Si descriva lo schema di crittografia a chiave simmetrica e come esso viene utilizzato nella comunicazione tra due entità.

Nella crittografia a chiave simmetrica si usa la stessa chiave e lo stesso algoritmo per la codifica e la decodifica del messaggio.

Il problema principale di questo sistema riguarda la trasmissione della chiave. Poiché l'intercettazione della stessa comprometterebbe la segretezza della conversazione. Quindi la chiave va scambiata su un canale sicuro.

Tra i primi sistemi di crittografia a chiave simmetrica vi è la cifratura monoalfabetica: si spieghi come funziona tale schema e si indichi la dimensione dello spazio delle chiavi.

Il sistema di cifratura monoalfabetica si basa sul lo scambiare una lettera dell'alfabeto utilizzato *(es.alfabeto italiano se il messaggio originale è in italiano)* con un altra dello stesso alfabeto. Le chiavi possibili sono n! con n = numero delle lettere dell'alfabeto perché è l'insieme delle possibili permutazioni delle lettere.

Si descriva lo schema di crittografia a chiave asimmetrica e come esso viene utilizzato nella comunicazione tra due entità.

Nella crittografia a chiave assimetrica ogni utente possiede una coppia di chiavi.*Una pubblica e una privata.* Il **mittente** codifica con la chiave **pubblica** del **destinatario** che lo decodifica con la propria chiave **privata**.

Il sistema a chiave assimetrica richiede molte risorse quindi viene usato per codificare e inviare una chiave da utilizzare durante il resto della sessione con un algoritmo a simmetrico.

Si descriva, anche attraverso esempi, su quali fattori si basa l'autenticazione degli utenti, indicando aspetti positivi e negativi di ciascun fattore.

L'autenticazione degli utenti si basa su tre fattori:

- **Qualcosa che si conosce:** per esempio un username e una password.
- **Qualcosa che si è:** per esempio l'impronta digitale del pollice o la propria retina. Vantaggi: elevata sicurezza Svantaggi:
- **Qualcosa che si possiede:** per esempio una smart key o un generatore di codici. Vantaggi: difficile da replicare Svantaggi: possibile perdita del possesso dell'oggetto

Si mostri lo schema di funzionamento di PGP (Pretty Good Privacy).

Il mittente concatena al proprio messaggio in chiaro l'hash del messaggio firmato con la propria chiave privata, viene compresso, codificato con la chiave pubblica del destinatario e quindi spedito in formato ASCII

Si spieghi cosa si intende per Access Control List, specificando dove sono memorizzate le informazioni e come vengono utilizzate.

L'access control list è un metodo di memorizzazione dei permessi di accesso a determinate risorse. Si rappresenta attraverso una matrice memorizzata per colonna. Ogni colonna rappresenta una risorsa e ogni riga rappresenta i soggetti che hanno accesso alle risorse.

Sono adatte ai contesti in cui è importante garantire la protezione delle risorse perché è facile gestire l'accesso alle risorse.

Si illustri, anche attraverso esempi, cosa si intende per politica di tipo "Default deny" adottata da un Firewall.

In caso di politica di "Default Deny" addottata per un firewall tutti i processi a cui non è stata dato preventivamente il consenso non possono comunicare con l'esterno.

Esempio: Un mio programma appena scritto non ha il permesso e non può comunicare con l'esterno. Un programma a cui è stato dato il permesso invece può comunicare.

Si descriva attraverso quali meccanismi vengono controllati gli accessi alle risorse di un sistema (ad esempio, file, directory, programmi), dopo che l'utente si è correttamente autenticato.

I meccanismi per il controllo degli accessi alle risorse sono principalmente 2:

- DAC Discretional access control Basato sulla proprietà di una risorsa, il proprietario può garantire l'accesso a quella risorsa a un altro utente. (Può concedere permessi uguali ai propri, quindi per esempio se ha solo l'accesso in lettura non può concedere l'abitazione in scrittura).
- MAC Mandatory access control Basato sull' idea della gerarchia militare, ogni utente non può leggere al di sopra di proprio livello di sicurezza e non può scrivere al di sotto.

Si descriva il funzionamento del Message Authentication Code (MAC) per l'autenticazione di un messaggio (non è necessario garantire la confidenzialità dei dati).

Il messaggio originale viene spedito in chiaro al destinatario insieme alla versione codificata con la propria chiave privata dell'hash del messaggio. Il destinatario decodificherà l'hash con la chiave pubblica del mittente e lo confronterà con quello arrivato in chiaro. Se gli hash combaceranno il messaggio sarà autentico perché vorrà dire che nessuno ha modificato il messaggio in chiaro oppure l'hash codificato. Questa procedura viene anche chiamata **Firma Digitale**.

Un sistema di rilevamento delle intrusioni (IDS, Intrusion Detection System) si può basare su diversi modelli: rilevamento della anomalie, oppure rilevamento di uso malevolo, oppure rilevamento in base a specifiche. Si spieghi il principio di funzionamento di uno tra questi modelli, anche attraverso esempi.

- **Rilevamento delle Anomalie:** Sequenze di azioni non usuali possono essere intrusioni: Per esempio troppi tentavi di accesso a Windows possono essere un tentativo di attacco di forza bruta.
- **Rilevamento di uso malevolo:** Questo modello si basa su la conoscenza a priori che una determinata sequenza di azioni possa essere dannosa per il sistema.
- **Rilevamento in base a specifiche:** Si determina se una sequenza di azioni viola una specifica di come il programma o un sistema dovrebbe funzionare.

    NDR: Ho dovuto copiarla pari pari dalle slide, perché è palesemente una supercazzola.

Si illustrino le caratteristiche che le funzioni hash devono possedere per poter essere utilizzate in ambito crittografico

Le funzioni hash devono possedere le seguenti caratteristiche:

- Unicità: Cioè dato dato un input, l'output deve essere unico.
- Lunghezza fissata: Cioè qualsiasi sia la lunghezza dell'input, l'hash risultante deve avere una lunghezza uguale.
- Coerenti: Cioè dati due input uguali, output deve essere uguale.
- Non inveritibili: Cioè preso l'output, risalire all'input senza la chiave adeguata deve risultare impossibile.

Si dia una breve spiegazione di ciascuno dei tre principali obiettivi della sicurezza (confidenzialità, integrità, disponibilità), anche con l'aiuto di esempi che mostrino come tali proprietà possano essere compromesse.

- Confidenzialità: Nessuno deve poter accedere ad informazioni a cui non ha diritto. Questo principio viene meno se per esempio un utente è in grado di leggere un file personale di un altro utente.
- Integrità: Le informazioni non devono poter essere manipolate da chi non ha diritto a farlo.
- Disponibilità: Le informazioni devono essere disponibili a chi ne ha diritto nei tempi e nei modi previsti.

0.0.1 Cos'è un URL? Qual è la sua sintassi?

URL è l'acronimo per uniform resource locator, ed è il sistema standard per indicare la posizione di una risorsa. la sua sintassi è:

protocollo://[username[:password]@]host[:porta]</percorso> [?querystring][♯fragment]

Relativamente al Certificato Digitale, si descriva come viene creato, da chi viene creato, cosa contiene e il suo utilizzo.

Il certficato digitale viene creato da una autorità di certificazione per certificare che un utente sia chi dice di essere. C