanzamenti)

**Tabella 5**

Si potrebbe verificare che, di converso, nella stessa configurazione iniziale dei rotori, la lettera T verrebbe cifrata con A. Questo garantiva di poter usare un'altra macchina del tutto eguale anche per decifrare, ponendo i rotori nella medesima posizione di quelli usati nella macchina di cifratura e battendo il tasto corrispondente al carattere cifrato, ottenendo l'accensione della lettera originaria. Nel 1938 erano disponibili 6 rotori con collegamenti diversi: era pertanto possibile, scegliendone 3 e posizionandoli nella macchina in un certo ordine, ottenere una di 60 configurazioni diverse (tante quante sono le combinazioni di 3 numeri ordinati su un insieme di 6).

La versione militare disponeva di un'ulteriore complicazione, costituita una serie di contatti esterni mediante i quali era possibile effettuare una ulteriore sostituzione per scambio di 10 coppie di caratteri (6 caratteri non venivano sostituiti) che interessava sia il collegamento dalla tastiera al disco di ingresso ai rotori, sia dal percorso di ritorno verso la lampadina (figg. 12, 13). Lo scambio veniva fissato dall'operatore con connessioni manuali che rimanevano fisse una volta fissati i connettori (e quindi mantenendo il principio di reciprocità della trasformazione complessiva).

L'ulteriore importante caratteristica della macchina era che i rotori potevano ruotare durante la cifratura di una sequenza di caratteri: prima di essere usati per la trasformazione di ciascun carattere, il primo rotore veniva spostato di una posizione in avanti dalla pressione del tasto, il secondo se il primo aveva fatto un giro completo, il terzo se lo aveva fatto il secondo (come un contachilometri). Il punto di avanzamento impresso al rotore successivo dipendeva dalla posizione dell'aggancio solidale all'anello dell'alfabeto, anello che poteva essere fatto girare rispetto al corpo delle connessioni prima che il rotore fosse messo in posizione nella macchina (vedi fig. 7). In questo modo ogni tasto era sottoposto ad una trasformazione diversa rispetto a tasti successivi, dovuta al diverso modo in cui i rotori si presentavano al contatto con i dischi/rotori adiacenti. La trasformazione complessiva era pertanto determinata dalla combinazione iniziale dei rotori che, in pratica, costituiva la chiave di cifratura, mentre i dettagli costruttivi della macchina e le modalità di collegamento costituivano l'algoritmo di cifratura applicato. Si può dimostrare che, tenendo conto di tutte le possibili configurazioni iniziali (rotori scelti, posizionamento mutuo dei rotori nella macchina, posizione iniziale di ciascun rotore e dell'anello dell'alfabeto, collegamenti esterni) il numero di combinazioni possibili (ovvero della chiave) è dell'ordine di $1.5*10^{20}$. Questo fatto faceva ritenere ai suoi utilizzatori la macchina del tutto sicura. Periodicamente, attraverso canali sicuri, venivano trasmesse tabelle che mostravano la scelta giornaliera dei rotori, la loro predisposizione iniziale dell'anello d'alfabeto, l'insieme di contatti esterni, ma non la trasposizione iniziale, cioè la posizione dei rotori una volta incastrati all'interno della macchina. Questa posizione doveva essere diversa all'inizio di ogni messaggio: per questo nel preambolo del messaggio veniva spedito in chiaro una sequenza di 3 trasposizioni (ad esempio BBD per i fattori di trasposizione 1,1,3, corrispondenti alle cifre 2,2,4 dell'anello d'alfabeto che emergevano dalle finestrelle della copertura della macchina) e, ponendo la macchina in questa configurazione, iniziale si cifrava due volte, e si spediva quindi cifrata, la configurazione iniziale da adottare per cifrare il messaggio vero e proprio. Ciò bastava per ottenere una cifratura a chiave segreta di messaggi di lunghezza arbitraria che, nella forma cifrata, ad esclusione dei primi 3 caratteri del preambolo, venivano spediti per radio via alfabeto morse e decifrati con una macchina dello stesso tipo.




1 riflettore
2 rotori
3 banco lampadine
4 batteria
5 tastiera
6 connessioni esterne

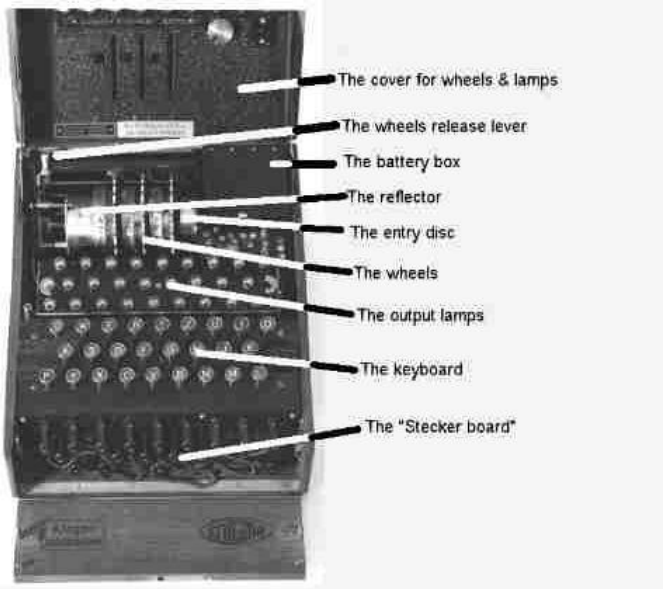



**Figura 12** **Figura 13**

L'algoritmo di cifratura presentava, dal punto di vista crittoanalitico, 4 lati deboli: il principio di reciprocità, l'impossibilità di cifrare alcuna lettera con se stessa, la posizione d'aggancio di avanzamento rispetto all'anello d'alfabeto che era diversa per ciascun tipo di rotore, e la cifratura 2 volte nel preambolo della medesima sequenza di 3 caratteri. Queste debolezze furono sfruttate dapprima dai ricercatori polacchi che si erano impadroniti, già prima della guerra, di un esemplare della macchina, e soprattutto dal gruppo inglese che durante la guerra lavorò a Bletchley Park sotto la guida del famoso teorico Alan Turing che, utilizzando una apparecchiatura che

in qualche modo costituiva un computer primordiale (denominato 'Colossus') riuscì a scoprire una tecnica di attacco in grado di decifrare il messaggio. Per alcuni questo risultato fu una delle cause principali della sconfitta tedesca.

# 10 PGP (*Pretty Good Privacy*)

Questa applicazione, pensata all'inizio degli anni '90 da Philip Zimmermann e freeware, include sostanzialmente tutte le funzionalità descritte sopra e agevola la gestione delle chiavi. È disponibile per molte piattaforme (Windows, OS/2, Mac, Amiga, Unix/Linux, Vms, ecc.) e per Unix anche in formato sorgente modificabile. Esiste come plug-in di alcuni diffusi client di posta elettronica.

Rispetto a quanto detto in precedenza, PGP apporta alcune varianti tecnicamente giustificate: in particolare, per motivi di efficienza legati alla durata della cifratura asimmetrica nel caso di lunghi messaggi, per la cifratura del messaggio viene utilizzato un più veloce algoritmo simmetrico utilizzando, come chiave segreta, una chiave casuale generata dal mittente all'atto dell'invio, chiave che viene cifrata con la chiave pubblica del destinatario. L'utente X che vuole inviare a Y il messaggio M effettua questi passaggi:

1. Viene utilizzato l'algoritmo MD5 per calcolare l'impronta del messaggio lunga 160 bit, ovvero I = MD5(M): il codice così ottenuto viene cifrato via RSA con la chiave privata del mittente $Kx_s$ e concatenato al messaggio, ottenendo M' = M || C(I, $Kx_s$).
2. M' viene compresso con un algoritmo di tipo zip in modo da ridurne reversibilmente la lunghezza, ovvero M" = ZIP(M').
3. Viene generato un numero casuale C di 128 bit denominato *session key*: esistono appositi algoritmi, da tempo disponibili, per ottenere una sequenza di numeri pseudocasuali caratterizzata da determinate proprietà statistiche; nel caso presente i numeri generati in una sequenza devono essere equiprobabili (come dire, nel caso dei numeri da 1 a 6, come se si tirasse ogni volta un dado).
4. Viene applicato l'algoritmo di crittografia convenzionale IDEA utilizzando come chiave il *session key* C, ottenendo Mc = IDEA(M", C). Rispetto ad un algoritmo di crittografia con chiave asimmetrica, l'algoritmo IDEA comporta un onere computazionale inferiore e quindi riesce a cifrare in tempi brevi, sebbene con un livello di sicurezza modesto, anche messaggi molto lunghi.
5. La chiave C viene cifrata con l'algoritmo per crittografia a chiave asimmetrica RSA (oppure con l'algoritmo Diffie-Hellman/DSS) utilizzando come chiave la chiave pubblica del destinatario $Ky_p$ e il risultato concatenato al messaggio, ottenendo Mx = Mc || RSA (C, $Ky_p$). Essendo RSA un algoritmo ad elevato livello di sicurezza, tanto maggiore quanto è più lunga la chiave $Ky_p$, è quindi computazionalmente più oneroso di un algoritmo per crittografia convenzionale ma applicato ad una informazione compatta quale C (che, come detto, ha lunghezza fissa di appena 128 bit).
6. Viene infine applicato su Mx l'algoritmo di trasformazione reversibile a testo ASCII denominato Armor Radix-64 che produce un messaggio di tipo testuale composto solo da codici ASCII, ottenendo Ax = AR64(Mx). Ax sarà il messaggio effettivamente spedito attraverso il canale non sicuro e la sua forma di testo ASCII ne rende facile la manipolazione da parte di tutti i client e server di posta elettronica.

L'interfaccia di PGP consente di decidere se firmare o meno il messaggio, se trasformarlo o meno in un testo ASCII, e altre opzioni. PGP è anche dotato di alcune funzioni ausiliarie per la gestione delle chiavi. Consente di generare coppie di chiavi pubblica/privata, generazione protetta da "frasi chiave" (*passphrase*) per aumentarne il grado di fidatezza. L'archivio di chiavi può essere memorizzato su file, possibilmente su supporto removibile per una conservazione 'sicura'. Sarà anche cura dell'utente evitare la divulgazione della *passphrase* che può rendere accessibile l'archivio privato delle chiavi. In merito al grado di sicurezza si deve anche tenere presente che la legge americana da tempo fa equivalere l'esportazione di metodi di crittografia con chiavi superiori ad un certo numero di bit (crittografia forte) all'esportazione di armi, perché ritenuta un pericolo per la sicurezza nazionale: questo ha prodotto la necessità di rendere disponibili due versioni del programma, una ad uso interno in USA e uno per l'esportazione.

La chiave pubblica può essere anche agevolmente spedita a uno o più siti di raccolta (*keyserver*) per la sua pubblicità. Molti *keyserver* sono collegati fra loro e si scambiano automaticamente le chiavi, evitando che gli utenti debbano provvedere esplicitamente a questa replicazione. I *keyserver* non sono però normalmente autorità di certificazione e quindi l'identificazione del destinatario non è in questo caso garantita.

Un'ultima accortezza riguarda il programma PGP stesso che potrebbe essere ottenuto in una versione maliziosamente modificata al fine di spedire di nascosto a terzi l'archivio personale delle chiavi: ci si accerti pertanto di scaricare il programma da siti ufficiali che diano un minimo di garanzia sotto questo aspetto.