Crittografia simmetrica

Da Wikipedia, l'enciclopedia libera.

> **Questa voce o sezione sull'argomento crittografia non cita le fonti necessarie o quelle presenti sono insufficienti**.

Con **crittografia simmetrica** (o **crittografia a chiave privata**) si intende una tecnica di cifratura. Rappresenta un metodo semplice per cifrare testo in chiaro dove la chiave di crittazione è la stessa chiave di decrittazione, rendendo l'algoritmo di cifratura molto performante e semplice da implementare. Tuttavia presuppone che le due parti siano già in possesso delle chiavi, richiesta che non rende possibile uno scambio di chiavi con questo genere di algoritmi. Lo scambio avviene attraverso algoritmi a chiave asimmetrica o pubblica, generalmente più complessi sia da implementare che da eseguire, ma che permettono questo scambio in modo sicuro. Dopodiché la comunicazione verrà crittata usando solo algoritmi a chiave simmetrica per garantire una comunicazione sicura, ma veloce.

Rappresentazione semplificata schematica della crittografia simmetrica.

Indice

Funzionamento

In questo genere di algoritmi si suppone che entrambe le parti conoscano già la chiave con cui crittare e decrittare il messaggio. Il mittente ha un messaggio P (PlainText o testo in chiaro). Il mittente critta il messaggio P con la chiave k usando un algoritmo di crittografia simmetrica chiamato S. Il messaggio risultante sarà C (CypherText o messaggio cifrato). In formule diventa:

$$S(P, k) = C.$$

A questo punto al destinatario arriva un messaggio cifrato che riesce a decrittare poiché è in possesso della chiave privata. Ora il ricevente applica l'algoritmo di decrittazione D con la stessa chiave che ha usato il mittente per crittare il testo. Diventa:

$$D(C, k) = P.$$

Se un attaccante ha intercettato il messaggio lungo il mezzo di comunicazione, avrà il messaggio crittato ma non la chiave che è stata scambiata in modo sicuro dai due interlocutori. Se l'attaccante vorrà leggere il messaggio crittato potrà solo usare metodi di decrittazione che richiedono elevate capacità di calcolo.

Nel caso di una comunicazione reale, questo colloquio viene criptato tramite un algoritmo a chiave pubblica, più complesso ma che non richiede nessuna trasmissione della chiave sul mezzo di comunicazione.

Componenti comuni nelle varie implementazioni

Tra i vari algoritmi di crittazione possiamo trovare alcune operazioni comuni, poiché aggiungono generalmente maggior sicurezza nel testo cifrato e sono operazioni rapide per la macchina.

Spesso una stessa operazione viene ripetuta più volte, riferendosi a questi passaggi come cicli o round. Ad esempio in AES la stessa routine viene ripetuta 10 volte. In DES il testo in chiaro subisce 16 volte la crittazione insieme alla chiave prima di terminare. Una volta disegnato l'algoritmo viene molto facile ripeterlo, rendendo più complesso un lavoro di decrittazione forzata tramite brute force. Se l'algoritmo di decrittazione è ben disegnato e non si riescono ad avere informazioni sulla chiave, questo è l'unico metodo attraverso cui è possibile la decrittazione del messaggio cifrato.

Tra i vari algoritmi simmetrici possiamo riconoscere alcuni parametri standard come la lunghezza della chiave e la dimensione del blocco.

La lunghezza della chiave è misurata in bit e ha valori che oscillano tra 32 bit e 512 bit. Generalmente la lunghezza della chiave è un valore fisso nonostante esistano alcuni algoritmi come AES che impiegano lunghezze variabili.

Ogni algoritmo generalmente cerca di crittare una stringa di bit attraverso una chiave in un'altra stringa di bit della medesima lunghezza. La lunghezza di questa stringa è uguale alla dimensione del blocco. Algoritmi più datati avevano questo valore pari a 64 bit in media. Oggi si preferisce adottare dimensioni di 128 bit.

Un problema che affligge la dimensione del blocco è il paradosso del compleanno che rilascia informazioni sulla chiave ogni volta che avviene una collisione. Possiamo ritenere sicura solo la radice quadrata di tutte le combinazioni possibili. Per esempio con una dimensione di 64 bit, che genererebbe 2^{64} possibili combinazioni, potremo impiegarne solo 2^{32} prima di cominciare a rivelare informazioni sulla chiave.

Metodi di cifratura a blocchi di cifre

Generalmente la dimensione del blocco scelta è della medesima lunghezza della chiave perché risulta semplice per l'implementazione di un algoritmo. Tuttavia è bene fare attenzione ad alcuni metodi che possono compromettere la sicurezza dell'algoritmo. Nei seguenti algoritmi individuiamo:

- k_i è l'i-esima cifra della chiave;
- P_i è l'i-esima cifra del testo in chiaro;
- C_i è l'i-esima cifra del testo cifrato.

Con $i = 1, \ldots, n$, dove n indica la dimensione del blocco e la lunghezza della chiave.

Electronic Code Book (ECB)

$$S(P_i, k_i) = C_i.$$

È l'implementazione più semplice, in cui l'unica cosa che nasconde il testo in chiaro è una cifra della chiave. Questo metodo risulta essere tanto semplice quanto insicuro. Infatti è sufficiente per l'attaccante raccogliere un numero sufficiente di campioni per scoprire la chiave. Su questo metodo si basa il cifrario di Cesare.

Cipher Block Chaining (CBC)

$$S((IV \oplus P_1), k_1) = C_1.$$

$$S((C_{i-1} \oplus P_i), k_i) = C_i.$$

In questo metodo si aggiunge un fattore di casualità inserendo nell'algoritmo anche la cifra precedentemente crittata, più precisamentre, si effettua uno XOR, indicato con il simbolo $\oplus$ prima di crittare il testo. In questo modo non vi è una associazione univoca tra chiave e testo in chiaro ma si aggiunge la dipendenza dalla cifra precedente. Inserendo la dipendenza dalla cifra precedente, si crea la necessità di aggiungere un elemento per crittare la prima cifra del blocco, chiamato vettore di inizializzazione (IV nelle formule).

Cipher Feed-Back (CFB)

$$S(IV, k_1) \oplus P_1 = C_1.$$

$$S(C_{i-1}, k_i) \oplus P_i = C_i.$$

Molto simile al CBC ma l'operazione di XOR con il testo in chiaro viene eseguita dopo la crittazione. Si critta prima la chiave con la cifra precedente o il vettore di inizializzazione nel caso della prima cifra. Rispetto a CBC è sempre presente la dipendenza dalla cifra precedente, ma soffre ancora del problema di malleabilità, anche se solo localmente alla singola cifra.

Metodi di crittazione a flusso di cifre

Anziché lavorare su un blocco di cifre con una chiave delle stesse dimensioni, la chiave viene combinata all'intero messaggio, di solito attraverso operazioni XOR. RC4 si basa su questo metodo.

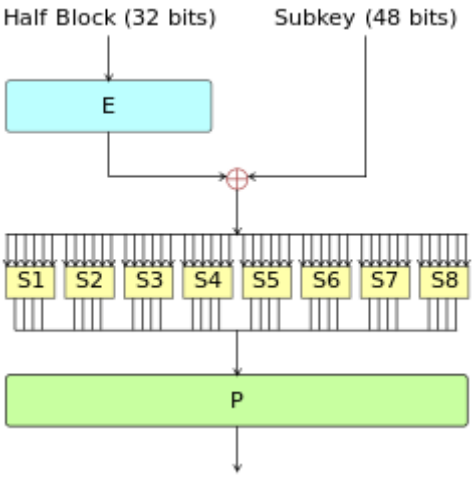
Esistono due tipi di algoritmi:

- *sincroni*, in cui lo stato viene mantenuto dall'algoritmo, ma non è legato né al testo in chiaro né al testo cifrato;
- *auto-sincronizzanti*, in cui lo stato viene mantenuto ottenendo informazioni dal testo.

Algoritmi

DES (Data Encryption Standard)

DES è uno degli algoritmi a chiave simmetrica più famoso, pubblicato nel 1976 da IBM e scelto come standard per la Federal Information Processing Standard. È diventato in seguito lo standard fino a quando non fu decrittato nel 1997 in 3 giorni di calcolo. Nell'anno successivo fu sufficiente un giorno soltanto impiegando un cluster di computer e con l'avanzare i tempi si riducono ulteriormente. Il suo successore fu 3DES. Impiega una chiave di 56 bit e opera su blocchi di 64 bit.

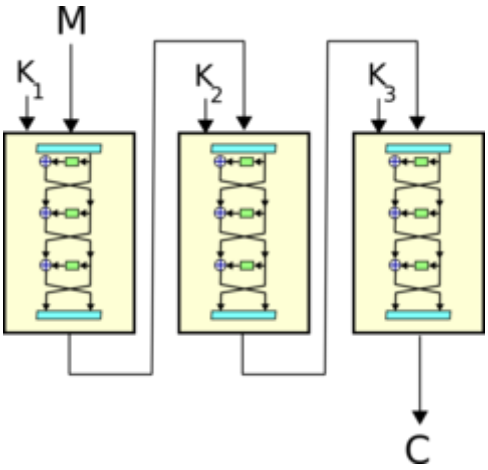


Schema del DES

3DES (Triple DES)

Quando DES non fu più sicuro, si cercò un metodo che mantenesse le meccaniche del DES ma che permettesse di avere una chiave più lunga. In questo algoritmo si esegue una tripla crittazione impiegando 3 chiavi DES standard, a 56 bit, ottenendo una chiave a 168 bit. È possibile anche invertire il secondo passaggio, ovvero eseguire una crittazione e una decrittazione. Tuttavia non modifica la sicurezza generale dell'algoritmo.

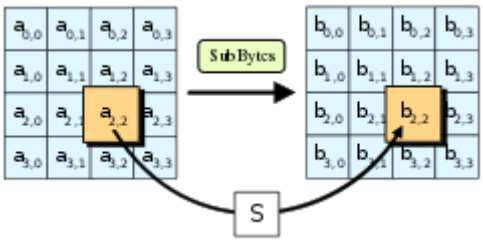
Anche questo algoritmo oggi non viene più impiegato poiché le tecnologie si stanno evolvendo e molti algoritmi di crittazione non risultano abbastanza forti da sopportare le elevate capacità di calcolo dei computer moderni, soprattutto con l'avvento delle GPGPU. 3DES ha lasciato il posto a AES, il nuovo standard ormai.



Schema del 3DES

AES (Advanced Encryption Standard)

Nel 1999 si presentarono vari algoritmi candidati a diventare lo standard di crittografia simmetrica. Questi candidati furono MARS proposto dalla IBM, RC6, Serpent, Twofish e Rijndael. Tutti questi algoritmi furono testati per efficienza e sicurezza su varie architetture, sia hardware che software. Tra questi ricevette un feedback positivo Rijndael che nel 2000 divenne il nuovo standard con il nome di AES. Fu dapprima impiegato dal governo degli USA e dopodiché il suo successo divenne globale.



Schema dell'AES

AES lavora su blocchi a dimensione fissa di 128 bit[1]. Ha una chiave di 128 bit, ma possono essere impiegate chiavi più lunghe da 192 e 256 bit per crittare documenti di particolare importanza.

Note

1. ^ *Announcing the ADVANCED ENCRYPTION STANDARD (AES)* (PDF), 26 novembre 2001.

Bibliografia

- *Advanced Encryption Standard*, su *searchsecurity.techtarget.com*. URL consultato il 31 maggio 2016.
- *Triple data encription*, su *vocal.com*. URL consultato il 31 maggio 2016.
- *Crittografia a chiave simmetrica*, su *cs.cornell.edu*. URL consultato il 12 giugno 2016.

Voci correlate

- 3DES
- AES
- Crittografia asimmetrica
- Data Encryption Standard
- Differenza fra cifratura simmetrica e asimmetrica

Controllo di autorità	GND (DE) 4317451-6 (https://d-nb.info/gnd/4317451-6)