

Una introduzione alla Crittografia

1. DEFINIZIONE di Crittografia (o crittografia)

DEFINIZIONE (DA “IL VOCABOLARIO DELLA LINGUA ITALIANA” DEVOTO-OLI): *s.f.* **1.** Scrittura convenzionale segreta, che può essere decifrata solo da chi sia a conoscenza del codice. **2.** Tipo di rebus che si risolve se vengono considerati come un unico assieme tutti i segni tipografici (lettere e figure) presentati. **3. estens.** Testo oscuro, di non facile interpretazione. [Comp. di *critto-* e *-grafia*]

2. Il Cifrario di Cesare

Un esempio di crittografia impiegata in passato è il Cifrario di Cesare. Consiste nell’associare una lettera dell’alfabeto con quella che la segue di 3 posizioni: alla lettera A è associata la D, e così via, considerando inoltre la lettera A successiva alla Z.

Alfabeto: ABCDEFGHILMNOPQRSTUVWXYZ
Alfabeto cifrato: DEFGHILMNOPQRSTUVWXYZABC

Il Cifrario di Cesare si basa sul principio della sostituzione con una traslazione di ordine 3. La chiave è costituita dal numero indicante le posizioni con il quale spostare le lettere per codificare e decodificare il messaggio.

Un esempio è il seguente:

Testo in chiaro: CIAO

Testo cifrato: FNDR

Conoscendo l’alfabeto è possibile arrivare all’alfabeto cifrato per tentativi, ne bastano 20, e decriptare il messaggio (operando a “forza bruta”).

Una introduzione alla Crittografia

3. Crittografia simmetrica

In un algoritmo *simmetrico* la medesima chiave è utilizzata sia per cifrare il messaggio sia per decifrarlo, mediante la trasformazione inversa di quella impiegata per la cifratura. In Figura 1 è rappresentata la modalità di comunicazione tra un mittente ed un destinatario che impiegano un algoritmo simmetrico. Il mittente codifica il messaggio in chiaro usando la chiave segreta, spedisce il messaggio cifrato ottenuto al destinatario, che estrae il messaggio originale usando ancora la chiave segreta.

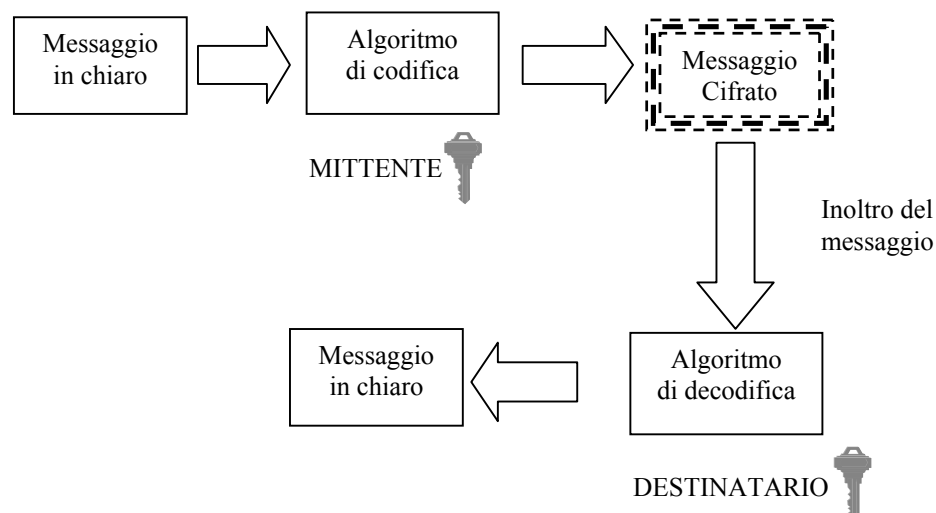


Figura 1. Modalità di comunicazione con un algoritmi simmetrico

Il problema di fondo degli algoritmi simmetrici è la comunicazione della chiave tra mittente e destinatario. Solo e soltanto loro devono conoscere tale chiave, altrimenti la riservatezza (confidenzialità) può decadere.

Un altro problema riguarda il numero di chiavi necessarie affinché un gruppo di n persone possa comunicare tra loro in modo “sicuro” : $[n * (n-1)]/2$, ogni coppia di utenti deve condividere una chiave segreta.

Una introduzione alla Crittografia

4. L'algoritmo Data Encryption Standard

Negli anni '70 IBM sviluppò l'algoritmo *Data Encryption Standard* (DES). Esso utilizza una chiave a 56 bit, che consente un numero di combinazioni pari a 2^{56} , circa 72 milioni di miliardi. Per molti anni l'uso di DES con chiave a 56 bit è stato ritenuto inviolabile, ma nel 1998 un calcolatore da 250.000 dollari è riuscito a decodificare, in circa 60 ore, un messaggio cifrato con DES. Per garantire la riservatezza dei messaggi cifrati con algoritmi simmetrici occorre allora aumentare la dimensione della chiave, ad esempio 128 bit.

Lo schema di Figura 2 mostra il funzionamento dell'algoritmo. Il generico messaggio da codificare deve essere suddiviso in blocchi di 64 bit, e ciascuno di questi viene codificato mediante una chiave a 56 bit. Ogni blocco codificato ha dimensione di 64 bit. Per ottenere il corrispondente blocco cifrato, il generico blocco di 64 bit del messaggio subisce le seguenti elaborazioni:

- permutazione: (cioè ogni bit viene sostituito con un altro, che si trova spostato rispetto al primo di un certo numero di posizioni),
- cifratura: 16 volte in modo iterativo attraverso una funzione della chiave a 56 bit;
- scambio dei 32 bit più significativi (quelli più a sinistra) con gli ultimi 32 bit;
- permutazione.

Ciascuna iterazione è un insieme di operazioni svolte su blocchi di 48 bit. Tra le operazioni esiste la funzione S-BOX, elaborata da IBM, che dato un blocco in ingresso di 48 bit restituisce un output di 32 bit.

Una introduzione alla Crittografia

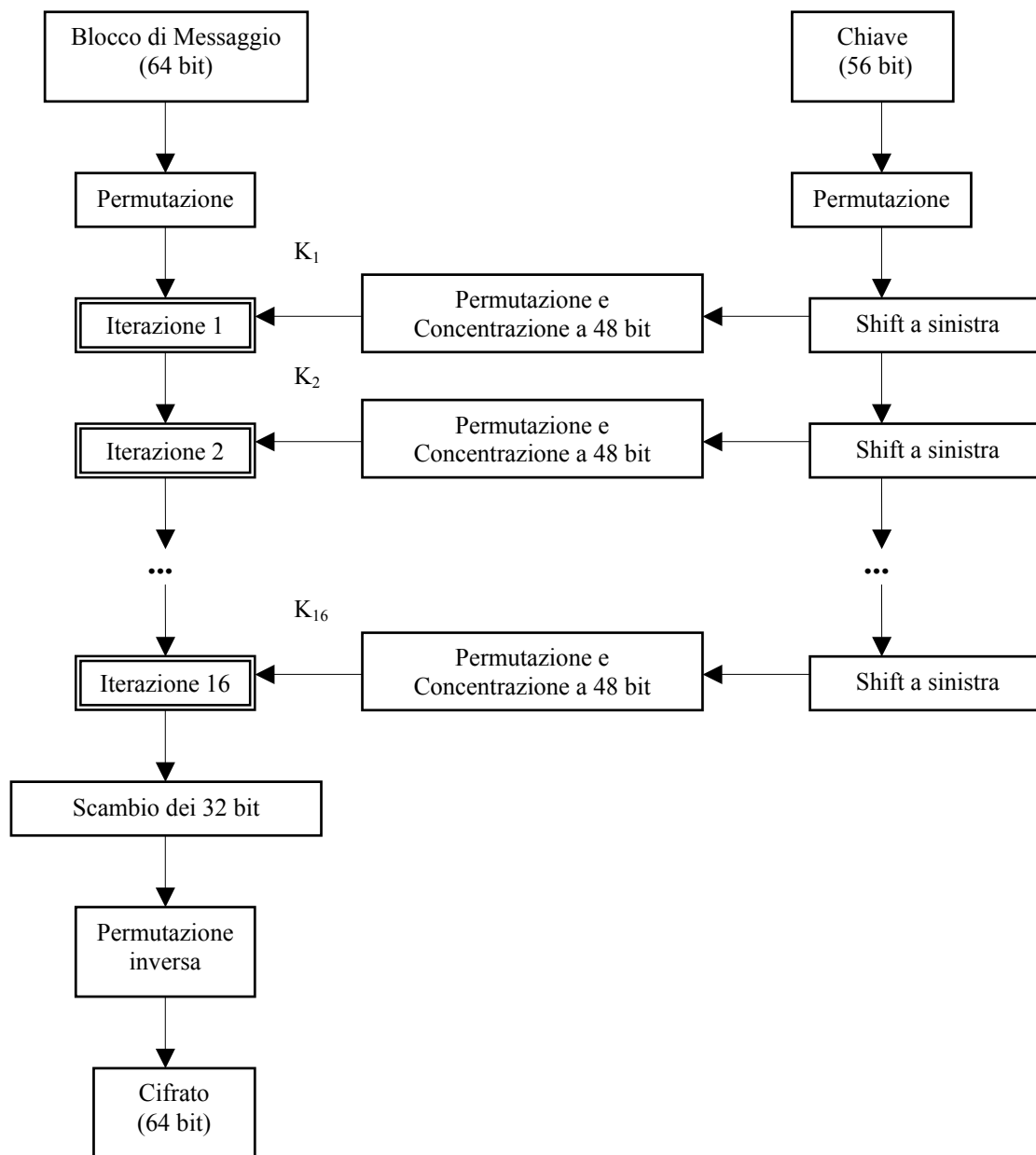


Figura 2. Schema del principio di funzionamento dell'algoritmo DES

Una introduzione alla Crittografia

5. Crittografia asimmetrica

Il concetto di crittografia *asimmetrica*, o a chiave pubblica, si basa sull'uso di due chiavi legate tra loro da una funzione matematica, ma tali che sia impossibile ricavare una delle due, nota l'altra (Diffie e Hellman, 1975). Una è chiamata *chiave privata* e deve essere mantenuta segreta, l'altra è chiamata *chiave pubblica* e viene resa nota al pubblico. Ogni messaggio che viene cifrato con una delle due chiavi può essere decifrato solo e soltanto dall'altra chiave ad essa corrispondente.

La crittografia asimmetrica può essere utilizzata per realizzare tre funzioni distinte:

1. Il mittente vuole garantire la confidenzialità del messaggio, cioè assicurarsi che solo il destinatario possa decifrare il testo cifrato. Per ottenere questo il mittente deve cifrare il testo in chiaro con la chiave pubblica del destinatario; infatti solo chi possiede la chiave privata corrispondente, sarà in grado di decifrare il messaggio.
2. Il mittente vuole garantire l'autenticazione del messaggio, cioè provare che soltanto lui può avere spedito il messaggio stesso. Il mittente deve cifrare il testo in chiaro con la propria chiave privata (nota a lui solo); poiché la corrispondente chiave pubblica può essere nota a tutto il mondo, il destinatario può recuperarla e usarla per decifrare il messaggio, avendo conferma dell'identità del mittente.
3. Il mittente vuole garantire confidenzialità e autenticazione del messaggio. Il mittente deve applicare in cascata le metodologie indicate nei due punti precedenti.

Il numero di chiavi necessarie affinché un gruppo di n persone possa comunicare tra loro in modo "sicuro" è in questo caso di $2*n$. La crittografia a chiave pubblica permette l'autenticazione "uno a molti".

Il principale svantaggio consiste nella maggior complessità computazionale.

Una introduzione alla Crittografia

6. L'algoritmo RSA

L'algoritmo a chiave pubblica maggiormente utilizzato è l'algoritmo RSA (il nome deriva dalle iniziali dei suoi tre inventori Rivest, Shamir e Adleman).

La modalità di funzionamento può essere schematizzata come segue:

- [1] si considerano due numeri primi p e q , molto grandi (dell'ordine di grandezza di 10^{100}). (Per fare un esempio consideriamo $p=11$ e $q=3$);
- [2] si calcolano i prodotti $n = p*q$ e $z = (p-1)*(q-1)$; z non può essere primo perché è pari; se b è il numero desiderato di bit della chiave, deve essere $2^b < n < 2^{b+1}$ ($n = p*q=33$, $z = (p-1)*(q-1)= 10*2=20$);
- [3] si sceglie un numero $e < n$ che sia primo con z ; e deve essere dispari ($e=3$);
- [4] si determina un numero d tale che sia verificata l'espressione $e*d \bmod z = 1$; si dimostra che d esiste sempre, per ogni e e z (nell'esempio $d=7$);
- [5] si divide il testo da cifrare in blocchi, in modo che ciascun blocco del testo in chiaro P abbia lunghezza in bit minore di n (questo può essere fatto raggruppando il testo in chiaro P in blocchi di k bit, dove k è il più grande intero per il quale è verificata la relazione $z^k < n$);
- [6] il messaggio cifrato è $C = P^e \bmod n$, dove P è il testo in chiaro
- [7] per ottenere il messaggio originale bisogna calcolare $P = C^d \bmod n$.

Si dimostra che, per tutti i messaggi P che soddisfano la condizione al punto [5], la funzione usata per cifrare è l'inversa di quella usata per decifrare. Per cifrare il testo in chiaro P occorre calcolare e ed n , per decifrare il testo cifrato C sono necessari d ed n . La chiave pubblica è quindi costituita dalla coppia (e, n) mentre la chiave privata è formata dalla coppia (d, n) ; e è anche definito "esponente pubblico" e d "esponente privato".

La sicurezza di questo algoritmo risiede nella difficoltà di fattorizzare (cioè scomporre un numero nel prodotto dei numeri primi che lo compongono) i numeri n utilizzati (che sono grandi). Ad oggi non esiste nessun algoritmo efficiente in grado di effettuare questa operazione e la fattorizzazione è possibile solo procedendo a forza bruta, esaminando tutti i possibili numeri primi. Da questo discende anche la seconda caratteristica propria degli algoritmi asimmetrici: la chiave pubblica può essere nota a tutto il mondo perché non esistono metodi efficienti per calcolare d , p e q dati n ed e .