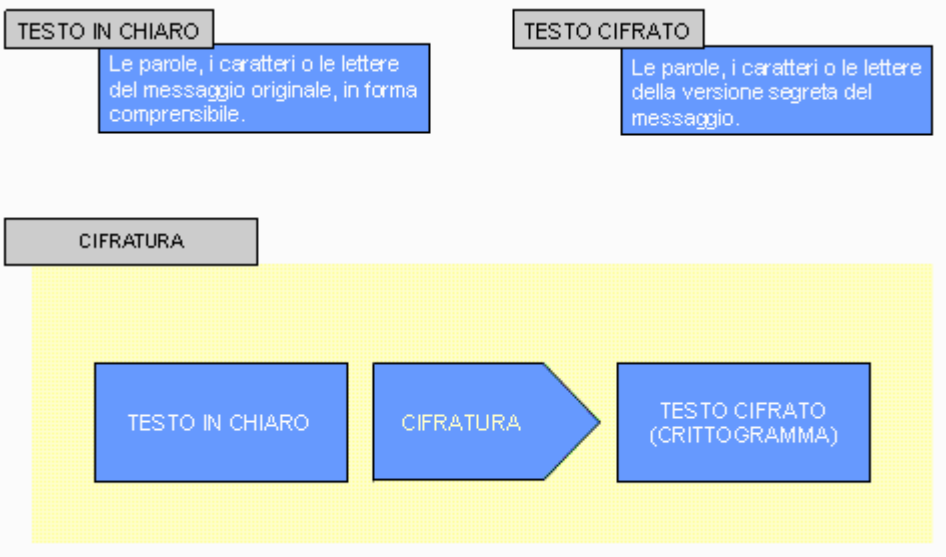
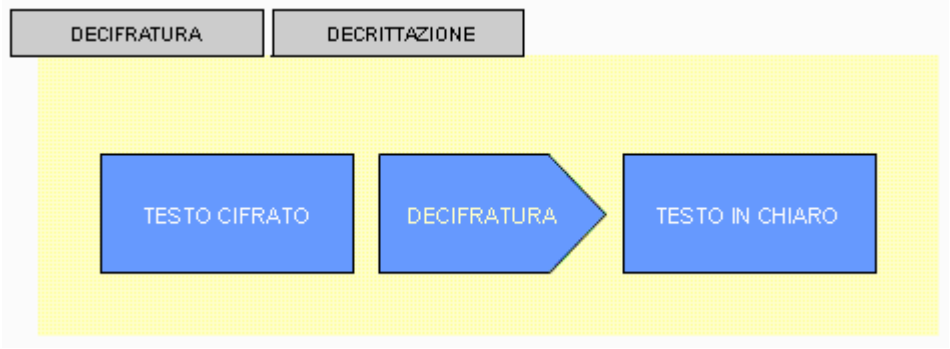
Terminologia

Prima di tutto vediamo cosa si intende per testo in chiaro, testo cifrato e cifratura.

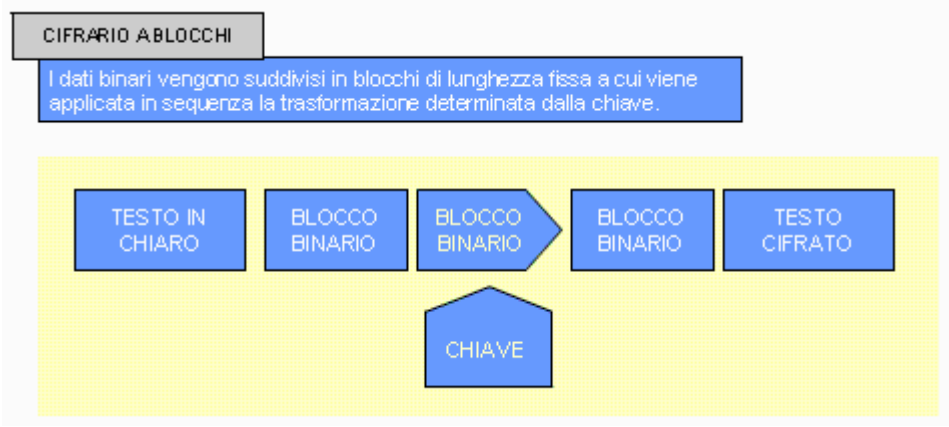


E' evidente che la cifratura non è altro che il procedimento che ci permette di ottenere il testo cifrato, o crittogramma, partendo dal testo in chiaro.

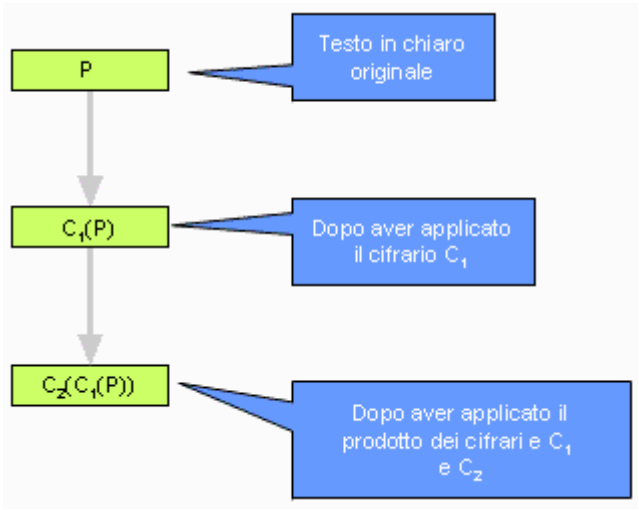
L'operazione opposta, cioè il passaggio dal testo cifrato al testo in chiaro, prende il nome di decifratura, se eseguita dall'utente legittimo oppure di decrittazione se eseguita da un utente esterno non autorizzato, utilizzando strumenti di crittoanalisi

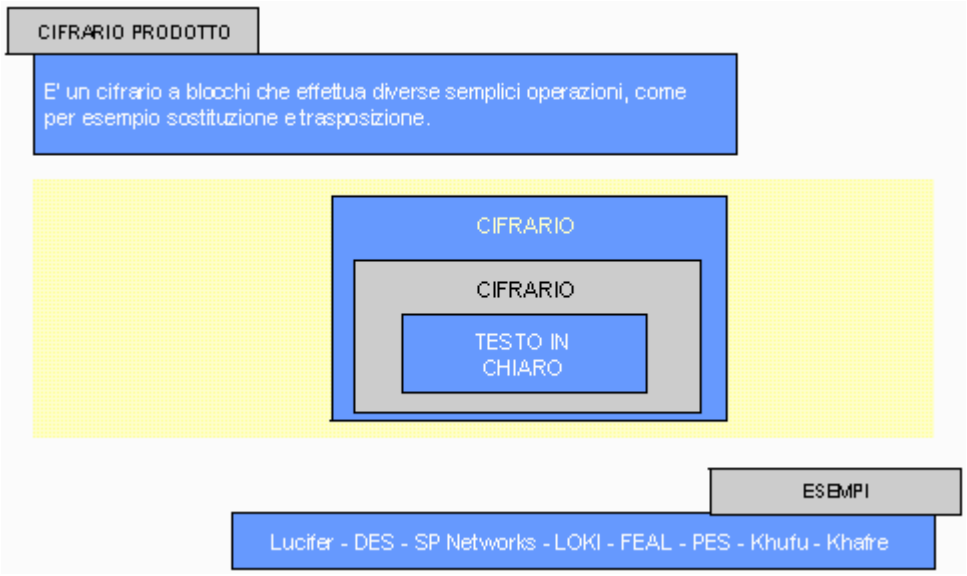


Iniziamo vedendo il cifrario più semplice, quello a blocchi.

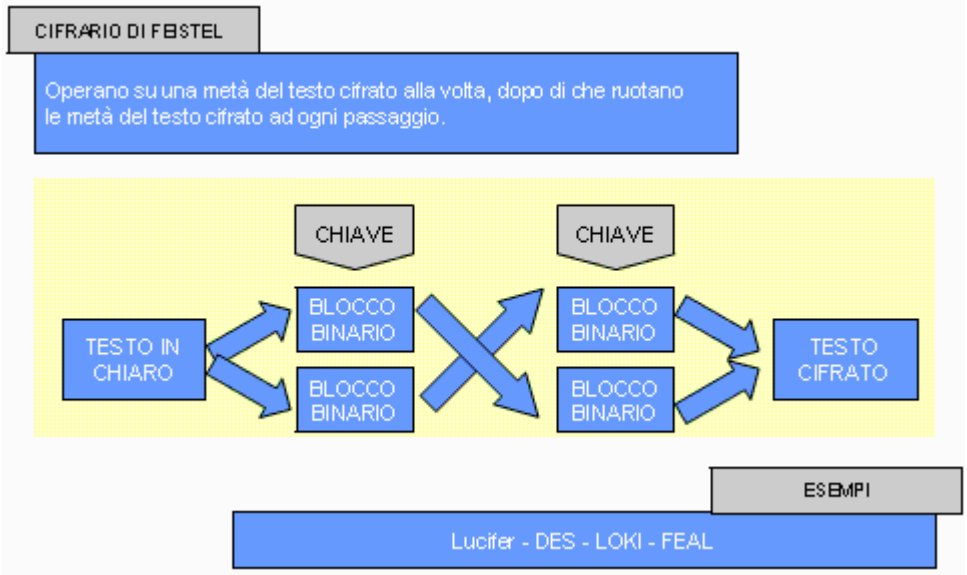


Dopo di che, passiamo al cifrario prodotto.

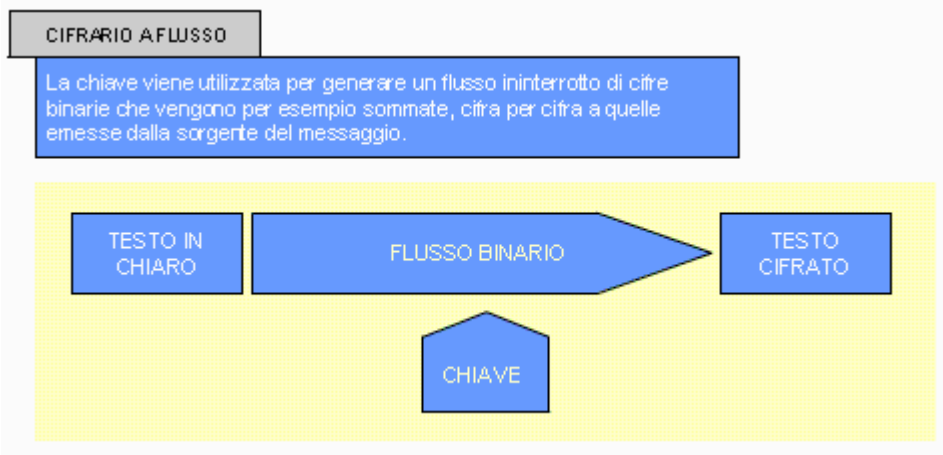




Come potete vedere dalla lista, il cifrario prodotto, per la sua semplicità, è ampiamente utilizzato, così come un tipo particolare di cifrario, quello detto di Feistel, dal cognome del suo inventore, Horst Feistel.



Non posso fare a meno di inserire, in questa breve introduzione, almeno un altro tipo di cifrario, largamente utilizzato, e cioè quello a flusso.



Al termine cifrario è associato sempre quello di procedimento. E' naturale quindi proseguire il discorso, concentrandosi su questi ultimi.

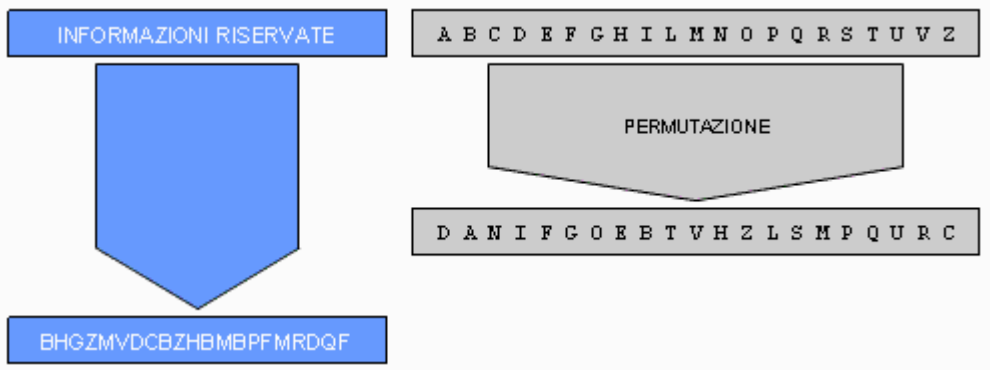
I procedimenti possono essere differenziati per il sistema di codifica utilizzato. In particolare:

- Tipo di trasformazione usata:
  - Sostituzione;
  - Trasposizione;
  - Sostituzione e trasposizione.
- Tipo di chiave di codifica e decodifica:
  - Sistemi a chiave privata;
  - Sistemi a chiave pubblica.
- Invertibilità o meno dell'algoritmo di codifica:
  - Invertibili;
  - Non invertibili.

Sostituzione

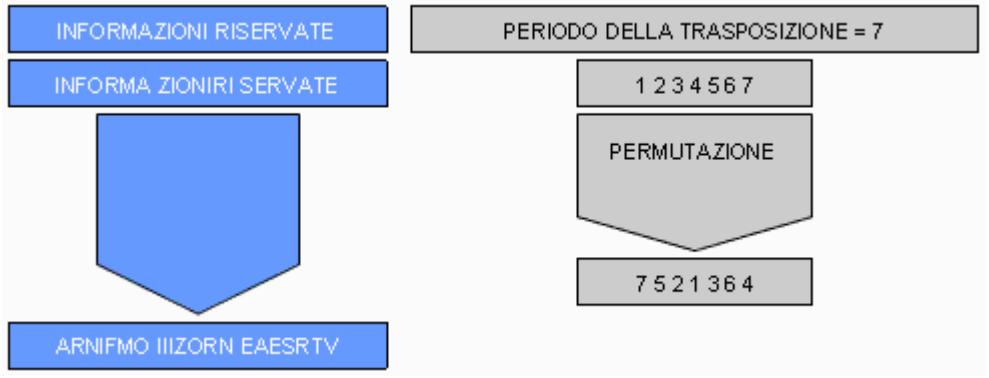
E' un'operazione con la quale gli elementi del testo in chiaro vengono sostituiti con altri elementi secondo apposite regole, note esclusivamente ai corrispondenti.

Nell'esempio seguente, partendo dal testo in chiaro 'informazioni riservate', colui che dovrà cifrare, utilizzerà l'alfabeto permutato deciso in precedenza con il corrispondente, riportato a destra. Il corrispondente, ricevuto il crittogramma, effettuerà la stessa operazione al contrario per ottenere nuovamente il testo in chiaro.

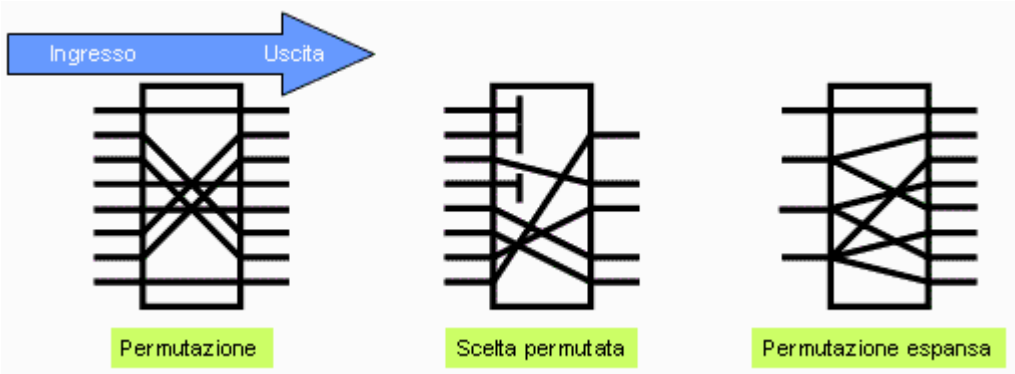


Trasposizione

La trasposizione, è un'operazione mediante la quale gli elementi di un testo in chiaro vengono cambiati di posto, ossia trasposti, secondo una regola stabilita in modo che la ricostruzione del testo in chiaro non sia possibile a chi non conosca quella regola.



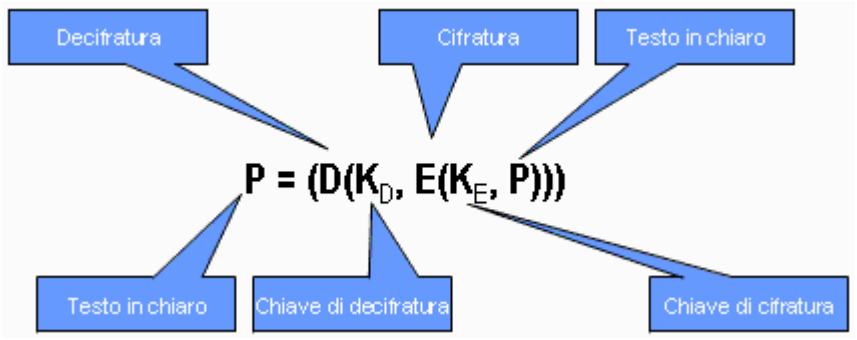
I tipi di permutazione a nostra disposizione sono diversi, per esempio, partendo da quella semplice, possiamo anche ottenere:



Crittografia Asimmetrica

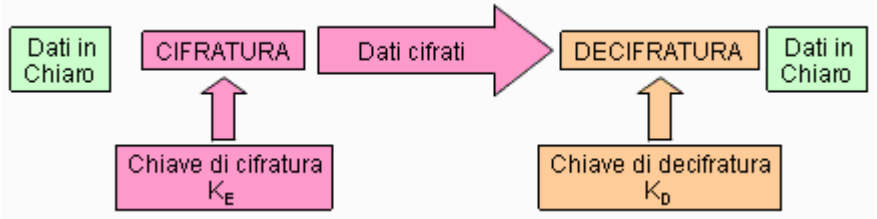
Modello utilizzato

In questo modello le chiavi di cifratura e decifratura sono utilizzate in coppia. In pratica una chiave di decifratura, K_D, inverte la cifratura della chiave K_E, così da avere:



Gli algoritmi di cifratura di questo tipo vengono detti asimmetrici, perché per convertire il dato dalla forma cifrata a quella in chiaro non basta invertire i passi di E.

Lo schema del modello è il seguente:



Vantaggi

La chiave pubblica può essere trasmessa tramite un canale insicuro, in quanto la sua conoscenza da parte di terzi non è sufficiente a mettere in pericolo la sicurezza dei dati crittografati con essa. Ciascuna chiave segreta resta sotto la responsabilità del solo utente proprietario.

In un sistema a chiave segreta per ogni possibile coppia di utenti deve esistere una chiave, per cui per n utenti occorrono:

$$\frac{n*(n-1)}{2}$$

chiavi; in un sistema a chiave pubblica deve esistere una coppia di chiavi per ogni possibile utente, ovvero per n utenti occorrono 2*n chiavi.

Esempio di combinazioni possibili:

Numero di utenti	Numero di chiavi in un sistema a chiave pubblica	Numero di chiavi in un sistema a chiave privata
10	20	45
100	200	4.950
1.000	2.000	499.500
10.000	20.000	49.995.000
100.000	200.000	4.999.950.000
1.000.000	2.000.000	499.999.500.000

Gli algoritmi simmetrici e quelli asimmetrici necessitano di chiavi di lunghezze differenti per raggiungere il medesimo grado di sicurezza teorica.

Simmetrica	Asimmetrica
56	384
64	512
80	768
112	1792
128	2304

La lunghezza raccomandata per la chiave è:

Anno	Privato	Azienda	Governo
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

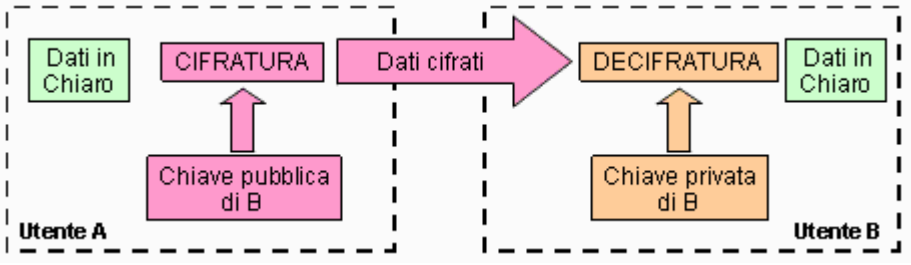
Svantaggi

Generalmente gli algoritmi asimmetrici sono molto più lenti da eseguire, rispetto a quelli simmetrici, per cui risulta poco agevole il loro uso per crittografare lunghi messaggi.

Caratteristiche

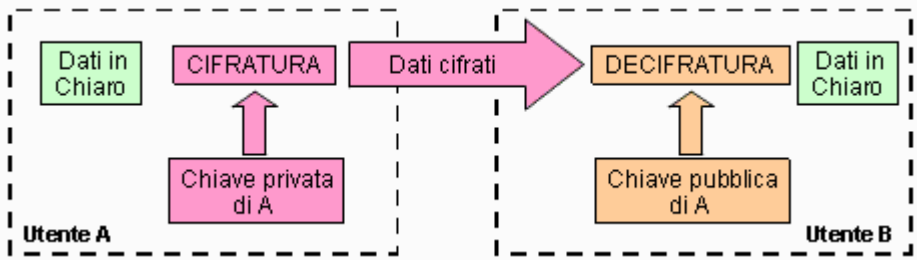
Riservatezza

L'utente A vuole inviare un messaggio all'utente B e lo cifra utilizzando la chiave pubblica di quest'ultimo. Solo il legittimo destinatario, l'utente B, utilizzando la propria chiave privata sarà in grado di decifrare il messaggio.



Autenticazione del mittente

L'utente A cifra il suo messaggio con la propria chiave privata. Chiunque, avendo accesso alla chiave pubblica di A, può decifrare quel messaggio. Se la procedura riesce, si è allora sicuri che esso è stato scritto dall'utente A, l'unico a possedere la corrispondente chiave segreta. L'utente A ha quindi posto la sua firma elettronica sul messaggio.

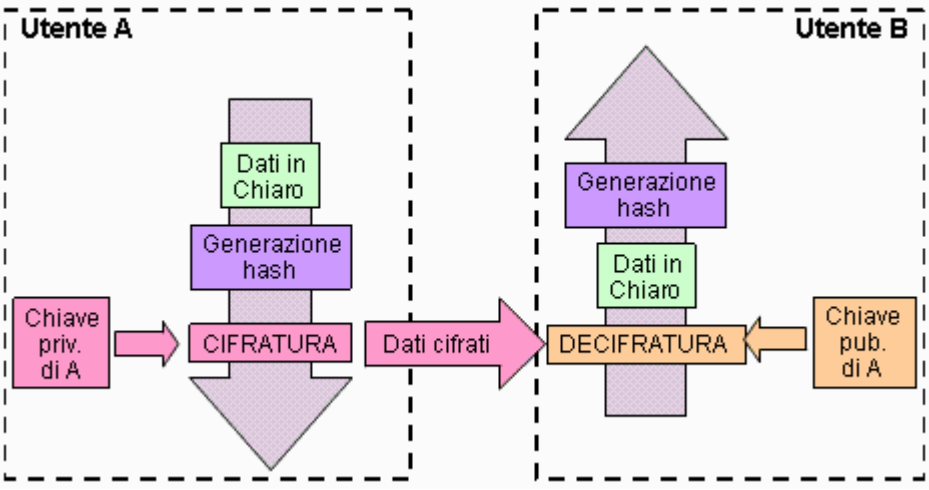


E' possibile autenticare oltre al mittente anche il contenuto del messaggio, generando un "hashing" dello stesso. Se il messaggio viene alterato, l'hash, aggiunto in fondo al messaggio, non corrisponde più.

Autenticazione del mittente e del messaggio

Il mittente può firmare con la propria chiave privata tutto l'insieme, oppure lasciare il messaggio vero e proprio in chiaro e firmare solo l'hash. Chiunque può decifrare l'insieme ricevuto o il solo hash con la chiave pubblica del mittente e così è sicuro dell'origine del messaggio.

Se inoltre, una volta effettuata la procedura, messaggio ed hash corrispondono, si è sicuri che nessuno dei due è stato alterato in qualche maniera.



Riservatezza ed autenticazione

E' possibile utilizzare contemporaneamente le due coppie di chiavi in modo da ottenere sia la riservatezza della comunicazione che l'autenticazione: L'utente A vuole inviare un messaggio all'utente B, e cifra il messaggio usando la chiave pubblica di quest'ultimo. Solo l'utente B, che ha la corrispondente chiave segreta, è in grado di decifrare e leggere il messaggio.

L’utente A cifra inoltre il suo messaggio con la propria chiave privata. Se l’utente B, che possiede la chiave pubblica dell’utente A, riesce nella decifrazione, è allora sicuro che esso è stato scritto dall’utente A, l'unico a possedere la corrispondente chiave segreta. L’utente A ha quindi posto la sua firma elettronica sul messaggio.