La crittografia

La crittografia è una branca della matematica che studia i metodi per trasformare un messaggio in modo che possa essere visibile solo alle persone autorizzate (tipicamente il mittente e il destinatario del messaggio) e non possa esser letto da terzi non autorizzati.

I primi esempi di crittografia risalgono ad alcuni secoli avanti Cristo.

Vediamo alcune definizioni:

- **Crittografia**: procedimento di cifratura e decifratura di messaggi basato su funzioni parametriche
- **Testo in chiaro**: messaggio originario
- **Algoritmo di cifratura**: effettua sostituzioni e trasformazioni sul testo in chiaro
- **Testo cifrato**: output dell'algoritmo di cifratura che risulta inintelligibile a un intruso
- **Algoritmo di decifratura**: effettua il lavoro inverso dell'algoritmo di cifratura
- **Chiave**: parametro dell'algoritmo di cifratura o decifratura

La sicurezza della cifratura dipende dalla segretezza della chiave piuttosto che dalla segretezza dell'algoritmo.

La tecnica della crittografia deve rispondere a diverse esigenze:

- **riservatezza** il messaggio o i dati devono essere accessibili solo alle persone autorizzate
- **integrità** l'informazione non può essere alterata durante il transito tra il mittente e il destinatario senza che sia rilevata l'alterazione
- **autenticazione** mittente e destinatario possono confermare l'identità dell'altro e l'origine/destinazione dell'informazione
- **non ripudio** sia il mittente che il destinatario non devono poter negare di aver inviato/ricevuto il messaggio o i dati.

Uno dei primi esempi di cifratura è quello chiamato «codice di Cesare» nel quale la lettera del testo in chiaro viene spostata di un numero fisso di posti.

Esempio:

Chiave: 3

Testo in chiaro: a u g u r i

Testo cifrato: d x j x u l

a u g u r i --> d x j x u l

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

La lettera **a** spostata di 3 posti diventa la lettera **d** e lo stesso avviene con gli altri caratteri.

Altro esempio di cifratura è quello chiamato «Vigenere» nel quale il testo cifrato si ottiene spostando ogni lettera del testo in chiaro di un numero fisso di caratteri, pari al numero ordinale della lettera corrispondente della parola chiave che è detta verme.

Esempio:

Testo in chiaro: DOMANI ARRIVANO I RINFORZI

Chiave (verme): CIAO

Testo cifrato: GWMOPQAFTQVOPWIFKVFCTHI

La chiave fa spostare i caratteri di 3 (C), 9 (I), 1 (A) e 15 (O) posizioni e si ripete finché non si cifra tutto il testo.

Vediamo che la lettera **d** viene spostata di 3 posti e diventa la lettera **g** e lo stesso avviene con gli altri caratteri.

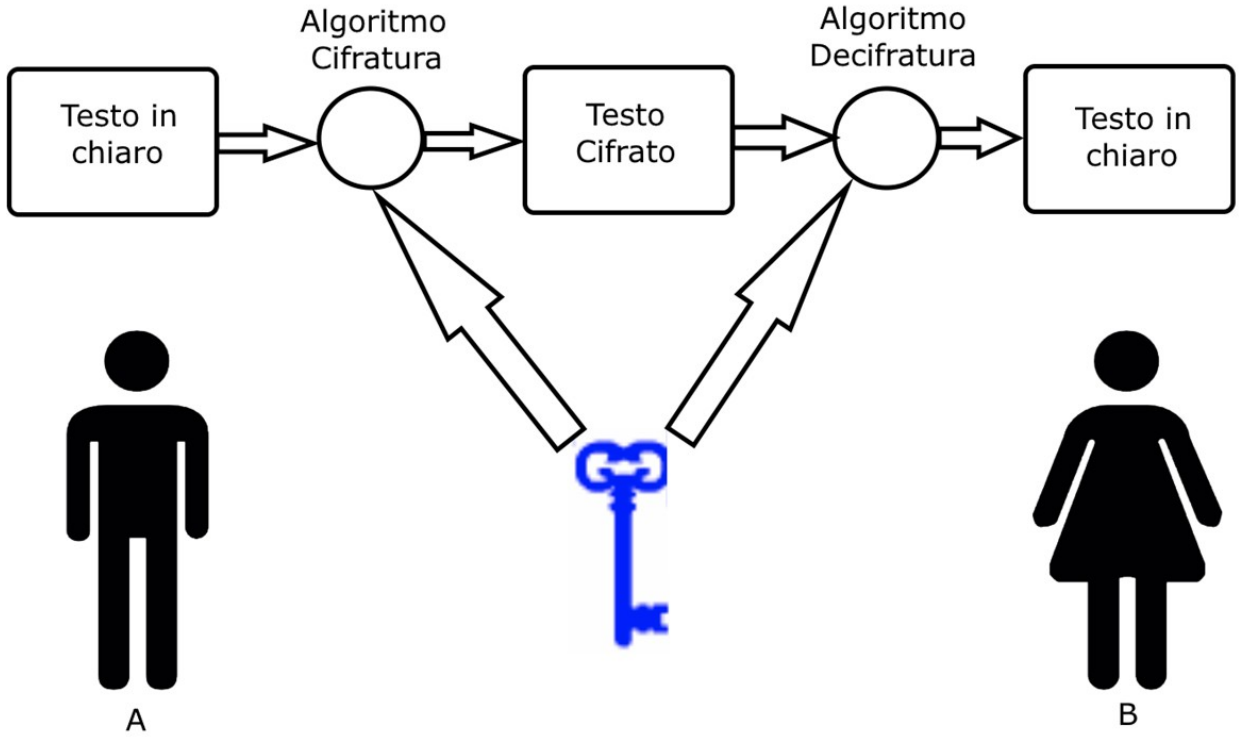
Per riottenere il testo in chiaro si fa il passaggio inverso.

Gli algoritmi attualmente in uso nella crittografia si possono suddividere in algoritmi a:

- **chiave simmetrica** – in questo caso esiste una sola chiave che deve essere condivisa e tenuta segreta tra chi crea il testo in chiaro ed il destinatario del messaggio.
- **chiave asimmetrica** – in questo caso esistono due chiavi diverse legate tra loro la chiave privata e la chiave pubblica ed ambedue possono essere utilizzate per la cifratura e la decifratura del testo in chiaro.

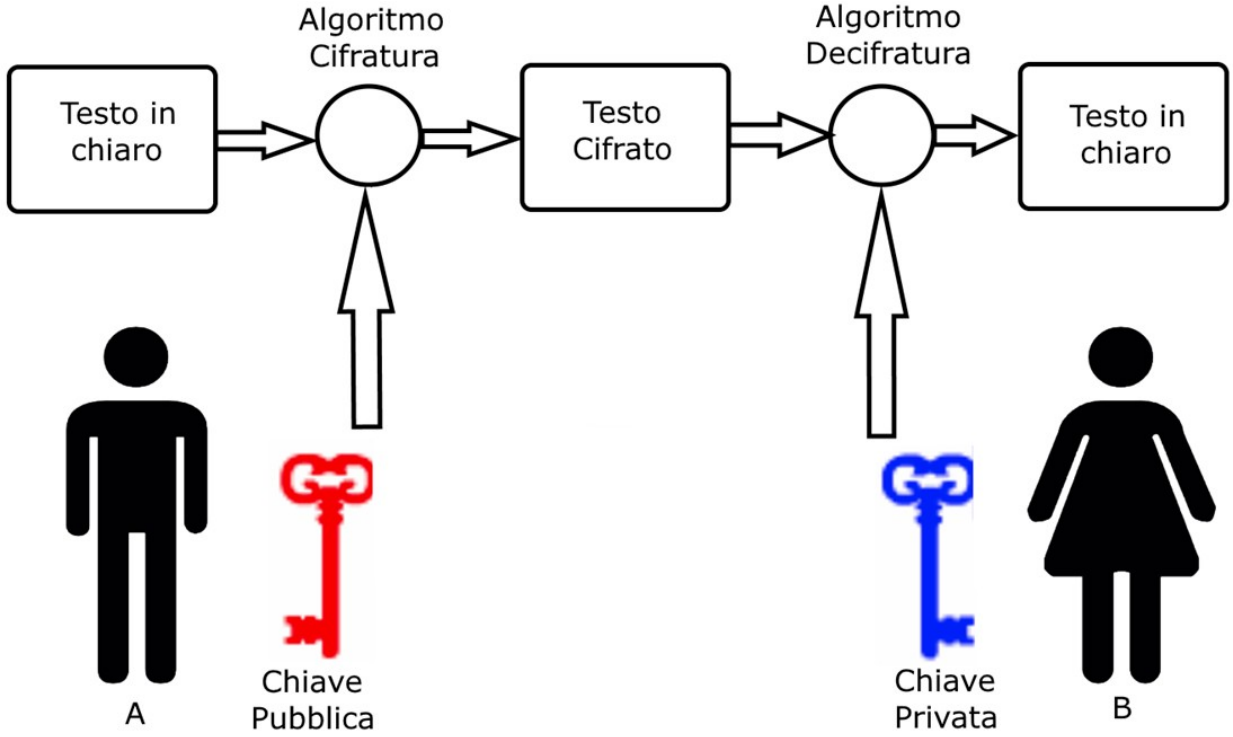
Crittografia a chiave simmetrica

Esiste una sola chiave che deve essere tenuta segreta e deve essere nota solo a chi crea il testo in chiaro (A) ed al destinatario del messaggio (B).



Crittografia a chiave asimmetrica

Esiste una chiave pubblica ed una chiave privata.



Crittografia asimmetrica semplice:

A esegue la cifratura utilizzando la chiave pubblica di B che poi lo decifrerà con la sua chiave privata.

Crittografia asimmetrica a doppia codifica:

A esegue la cifratura utilizzando propria chiave privata e successivamente la chiave pubblica di B che poi lo decifrerà utilizzando prima la propria chiave privata e poi la chiave pubblica di A.

Esempi di applicazioni:

- certificati e public key infrastructure
- protocolli di trasporto ssl, tls e ssh
- protocolli di autenticazione di livello 2
- virtual private networks
- altre applicazioni
  - ◆ one time passwords
  - ◆ documenti crittografati
  - ◆ filesystem

La firma digitale

La firma digitale è l'equivalente elettronico di una tradizionale firma autografa apposta su carta ed ha lo stesso valore legale.

La firma digitale viene associata ad un documento informatico sotto forma di **digest** (riassunto) che viene allegato al messaggio e spedito in coda al medesimo.

La fima digitale attesta:

- **integrità**
- **autenticazione**
- **non ripudio**
- **valore legale**

Il documento informatico sottoscritto con firma digitale deve rispettare le regole tecniche stabilite ai sensi del D.L. n.82-CAD del 7 marzo del 2005 che garantiscono l'identificabilità dell'autore e l'integrità del documento.

La firma digitale si basa sul sistema di crittografia asimmetrica e

può essere richiesta da:

- singoli cittadini
- imprese
- pubbliche amministrazioni

La **firma digitale** è divenuta obbligatoria per le aziende che devono quindi dotarsi di tale strumento.

La **firma digitale** viene rilasciata sotto forma di un certificato da **enti certificatori** i quali sono responsabili non solo del rilascio ma anche della gestione e della revoca del medesimo.

Una firma digitale non è valida se non lo è il suo certificato ed ogni certificato ha una scadenza temporale per cui deve essere rinnovato periodicamente.

La rete VPN

Una rete VPN (Virtual Private Network) è una rete privata virtuale che permette a computer situati in sedi fisiche diverse di stabilire un collegamento sicuro, affidabile e poco costoso.

Questo tipo di collegamento in sostanza consente alle aziende di fare in modo che:

- i dipendenti che lavorano fuori sede possono accedere in modo sicuro a dati e programmi aziendali
- le sedi dell'azienda (sparse sul territorio) possono comunicare tra di loro in modo affidabile
- condividere il lavoro con altre aziende creando una rete VPN per le comunicazioni e lo scambio di dati

Nelle reti VPN i dati viaggiano crittografati per assicurarsi la protezione da attacchi esterni.