Crittografia e sicurezza

Cos'è?

La crittografia è lo studio della codifica e della decodifica dei dati. Il termine crittografia viene dalle parole greche "kryptos" che significa nascosto, "graphia", che significa scrittura.

Perché la crittografia?

La crittografia risponde alla maggior parte dei servizi contemplate nelle architetture di sicurezza stabile della ISO (International Organization for Standardization) che individuate cinque classi di funzionalità necessaria per garantire il desiderato livello di sicurezza:

- Confidenzialità
- Integra dei dati
- Autenticazione
- Non ripudio
- Controllo degli accessi

Pertanto, i sistemi di crittografia rivestono un'importanza fondamentale nella soluzione di molte problematiche di sicurezza connesse con la protezione di informazioni.

Perché la crittografia: Confidenzialità

Con tale funzionalità si vuole impedire di rivelare informazioni riservate ad entità non autorizzate alla conoscenza di tali informazioni; la confidenzialità è ottenuta tramite tecniche crittografiche di cifratura dei dati.
Nella vita reale:

- Invio di lettera chiusa
- Documenti in cassaforte

Perché la Crittografia: Integrità dei dati

I servizi dei dati proteggono contro gli attacchi attivi finalizzati ad alterare illegittimamente il valore di un dato; l'alterazione di un messaggio può comprendere la cancellazione, la modifica, o il cambiamento dell'ordine dei dati.

- Attacco passivo: un attacco con cui un intrusione intercetta semplicemente un flusso di informazioni senza apportare alcun genere di modifiche
- Attacco attivo: l'intrusione introduce alterazione di flusso di dati che possono comprendere modifica del contenuto informativo, eliminazione di tutto o solo di alcune parti del messaggio o trattenimento del messaggio per poi replicarlo in tempi successive.

Perché la Crittografia: autenticazione.

I servizi di autenticazione garantiscono l'accertamento dell'identità, quando a qualcuno (o qualcosa) si attribuisce una certa identità, i servizi di autenticazione forniscono lo strumento con cui verificare la correttezza di tale affermazione di identità.
Servizi di autenticazione dell'entità; in questo caso si autentica l'identità presentata ad un entità remota che partecipa ad un sessione di comunicazione (es. le password)

Servizi di autenticazione dell'origine dei dati: in questo caso si autentica l'identità che l'originatore di un messaggio rivendica di avere.

Perchè la Crittografia: Non ripudio

Tali servizi hanno la finalità di impedire che un'entità riesca successivamente a rinnegare con successo la partecipazione a transizione o comunicazione a cui in realtà ha preso parte, i servizi di non ripudio non prevengono il ripudio di una comunicazione di una transazione, forniscono, invece, gli elementi per dimostrare in caso di contenzioso l'evidenza dei fatti.

È lo strumento con cui dimostrare ad una terza parte e dopo l'accadimento del fatto che una comunicazione o transizione è stata originata o avviata da una certa entità o consegnata una certa entità.

Perché la Crittografia: Controllo degli accessi

Una volta che l'autenticazione è avvenuta, è possibile eseguire un controllo degli accessi in modo tale da verificare che vengano utilizzate solo quelle risorse o servizi ai quali si è autorizzati.

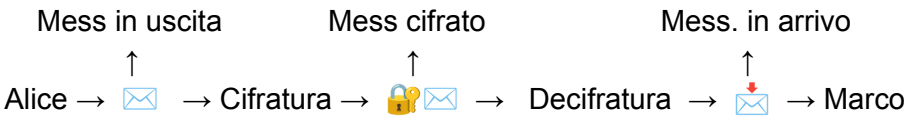
Definizione tecnica

La crittografia è una tecnica dei messaggi che mira a nascondere il contenuto informativo a tutti coloro che non dispongono di opportuni codici, password o chiavi di accesso. In assenza di sistemi di sicurezza il paradigma della comunicazione è:

Mittente	→	Invia messaggio	→	Destinatario
Alice	→	✉️	→	Marco

mentre con una comunicaazione sicura esso diventa:

1. Il mittente cifra il messaggio
2. Il mittente invia il messaggio cifrato al destinatario attraverso un canale non sicuro
3. Il destinatario decifra il messaggio



Un sistema di crittografia è rappresentato da due elementi essenziali:

- Algoritmi di crittografia
- Chiavi di crittografia

Gli algoritmi di crittografia implementano procedure matematiche finalizzate a cifrare e a decifrare i dati, trasformando i dati in chiaro in dati cifrati e viceversa.

Esistono due tipi principali di algoritmi di crittografia:

- Algoritmi a chiave simmetrica (o chiave segreta) utilizzano la stessa chiave per cifrare e decifrare i dati; la sicurezza di questi algoritmi dipende dalla segretezza della chiave utilizzata

- Algoritmi a chiave asimmetrica (o chiave pubblica) utilizzano una coppia di chiavi, una chiave pubblica per cifrare i dati e una chiave privata per decifrarli. La chiave pubblica può essere condivisa liberamente, mentre la chiave privata dev'essere mantenuta segreta.

Chiavi di crittografia

Le chiavi di crittografia sono valori segreti utilizzati per cifrare e devifrare i dati.
Quindi la sicurezza di un sistema di crittografia dipende in gran parte dalla segretezza e dalla complessità delle chiavi utilizzate. Queste chiavi possono essere di diverse lunghezze e tipi a seconda dell'algoritmo di crittografia.

Chiavi simmetriche

La stessa chiave vine usata per cifrare e decifrare. La gestione delle chiavi è uno degli aspetti critici della crittografia, dovendo mittente e destinatario avere gli stessi codici, questi ultimi dovranno essere scambiati di persona inviati in chiaro oppure posono essere condivisi usando a loro volta un sistema di crittografia.

Chiavi asimmetriche

Necessita obbligatoriamente di una chiave pubblica e di una privata.