

Testo estratto dal volume S. PIGLIAPOCO, *La memoria digitale delle amministrazioni pubbliche*, Santarcangelo di Romagna, Maggioli editore, 2005

CRITTOGRAFIA

Il termine crittografia indica la scienza che studia i sistemi segreti di scrittura, ovvero i metodi per rendere un testo comprensibile solo a chi conosce un determinato codice o chiave. Con riferimento ai documenti informatici, la finalità principale di un processo crittografico è quella di garantire la loro riservatezza in ogni operazione di trattamento. Esso comprende una fase di codifica e una fase di decodifica. La prima consiste nell'applicare al file contenente la rappresentazione digitale del documento una funzione matematica che, utilizzando un codice K_c denominato *chiave di codifica*, produce una configurazione binaria tale da non permettere a chiunque e con qualunque software la visualizzazione o la stampa del documento. La seconda, invece, consiste nell'applicare al file crittografato un'altra funzione matematica che, utilizzando il codice K_d denominato *chiave di decodifica*, riproduce la configurazione binaria di partenza. Lo schema che rappresenta queste due operazioni è riportato in figura 1.4.

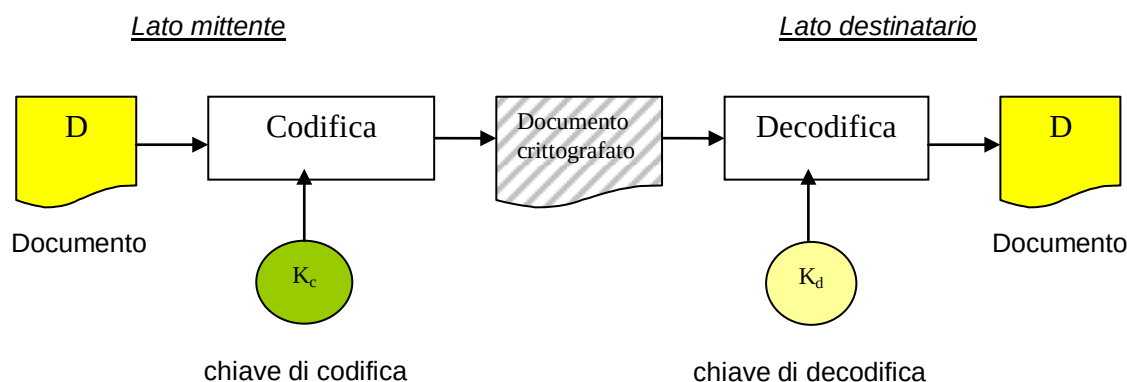


Figura 1.4 - Schema di un processo crittografico

Si parla di *crittografia simmetrica* se la chiave di codifica K_c è uguale alla chiave di decodifica K_d , ovvero si utilizza lo stesso codice per codificare e decodificare il documento. Il DES (Data Encryption Standard) è sicuramente il più noto e diffuso algoritmo di crittografia simmetrica; è stato sviluppato nel 1974 dalla IBM in risposta ad un bando del National Bureau of Standards (NBS) e ufficialmente adottato come standard federale statunitense nel 1976 per l'utilizzo nelle comunicazioni nel settore pubblico e privato. Il DES suddivide il file in blocchi da 64 bit e li codifica con i metodi della sostituzione e della trasposizione¹ ripetuti per 16 cicli, utilizzando chiavi di lunghezza pari a 64 bit. Questo

¹ Il metodo della sostituzione consiste nel sostituire ciascuna lettera del messaggio in chiaro con un'altra lettera o simbolo con una logica più o meno complessa a seconda del livello di riservatezza che si vuole raggiungere

algoritmo assicura una velocità di codifica e decodifica molto elevata e quindi è particolarmente adatto per le applicazioni basate su Internet; tuttavia, sotto il profilo della sicurezza presenta dei limiti riconducibili alla limitata lunghezza della chiave. Un'evoluzione del DES è il Triple-DES (3-DES), che consiste nel ripetere tre volte lo stesso algoritmo con due chiavi diverse, permettendo così di raddoppiare la lunghezza della chiave. Per anticipare l'aumento di potenza dei computer, il NIST (National Institute of Standards and Technology) statunitense ha recentemente promosso lo sviluppo di uno standard di crittografia avanzata, l'AES (Advanced Encryption Standard), fissando come vincoli:

- la libera diffusione senza diritto di sfruttamento;
- l'utilizzo della crittografia simmetrica a blocchi di 128 bit;
- l'utilizzo di chiavi di lunghezza pari a 128, 192 e 256 bit.

Dalla selezione effettuata dal NIST è risultato vincente l'algoritmo Rijndael (dai nomi dei creatori Vincent Rijmen e Joan Daemen) che il governo degli Stati Uniti ha adottato nel dicembre 2001, indicandolo come standard per l'elaborazione delle informazioni federali FIPS (Federal Information Processing Standard)².

Se la chiave di codifica K_c è diversa da quella di decodifica K_d , si parla di *crittografia a chiavi asimmetriche*. Ogni soggetto che utilizza un algoritmo di questo tipo deve dotarsi di una coppia di chiavi: una pubblica K_p e una segreta K_s . La prima deve essere resa nota a tutti, mentre la seconda deve essere conosciuta solo dal titolare della coppia. L'algoritmo assicura che:

- da una chiave della coppia non è possibile risalire all'altra chiave della stessa coppia³;
- se la codifica di un documento è eseguita con una chiave di una coppia, l'operazione inversa di decodifica può essere effettuata solo con l'altra chiave della stessa coppia.

Da ciò consegue che per trasmettere un messaggio ad un destinatario in modo riservato, utilizzando un algoritmo di crittografia asimmetrica, è sufficiente codificarlo con la chiave pubblica del destinatario. Così facendo, infatti, il messaggio potrà essere decodificato solo da chi possiede la chiave segreta del destinatario (l'altra chiave della stessa coppia) che per definizione solo lui può conoscere. Lo schema che rappresenta una comunicazione tra due soggetti crittografata con un algoritmo asimmetrico è riportato in figura 1.5.

L'algoritmo di crittografia a chiavi asimmetriche più noto è l'algoritmo RSA (dalle iniziali dei nomi degli inventori Rivest, Shamir, Adleman) che è stato introdotto nel 1978 e ancora

(sostituzione semplice, poligrafica, polialfabetica, etc.). Il metodo della trasposizione, invece, consiste nel "mescolare" il testo in chiaro secondo una regola reversibile

² Cfr. C. PFLEGER, S. PFLEGER, *Sicurezza in informatica*, Milano, Pearson Education Italia, 2004, pp. 73-80

³ Con l'espressione "non è possibile risalire" non si intende l'impossibilità in senso assoluto, ma che l'operazione richiederebbe una potenza di calcolo così elevata e un tempo di elaborazione così lungo da ritenere pressoché nulla la probabilità che essa sia eseguita.

oggi appare sicuro. Esso si basa sulla teoria dei numeri e sulla difficoltà di determinare i fattori primi di numero di grandi dimensioni. Le coppia di chiavi utilizzabili con l'algoritmo RSA sono determinate in questo modo:

- si scelgono due numeri primi⁴ X e Y di grandi dimensioni (devono contenere almeno 100 cifre ciascuno);
- si calcola Z come il prodotto di X per Y (quindi avrà una dimensione minima di 200 cifre)⁵;
- si determina una chiave della coppia scegliendo un numero primo maggiore sia di (X-1) che di (Y-1), ovvero che sia primo in relazione al prodotto di (X-1) per (Y-1);
- si determina l'altra chiave della coppia in modo tale che il prodotto delle due chiavi sia uguale al modulo di Z⁶;
- si conservano le due chiavi e il valore di Z, mentre si scartano, ovvero si distruggono senza essere rivelati, i valori di X, Y e ogni altro elemento utilizzato nel calcolo.

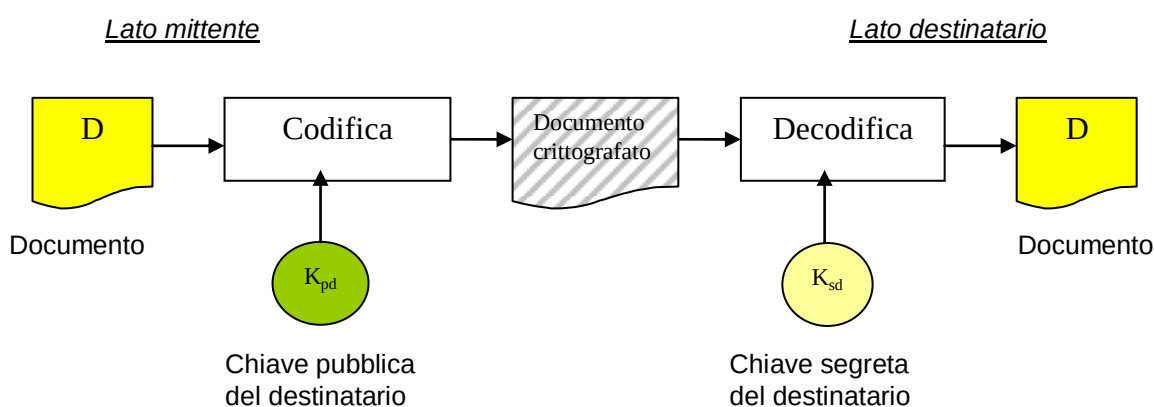


Figura 1.5 - Schema di un processo crittografico asimmetrico

Il problema della ricerca di due numeri primi X e Y, che richiederebbe il calcolo di almeno 10^{50} possibili fattori, è risolto con il metodo di Solovay e Strassen il quale prevede la generazione casuale di un numero di grandi dimensioni e l'esecuzione di una serie di test per verificare che esso sia un numero primo. In caso di insuccesso di un test, si passa alla generazione di un altro numero e così via. Se r è il numero dei test eseguiti che hanno dato esito favorevole, la probabilità che il numero generato non sia un numero primo è pari a $1/2^r$, per cui tanto più è grande r e tanto più elevata è la sicurezza dell'algoritmo RSA⁷.

⁴ Un numero primo è un numero maggiore di 1 divisibile solo per sé stesso e per 1.

⁵ Tanto più è grande Z e tanto più tende ad annullarsi la possibilità di ricavare da esso i valori di X ed Y con la funzione di fattorizzazione

⁶ Il modulo di un intero non negativo indica il resto dopo la divisione.

⁷ Per poter utilizzare l'algoritmo RSA per la generazione di firme elettroniche con valenza giuridica equivalente alle firme autografe, l'affidabilità del processo di generazione delle coppie di chiavi è un'esigenza irrinunciabile e, pertanto, il valore di r deve essere molto elevato.

A partire da una coppia di chiavi (K_s , K_p), la formula per la codifica di un testo T è la seguente:

$$C = T^{K_p} \bmod z$$

La formula inversa per la decodifica è:

$$T = C^{K_s} \bmod z.$$

Un algoritmo crittografico asimmetrico presenta lo svantaggio di essere più lento rispetto ad uno simmetrico come il DES, ma anche alcuni vantaggi. In primo luogo, richiede il rilascio di un numero minore di chiavi; ad esempio, per un comunità di N soggetti sono necessarie esattamente $2N$ chiavi, mentre con un sistema simmetrico si dovrebbe dare ad ogni possibile coppia di corrispondenti una chiave segreta per un numero complessivo di codici da assegnare pari a $N(N-1)/2^8$. In secondo luogo, può essere utilizzato per la generazione di firma elettroniche in quanto una delle due chiavi della coppia rimane segreta e in possesso esclusivo del titolare, mentre nei sistemi simmetrici ogni chiave è posseduta almeno da due soggetti: il mittente e il destinatario. In ultimo, garantisce un grado di riservatezza elevato se si utilizzano chiavi a 1024, 2048, 4096 bit o anche più lunghe.

HASH CRITTOGRAFICO

Il processo di generazione di una firma elettronica comprende l'applicazione di una *funzione di HASH* al file contenente la rappresentazione digitale del documento. Si tratta di una funzione matematica che, a partire da un'evidenza informatica di lunghezza arbitraria - il file da firmare - permette di generare una stringa binaria di lunghezza fissa, denominata *impronta digitale* del file o message digest, garantendo:

- l'*unidirezionalità*, cioè l'impossibilità di risalire al documento informatico partendo dalla sua impronta digitale;
- la *resistenza alle collisioni*, cioè l'impossibilità di generare una stessa impronta digitale a partire da due file diversi.

Gli algoritmi di HASH più conosciuti sono l'MD5 (Message Digest 5), che produce impronte digitali di 128 bit, l'SHA-1 (Secure Hash Algorithm 1) e il RIPEMD-160 (nato nell'ambito del progetto europeo RIPE - Race Integrity Primitives Evaluation) definiti nella norma ISO/IEC 10118-3:1998, che producono impronte a 160 bit, l'algoritmo, definito nella norma ISO/IEC 10118-3:2004: dedicated hash-function 4, corrispondente alla funzione SHA-256⁹.

⁸ Per N maggiore di 5 un sistema asimmetrico richiede il rilascio di un numero minore di chiavi

⁹ Attualmente è questa la funzione di HASH da utilizzare per la generazione di firme digitali conformi alla normativa vigente in materia.

La resistenza alle collisioni è un requisito irrinunciabile perché, essendo la firma digitale il risultato di un algoritmo crittografico applicato all'impronta digitale del documento informatico, se due documenti diversi dessero origine alla stessa impronta, la firma generata a partire da questa potrebbe essere riferita indifferentemente all'uno o all'altro documento con conseguente perdita della certezza giuridica. Le funzioni di HASH non garantiscono al 100% che da due documenti diversi non sia possibile generare la stessa impronta, ma assicurano che la probabilità che ciò accada è infinitamente piccola e che è estremamente difficile produrre collisioni in modo intenzionale.