Principi di Crittografia

Classe 5ASI
ITCG Fermi

Definizioni

- **Riservatezza** (o **confidenzialità**, o **segretezza**) **dei dati**: dati leggibili e comprensibili solo dalle persone autorizzate
- **Integrità dei dati**: dati letti e/o modificati solo da persone autorizzate
- **Disponibilità dei dati**: dati devono essere disponibili in qualunque momento per le persone autorizzate per cui occorre garantire la continuità del servizio
- **Paternità** (o **non ripudiabilità**) **dei dati**: ogni dato deve essere associato ad un utente che non può ripudiare i dati da lui spediti e/o firmati.
- **Autenticazione** ("o" **autenticità**): processo di riconoscimento delle credenziali dell'utente per assicurarsi dell'identità di chi invia e/o esegue operazioni.
  Metodi di verifica dell'identità di un utente: (1) informazioni riservate (es. password), (2) oggetti elettronici (es. smart card), (3) strumenti di riconoscimento biometrici (es. impronta digitale, fondo retina ecc.)
- **Autorizzazione**: per l'utente autenticato occorre stabilire l'insieme delle autorizzazioni (azioni permesse, risorse accessibili, dati consultabili e/o modificabili)

Crittografia

Problema: le reti, per loro natura, non sono sicure, infatti basta un **analizzatore di rete** (o **packet sniffer**) come **Wireshark** per intercettare le informazioni (per fortuna cifrate) che viaggiano su una rete.

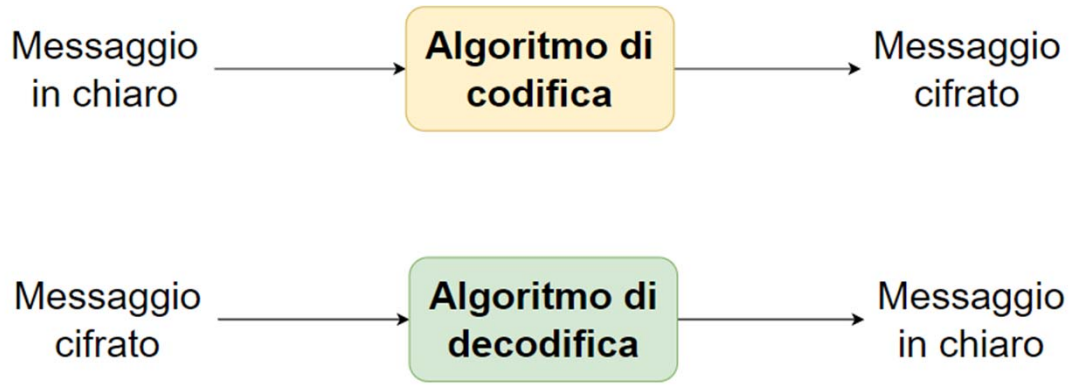
Crittografia (o **criptografia**, o **crittaggio**, o **criptaggio**, o **cifratura**, o **codifica**, o **codificazione**): significa *scrittura nascosta*, e riguarda i metodi per rendere un messaggio non comprensibile a persone che non sono autorizzate a leggerlo.

Algoritmo di codifica (o **a. di cifratura**, o **a. di criptazione**): metodo per trasformare i simboli in chiaro, i quali compongono il messaggio in chiaro, in simboli cifrati i quali compongono il messaggio cifrato.

Algoritmo di decodifica (o **algoritmo di decifratura**): metodo per trasformare i simboli cifrati in simboli in chiaro.

Prof. Montemurro

Crittografia



Prof. Montemurro

Crittografia

Approfondimento

Differenza tra codifica e cifratura in crittografia

- **Codifica**: metodo che consiste nel sostituire alcune parole con altre
- **Cifratura**: metodo che consiste nel sostituire lettere o caratteri

Cifrario: sistema convenzionalmente stabilito, per tradurre il linguaggio chiaro in linguaggio segreto, comprensibile soltanto a chi sia a conoscenza della convenzione

Esempio

Vogliamo inviare la parola AIUTO.

- Metodo di codifica: invece di trasmettere AIUTO, trasmetto HELP, cioè sostituisco completamente la parola AIUTO con un'altra
- Metodo di cifratura: invece di trasmettere AIUTO, trasmetto BLVUP; in questo caso ciascuna lettera è stata sostituita con quella che la segue nell'alfabeto.

Prof. Montemurro

Cifratura Simmetrica e Asimmetrica

Crittografia si basa su due elementi fondamentali:

1. l'algoritmo di codifica;
2. le **chiavi** (o **parametri**); nell'esempio precedente, la chiave è la posizione del carattere sostitutivo (un carattere in avanti nell'alfabeto se inviamo BLVUP invece di AIUTO).

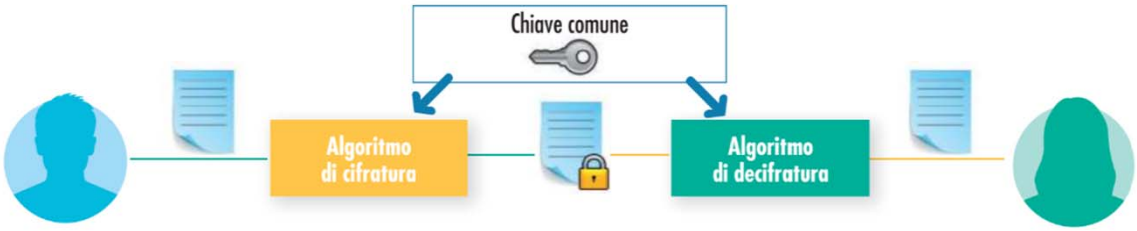
Chiave di cifratura + algoritmo di cifratura: servono per trasformare un messaggio in chiaro in un messaggio cifrato.

Chiave di decifratura + algoritmo di decifratura: servono per trasformare un messaggio cifrato in un messaggio in chiaro.

Prof. Montemurro

Cifratura Simmetrica e Asimmetrica

Cifratura simmetrica: chiave di cifratura e chiave di decifratura coincidono; in questo caso si parla di **chiave comune**.



Cifratura Simmetrica e Asimmetrica

Cifratura asimmetrica: chiave di cifratura e chiave di decifratura non coincidono; in questo caso la chiave di cifratura è chiamata **chiave pubblica** (o **Public Key**) **PK** in quanto è disponibile per chiunque, e la chiave di decifratura è chiamata **chiave privata** (o **private key**, o **Secret Key**) **SK** la quale è posseduta solo dal destinatario del messaggio cifrato.
Il destinatario (non il mittente) genera la coppia di chiavi (pubblica e privata); la chiave privata la tiene per sé, mentre la chiave pubblica la rende nota a tutti, compreso il potenziale mittente del messaggio. Il mittente userà la chiave pubblica inviatagli dal destinatario per criptare il messaggio; tale messaggio potrà essere decriptato solo dal destinatario in quanto solo lui possiede la chiave privata.

Cifratura Simmetrica e Asimmetrica

Esempio

Il destinatario compra un lucchetto, la chiave se la tiene, e manda il lucchetto aperto al mittente. Il mittente scrive il messaggio, lo chiude in una scatola di ferro che poi sigilla col lucchetto inviatogli dal destinatario. Dunque tale scatola può essere aperta solo dal destinatario in quanto solo lui ha la chiave del lucchetto.

Cifratura Simmetrica e Asimmetrica

Problema della cifratura asimmetrica: anche se il destinatario può verificare che nessuno abbia letto o modificato il messaggio durante il suo viaggio lungo la rete, purtroppo il destinatario non può verificare la paternità del messaggio, cioè non può avere la certezza del mittente. Ciò perché la chiave pubblica è per l'appunto pubblica per cui chiunque può usarla per cifrare un messaggio ed inviarlo al destinatario spacciandosi per un mittente noto al destinatario (es. Bob è amico di Alice; Alice condivide la chiave pubblica e si tiene la chiave privata; può capitare che un'altra persona usi la chiave pubblica per cifrare un messaggio e inviarlo ad Alice spacciandosi per Bob).

Soluzione per avere non ripudiabilità del mittente e del destinatario: **cifratura a doppia codifica**.

Cifratura a Doppia Codifica

Premessa: il mittente A genera una coppia di chiavi, la chiave privata A e la chiave pubblica A. Il destinatario B genera un'altra coppia di chiavi, la chiave privata B e la chiave pubblica B.

1. Il mittente A codifica il messaggio che vuole inviare a B con la propria chiave privata A (il contrario della cifratura asimmetrica); questa codifica garantisce la non ripudiabilità del mittente A, in quanto il destinatario B può leggere il messaggio di A solo utilizzando la chiave pubblica che il mittente A gli ha inviato (ricorda che solo la chiave pubblica che è stata generata insieme alla chiave privata può decodificare i messaggi cifrati con la chiave privata stessa).
2. Successivamente il mittente A sottopone il messaggio ad una seconda codifica usando la chiave pubblica B generata dal destinatario B. Ciò garantisce la riservatezza del messaggio in quanto solo il destinatario B è in possesso della chiave privata B in grado di decifrare il messaggio.

Prof. Montemurro

Cifratura a Doppia Codifica

3. Il destinatario B decodifica il messaggio usando la propria chiave privata B. Ciò garantisce:
   i. la riservatezza del messaggio (già detto prima);
   ii. la non ripudiabilità del destinatario B, cioè B non può negare di aver ricevuto il messaggio (prima abbiamo parlato della non ripudiabilità del mittente A) "in quanto" solo il destinatario B è in possesso della chiave privata B in grado di decifrare il messaggio inviatogli da A.
4. Successivamente il destinatario B sottopone il messaggio ad una seconda decodifica usando la chiave pubblica che il mittente A gli ha inviato. Ciò garantisce la non ripudiabilità del mittente A (già detto).

Prof. Montemurro

Cifratura a Doppia Codifica

Crittoanalisi

Crittoanalisi (o **criptoanalisi**): metodi di ricostruzione del testo in chiaro a partire da uno o più testi cifrati di cui non si possiede la chiave.

Criptosistema (o **crittosistema**, o **sistema criptografico**, o **sistema crittografico**, o **sistema di cifratura**): è una quintupla costituita da (1) algoritmo di codifica, (2) algoritmo di decodifica, (3) testo in chiaro, (4) testo cifrato, e (5) la chiave.

Principio di Kerckhoffs: la sicurezza di un crittosistema deve dipendere solo dalla segretezza della chiave, e non dalla segretezza dell'algoritmo di codifica e decodifica usato (in genere l'algoritmo è noto in quanto è uno standard).

Obiettivo dei cracker: individuare la chiave (visto che l'algoritmo è in genere noto).

One-Time Pad

One-Time Pad: è chiamato cifrario assolutamente sicuro; mittente e destinatario, per comunicare in modo segreto, condividono un blocco di testo (**pad**) costituito da una sequenza di lettere casuali, lunga quanto il messaggio da inviare. Questa sequenza viene condivisa segretamente in anticipo tra le due parti, cioè prima della comunicazione vera e propria.
La chiave cambia per ogni lettera, nel senso che non si usa la stessa regola di sostituzione per l'intero messaggio, ma una chiave diversa per ogni carattere del messaggio.

Esempio

Il messaggio CIAO viene codificato in ZUCY usando la chiave XMCK. Si considera A = 0, B = 1, C = 2 e così via. La lettera C viene codificata usando la chiave X (X = 23) per cui 2 + 23 = 25 = Z. Per decifrare:
numeroLetteraCodificata - numeroChiave = 25 - 23 = 2 = C