Crittografia

La *crittografia* è la scienza che si occupa di proteggere delle informazioni rendendole incomprensibili a chi le dovesse intercettare, in modo che possano essere lette e capite solo dal destinatario[1]

Figura A.1: Crittografia simmetrica.

Esempio:

Supponiamo che abbiano deciso che la chiave consista nel sostituire ad ogni lettera dell'alfabeto internazionale quella successiva, secondo questo schema:

Il grosso problema di questo approccio è però la *distribuzione delle chiavi*

Il problema è stato risolto in tempi relativamente recenti (**anni Settanta**) con l'invenzione della *crittografia a chiave pubblica*.

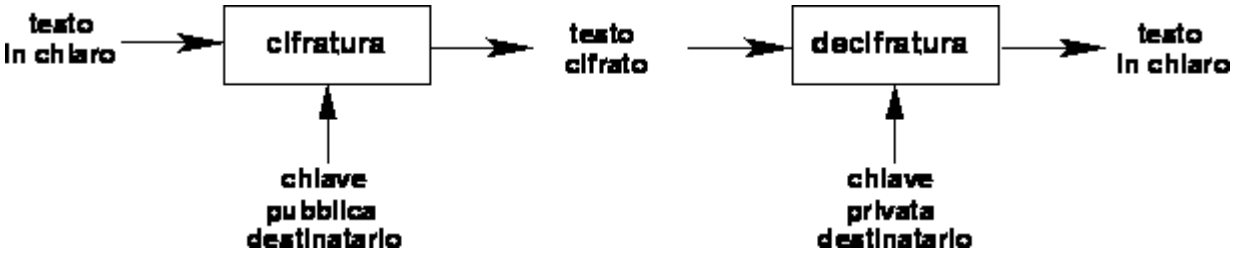


Figura A.2: Crittografia asimmetrica.

Con algoritmi di questo tipo ognuno ha due chiavi: una pubblica da distribuire a tutti quelli con cui vuole comunicare, e una privata da tenere segreta. Nella crittografia asimmetrica, Alice e Bob si scambiano un messaggio cifrato attraverso l'utilizzo di una chiave pubblica e una chiave privata attraverso le seguenti operazioni:

1. Bob genera una coppia di chiavi pubblica/privata
2. Bob comunica ad Alice la sua chiave pubblica
3. Alice usa la chiave pubblica di Bob per cifrare un messaggio
4. Alice spedisce il messaggio a Bob
5. Bob decifra il messaggio con la chiave privata

Nella serratura asimmetrica, per adoperare questa metafora, se chiudo con una chiave, apro il mio "cofanetto dei segreti" solo con l'altra chiave e viceversa. Quindi, se adopero la chiave pubblica per chiudere, apro il cofanetto solo utilizzando la chiave privata. Allora questa strana serratura mi permette di realizzare le funzioni di **autenticazione** e le funzioni di **segretezza**.

Ciò che viene cifrato con la chiave pubblica (operazione che può essere fatta da chiunque) può essere decifrato solo con la chiave privata corrispondente (operazione che può essere fatta solo dal proprietario

[1] Non bisogna confondere i sistemi **crittografici**, in cui il messaggio è identificabile ma incomprensibile, con quelli atti a *nascondere* l'informazione in modo che non ci si accorga della sua presenza (ad esempio scrivere un messaggio con inchiostro simpatico). La scienza che si occupa di queste ultime tecniche è detta ***steganografia***.

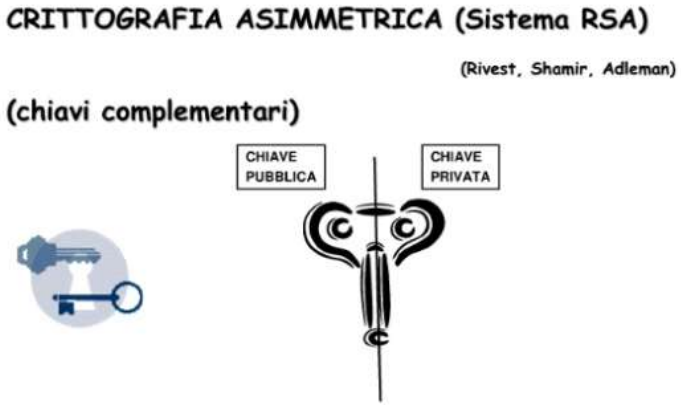
della chiave): per comunicare in modo sicuro con una persona basta cifrare il messaggio con la sua chiave pubblica, come illustrato nella figura precedente.

Gli algoritmi di questo tipo sono detti *a chiave asimmetrica*, e il più noto tra essi è probabilmente **RSA**

Una delle grosse innovazioni permesse dalla crittografia asimmetrica è la ***firma digitale***: il mittente di un messaggio può infatti firmarlo grazie alla sua chiave privata (che solo lui possiede), ma tutti sono in grado di verificare l'autenticità della firma grazie alla chiave pubblica (che è globalmente nota).

Esempio: Si ipotizzi che Tizio voglia mandare un messaggio a Caio: per prima cosa lo cifrerà con la propria chiave privata (**firma**) e poi con quella pubblica di Caio (**cifratura**), infine spedirà il messaggio.

Quando Caio lo riceverà, prima lo decifrerà con la propria chiave privata (operazione che solo lui può fare, per cui è garantita la confidenzialità) e poi con quella pubblica di Tizio: se l'operazione va a buon fine Caio ha la certezza che il mittente è davvero Tizio, perché solo lui può aver cifrato il messaggio con la propria chiave privata.



La **firma** può poi essere **abbinata alla normale cifratura**, ottenendo messaggi firmati e cifrati, nel modo seguente

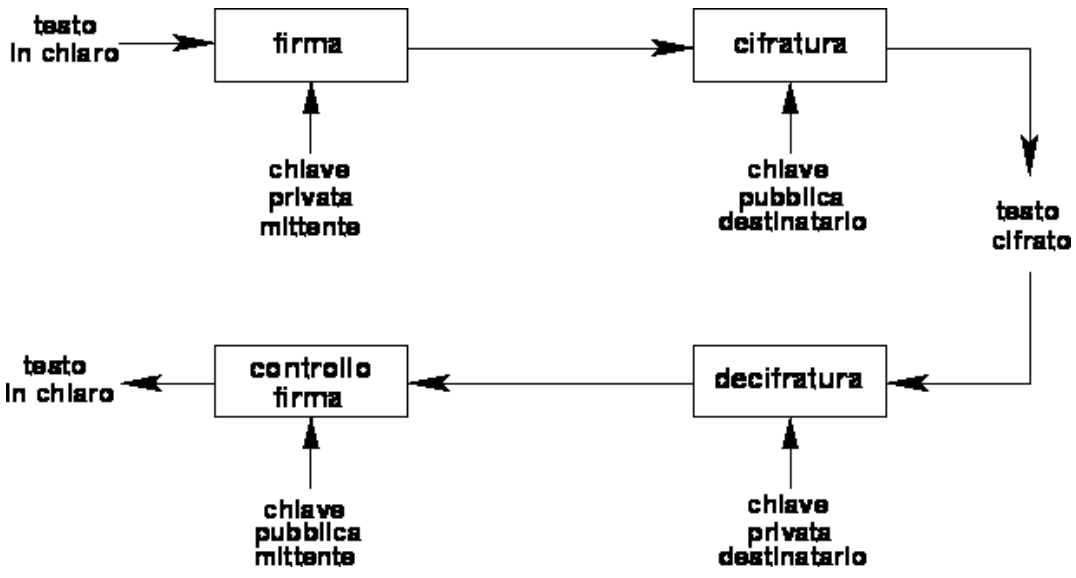
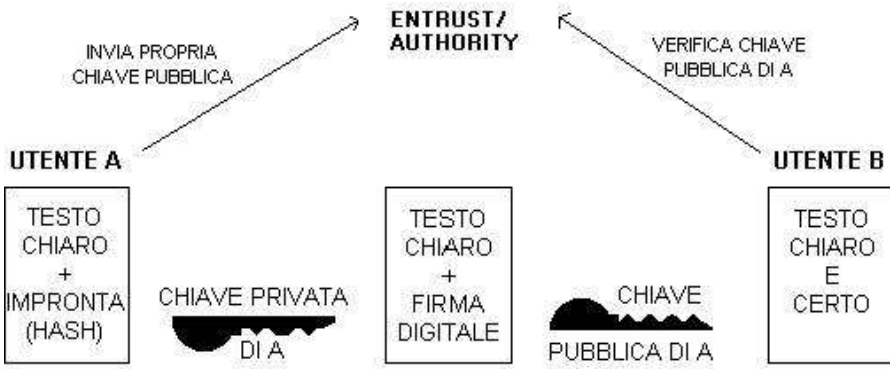
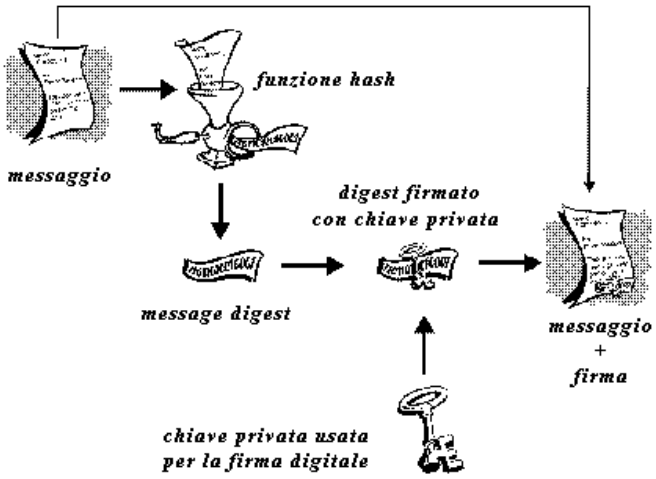


Figura A.3: Cifratura e firma digitale.

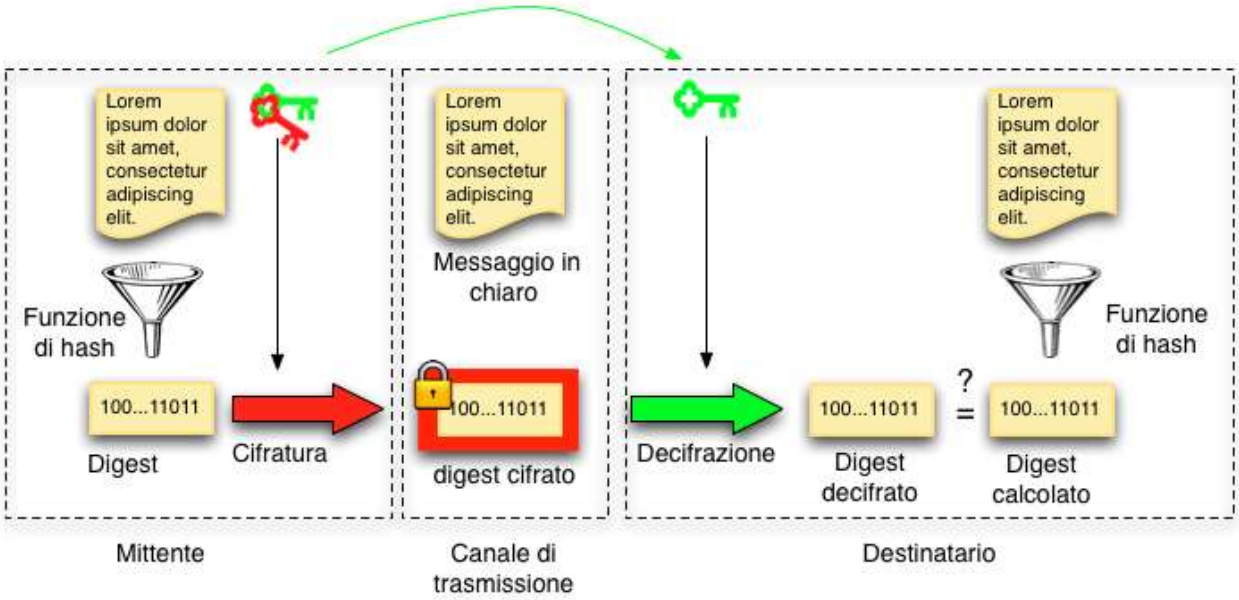
In realtà il modo in cui si realizza la firma digitale non è proprio questo, ma è leggermente più complicato:



ciò che il mittente cifra con la propria chiave privata per garantire l'autenticità non è l'intero messaggio, ma una sua ``**impronta**'' (detta *digest*) ottenuta mediante una particolare funzione[2] (*funzione di hash*); il digest cifrato viene poi allegato al messaggio e ne costituisce la firma. Il destinatario calcola il digest del messaggio ricevuto (la funzione di hash è pubblica) e lo confronta con quello che ottiene decifrando con la chiave pubblica del mittente la firma allegata: se coincidono la firma è autentica.



Si potrebbe pensare che dopo l'invenzione della crittografia a chiave pubblica quella a chiave segreta abbia perso interesse, ma le cose non stanno così. Gli algoritmi asimmetrici sono infatti computazionalmente molto più onerosi di quelli simmetrici, per cui il loro uso risulta molto più pesante.



Una soluzione comunemente adottata è l'uso della **crittografia asimmetrica** per concordare una **chiave segreta** da utilizzare poi per scambiarsi i **messaggi** tramite un algoritmo a **chiave simmetrica**: in questo modo il ``pesante'' algoritmo a chiave pubblica viene usato solo per trasmettere una piccola quantità di dati (la chiave segreta), mentre per il resto si usa il più leggero algoritmo a chiave segreta.

---

[2] Una *funzione di hash* è una funzione che, dato un qualunque messaggio di lunghezza arbitraria, ne produce un'*impronta* (detta *digest*) di lunghezza prefissata (di solito dell'ordine di 100-200 bit). L'utilità di una funziona di hash sta nel poter utilizzare l'impronta come rappresentazione compatta del messaggio stesso, tipicamente firmando l'impronta anziché l'intero messaggio; perchè questo possa avvenire è desiderabile che la funzione presenti due proprietà particolari, sia cioè *senza collisioni* e *unidirezionale*. (si veda l'appendice A.5) anche Hash e MAC

Glossario:

Crittologia: ***Crittografia*** + Crittoanalisi
Crittografia: progetto di cifrari sicuri ed efficienti.
Crittoanalisi: metodi, strumenti e tecniche per attaccare i cifrari (valutare la loro bontà).

RSA Questo metodo crittografico è stato ideato da R. **R**ivest, A. **S**hamir, L. **A**dleman, È basato sul problema della fattorizzazione intera, (moltiplicazione di due numeri primi) e consente sia la cifratura che la firma digitale. Il cifrario RSA è considerato sicuro perche al momento non sono noti algoritmi efficienti per fattorizzare un numero e si ritiene che non ne esistano.

- RSA(Rivest - Shamir - Adleman)
- **DSA**(Digital Segnature Algoritm)

MD5 (acronimo di Message Digest algorithm 5) è una funzione hash crittografica realizzata da Ronald Rivest nel 1991 e standardizzata con la RFC 1321. È un algoritmo che estrae da input di qualunque dimensione valori di *hash* di 128 bit che possono essere rappresentati con 32 cifre esadecimali:

```
MD5("a") = 60B725F10C9C85C70D97880DFE8191B3
MD5("Cantami o diva del pelide Achille l'ira funesta")
         = B4DD7F0B0CA6C25DD46CC096E45158EB
```

Tramite l'algoritmo MD5, come si può notare, da stringe in ingresso di lunghezza significativamente differente, sono stati calcolati due valori hash della stessa lunghezza. La lunghezza dei valori di hash varia a seconda degli algoritmi. Quelli a 128 bit sono i più comuni.

L'**algoritmo MD5** utilizza un buffer di 128 bit inizializzato a un valore prefissato. Divide il messaggio originale (visto come una stringa di bit) in blocchi di 512 bit aggiungendo se necessario dei *bit aggiuntivi* per arrivare a tale cifra e per ogni blocco di 128 bit vengono eseguiti quattro passi che consistono nel mescolare completamente i 512 bit in ingresso con il buffer di 128 fino a che tutti i blocchi in ingresso sono stati consumati. Alla fine il buffer sarà il *message digest* del testo in ingresso.

Solitamente per le **impronte** vengono utilizzati 128 bit, ma il valore può essere qualsiasi, tenendo conto che più basso è e più alta è la probabilità di collisione.

funzione hash Nel linguaggio matematico e informatico, la funzione hash è una funzione non iniettiva (e quindi non invertibile) che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione.

Firma digitale e **slide**

Classificazione tecniche **crittografiche**

Sicurezza e crittografia