appunti_interrogazione_sistemi__4

Introduzione

La **crittografia** è una parte della matematica il cui scopo è di **trasformare un messaggio, rendendo visibile solo alle parti interessate**. (*mittente e destinatario*)

Tipi di cifrari

Ci sono tre tipi principali di cifrari:

- **Shifting** (*sostituzione*)
  Come il *cifrario di Cesare*.
  Consiste nello spostamento dei valori del messaggio. (Come le posizioni delle lettere dell'alfabeto)

Essendo, di base, uno spostamento costante, è vulnerabile ad **analisi delle frequenze**.

Una versione avanzata dei cifrari a sostituzione è quella di *Vigenère*, che esegue lo spostamento rispetto ad una *chiave*. (Rispetto ad una tabella dell'alfabeto, la lettera del messaggio rappresenta la colonna, e la lettera della chiave la riga)

- **a Blocchi**
  Questo metodo consiste nella frammentazione del messaggio in più blocchi, a lunghezza fissa o variabile.
- **a Flusso**
  Questo metodo consiste nell'esecuzione della crittografia su tutto il messaggio unico, senza eseguire frammentazioni.
  (Più sicuro ma lento)

Le chiavi

Per rendere il messaggio facilmente decifrabile al destinatario, viene spesso condivisa in modo sicuro una *chiave*, che è la sequenza crittografica utilizzata dal mittente.
Senza chiave, un malintenzionato dovrà andare a rieseguire più volte l'algoritmo di decifratura, ogni volta con una chiave diversa. (Brute-forcing)

Ci sono 2 tipi di chiavi:

- **Simmetrica**, dove viene usata una sola chiave per sia i processi di cifratura che decifratura.
  Permette la verifica dell'*autorizzazione*, ma non dell'*identificazione*.
- **Asimmetrica**, dove ci sono più chiavi: una per la cifratura, l'altra per la decifratura
  Molto spesso queste chiavi vengono definite in **chiave pubblica** e **chiave privata**.
  La **chiave privata sarà posseduta solo dal mittente**, e verrà usata per cifrare il

messaggio, il quale potrà essere decifrato tramite l'uso della **chiave pubblica, condivisa con il destinatario**.

Sarà possibile eseguire la verifica dell'identità tramite l'invio della chiave privata del mittente, e la verifica dell'autorizzazione tramite la chiave pubblica.
(Il mittente invia la sua chiave privata, cifrandola con la chiave pubblica. Solo il destinatario potrà decifrare il messaggio e ottenere la chiave, verificando l'identità del mittente)

Algoritmi noti

DES (Chiave simmetrica e a blocchi)

Inventato nel *1976*, e rotto nel *1998* in meno di *60 ore*.

Viene usata una **chiave simmetrica a 64 bit**. (*56 per la trasformazione del messaggio, 8 per il controllo*)

I passaggi principali del DES sono:

1. Il **messaggio viene diviso in blocchi da 64 parti**
   - Successivamente diviso in 2 parti **Li e Ri**, 32 bit
2. Viene eseguita una **funzione di espansione** sul lato destro, estendendolo a *48 bit*
3. Sul lato destro viene eseguita l'operazione **XOR** con una sottochiave **Ki** di 48 bit, estratta in modo casuale dalla chiave principale
4. Il risultato viene diviso **in 8 blocchi da 6 bit**, sui quali viene eseguita una **S-Box**, che esegue una funzione di **riduzione a 4 bit**
5. Il risultato delle S-Box verrà operato con il **lato sinistro** tramite l'operazione **XOR**, e diventerà la nuova parte destra
   Questi passaggi vengono iterati *16 volte*.

Per eseguire la decifratura, basta ri-eseguire l'algoritmo in modo diverso, con l'ordine inverso delle sottochiavi.

(L'**S-Box** è una **matrice per l'esecuzione di trasformazioni non-lineari**, che rendono la cifratura sicura)

3-DES

Introdotto successivamente alla rottura del DES, consiste nell'applicazione ripetitiva del DES con chiavi diverse. (Svantaggio: molto lento)

- **Cifratura** : cifratura (*k1*) -> decifratura (*k2*) -> cifratura (*k3*)
- **Decifratura**: decifratura (*k3*) -> cifratura (*k2*) -> decifratura (*k1*)

AES

Versione successiva del DES.
Le chiavi possono essere di più lunghezze: *128, 192 o 256 bit*.
I messaggi vengono divisi in blocchi, disposti in *griglie di 4x4 byte*.

Su di essi verranno eseguite *4 operazioni, ripetute 10 volte*:

1. **Sostituzione dei byte**
   Su ogni casella della griglia viene eseguita una *S-Box*, che fornisce *non-linearità* all'algoritmo.
2. **Spostamento delle righe**
   Ogni riga viene spostata verso sinistra.
   - La prima di 0 posizioni
   - La seconda di 1 posizione
   - La terza di 2 posizioni
   - La quarta di 3 posizioni
3. **Mix columns**
   Su ogni colonna viene applicata una funzione *trasformazione lineare*. (*viene moltiplicata per un polinomio fisso*)
4. **Add round key**
   Ogni byte viene combinato, tramite operazioni **XOR**, con parte delle chiave

RSA

Algoritmo a **chiave asimmetrica**.

L'algoritmo utilizza una **chiave pubblica composta e una chiave privata**.

Il destinatario **seleziona 2 numeri primi, che moltiplicherà tra loro**. (*p* e *q*)
Questo primo valore diventa la **prima chiave pubblica**
Viene calcolata la funzione di Euclero (*b*).
Viene poi calcolato un secondo numero, il **più piccolo numero intero che non ha fattori in comune con l'altro numero** (*e*) (tramite la *funzione di Euclero*)
Questo secondo valore diventerà la **seconda chiave pubblica**
Queste chiavi pubbliche verranno condivise con il mittente.

La **chiave privata** viene calcolata tramite la selezione del **più piccolo numero intero**, *d*, che restituisca l'operazione *e * d mod b* = 1.
Diventerà la **chiave privata**

La **cifratura del messaggio** verrà eseguita tramite l'operazione:

$$c = m^e mod N$$

La **decifratura del messaggio** verrà eseguita tramite l'operazione:

$$c = m^d mod N$$

Algoritmi di hashing

In passato, per la verifica di mittente/destinatario venivano usate le chiavi, ma era molto lento e pesante in termini di costi di risorse.
Per questo, sono stati introdotti gli *algoritmi di hashing*, utilizzati per la condivisione di **firme digitali**.
I più popolari sono *MD5 (Message Digest)* e *SHA-3 (Secure Hash Algorithm)*.

MD5

Questo algoritmo produce un *checksum/hash* lungo *128 bit* (*32 caratteri*).
La creazione dell'hash è composta da 4 fasi:

1. **Aggiunta di bit di riempimento**, aggiungendo al messaggio bit di padding per raggiungere la lunghezza di *448 bit*.
2. **Aggiunta della lunghezza**, verranno aggiunti *64 bit*, che rappresentano la lunghezza originale del messaggio
3. **Inizializzato il buffer MD**
   - L'algoritmo genera *4 valori esadecimali lunghi 32 bit*
   - Il messaggio viene diviso in *16 blocchi da 32 bit*
     - Su questi *4 blocchi* verranno eseguite trasformazioni con i *16 blocchi*. Verranno eseguiti *4 tipi di operazioni, ognuna 16 volte*
4. **Generazione dell'hash**, i valori finali dei *4 blocchi* verranno convertiti in **valore esadecimale, che rappresenteranno l'hash**.

SHA

Algoritmo realizzato dall'*NSA*, modifica dell'*MD4*.

- Estende i blocchi di messaggio a *1024 bit*
- Estende i 4 blocchi da *32 a 64 bit*
  - Le cui iterazioni passeranno da 64 a 80 in totale
- L'hash finale sarà lungo *512 bit*

Firme e certificati digitali

Data la lentezza e i costi di risorse necessari per algoritmi a chiave asimmetrica come l'RSA, è stata introdotta la firma digitale.
La **firma digitale è un sistema di autenticazione basato su un codice crittografato a chiavi asimmetriche**, che garantisce:

- Il proprietario del documento
- La verifica, da parte dei destinatari, dell'identità del proprietario
- La certezza che il documento non sia stato alterato

Queste firme vengono generate tramite **algoritmi di hashing** (come *MD* e *SHA*), che generano un *hash*, una ***fingerprint***, che identifica univocamente il file.
Questo hash verrà aggiunto al file **.p7m**, che contiene:

- Il documento originale
- La firma digitale
- Il certificato della chiave pubblica (Che permette la verifica dell'identità del proprietario)

Il **certificato digitale** è un *file temporaneo* che garantisce l'identità.
Sono rilasciati da un **ente certificatore** (**CA**, *certification authority*) che garantisce l'identità del proprietario e la firma digitale, tramite una propria chiave.

Questi certificati contengono:

- *Informazioni personali*, come nome, cognome, data di nascita... del proprietario
- *Dati del certificato*, come data di emissione, di scadenza e numero di serie
- *Dati della CA*, come ragione sociale del certificatore e codice identificativo

L'emissione dei certificati viene svolta dalla **Registration Authority**. (*La CA invece svolge la gestione dei certificati*)
L'insieme di queste 2 autorità, e la loro infrastruttura, forma il **PKI**. (*Public Key Infrastructure*)

Due formati di certificati digitali popolari sono:

- chiavi **PGP/GPG**
  È possibile generarle in modo autonomo
- certificati **X.509**
  Per generarlo è necessario rivolgersi ad un ente adatto