<table>
<tr><td>ITI VE III
PALERMO</td><td>LABORATORIO
SeR – CLASSE QUINTA INFORMATICA</td><td>PROVA

N°
1</td></tr>
<tr><td colspan="3">ESERCITAZIONE: Firmare digitalmente un documento e verificarlo.</td></tr>
<tr><td colspan="3">OBIETTIVI DELLA PROVA: Firmare un documento in digitale e verificarlo con la chiave pubblica del soggetto, estratta dal suo certificato rilasciato da una CA.</td></tr>
<tr><td rowspan="2">DATA
19/11/2024</td><td rowspan="2">IGNAZIO LEONARDO
CALOGERO SPERANDEO</td><td>CLASSE: 5 Sez. Inf</td></tr>
<tr><td>SPECIALIZZAZIONE INFORMATICA E TELECOMUNICAZIONI</td></tr>
</table>

- - - CENNI TEORICI - - -

La criptografia rappresenta un insieme di tecniche utilizzate per rendere incomprensibile un messaggio da parte di terzi. Si definisce cifrario, l'algoritmo di criptografia, che può utilizzare una o più chiavi, ossia l'elemento il cui valore consente di decifrare il messaggio e renderlo leggibile. Il cifrario è pubblico a tutti ma il valore della chiave deve rimanere segreto. Il numero di chiavi previste in una tipologia di criptografia dipende dal cifrario. Tra le principali tipologie di criptografia troviamo:

- **Criptografia a chiave simmetrica**
- **Criptografia a chiave asimmetrica**

La criptografia asimmetrica è una tipologia di criptografia che sfrutta due chiavi per la criptazione e decriptazione dei messaggi. In particolare le chiavi sono 2 e si distinguono in:

- **Chiave pubblica:** resa nota a tutti.
- **Chiave privata:** non deve essere resa nota a tutti, la deve custodire solo il proprietario.

La chiave pubblica e la chiave privata sono matematicamente correlate tra di loro, il che significa che cifrando con la chiave pubblica un messaggio tale potrà essere decifrato soltanto da chi possiede la chiave privata e viceversa. Un altro aspetto molto importante della criptografia asimmetrica è quello che a partire dalla chiave privata si può risalire alla chiave pubblica ma non il viceversa. In particolare non è impossibile risalire dalla chiave pubblica alla chiave privata ma risulta essere un operazione inversa, matematicamente complessa. Sebbene ci sono diversi tipi di attacchi che potrebbero calcolare la chiave privata a partire dalla pubblica, a seconda della lunghezza delle chiavi, richiederebbe molto tempo di calcolo come ad esempio il Brute Force. Proprio per questo la criptografia asimmetrica è un sistema più sicuro rispetto alla criptografia simmetrica. Ma nonostante ciò, la criptografia simmetrica risulta essere più veloce rispetto alla criptografia asimmetrica.
Attraverso la criptografia asimmetrica si hanno 3 possibili scenari, ognuno dei quali garantisce una determinata sicurezza.

Il primo scenario prevede che il messaggio da inviare ad un destinatario (Bob) da parte del mittente (Alice), venga cifrato con la chiave privata di Alice e decifrato, da parte di Bob, con la chiave pubblica di Alice. Questo scenario garantisce l'identità del mittente che ha inviato quel messaggio, ma nonostante ciò, il messaggio cifrato risulta decifrabile da tutti, in quanto la chiave pubblica di Alice è disponibile a tutti. Su questo scenario si basa il funzionamento della firma digitale.

Il secondo scenario prevede che il messaggio da inviare a Bob da parte di Alice, venga cifrato con la chiave pubblica di Bob e decifrato, da parte di Bob, con la chiave privata di Bob. Questo scenario garantisce la segretezza, perché l'unico modo per poter decifrare il messaggio è utilizzando la chiave privata di Bob. Utilizzando questo scenario non si ha la garanzia che il messaggio provenga da Alice.

Il terzo e ultimo scenario, garantisce sia la l'identità e sia la segrettezza. In particolare, il messaggio che Alice dovrà inviare a Bob verrà, inzialmente, cifrato con la chiave privata di Alice (autocertificazione) e infine verrà cifrato con la chiave pubblica di Bob (riservatezza). Bob per poter decifrare completamente, il messaggio arrivato da Alice, dovrà prima, decifrare con la chiave privata di Bob e infine decifrare, nuovamente, attraverso la chiave pubblica di Alice. In questa maniera Bob è sicuro che il messaggio provenga da Alice e che nessuno lo possa decifrare. Questo tipo di scenario è utilizzato per lo scambio di chiavi di sessioni.

La firma digitale è un tipo di firma elettronica qualificata che garantisce:

- **Autenticità:** garantisce l'identita di chi ha firmato il documento.
- **Non ripudio:** garantisce che il documento ha piena validità legale.
- **Integrità:** garantisce che il documento firmato, non venga modificato dopo la firma.

La firma digitale si basa sulla criptografia asimmetrica, infatti per firmare digitalmente un documento bisogna seguire i seguenti passaggi:

1. **Calcolare l'hash** del documento da firmare, ottenendo un message digest.
2. **Cifrare il message digest** con la chiave privata di chi sta firmando il documento, questo passaggio determina la firma digitale di quel documento.

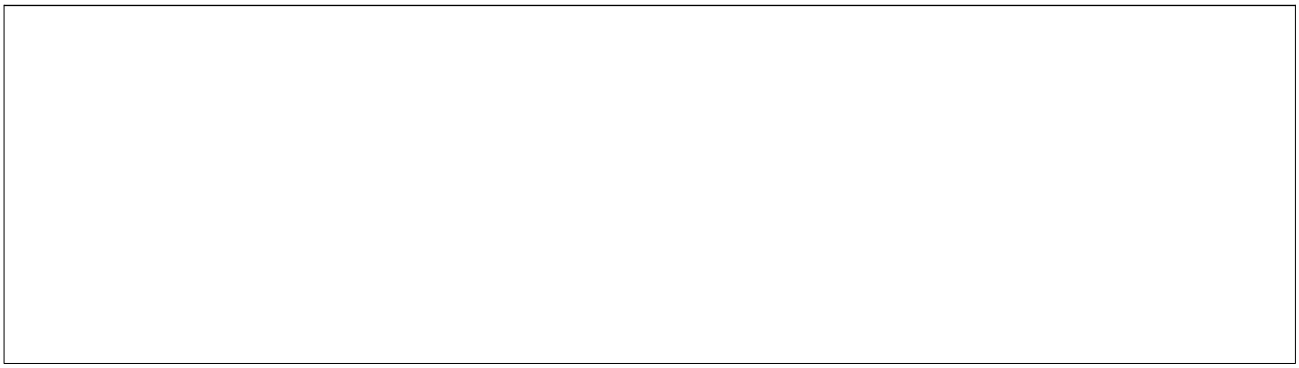
Per verificare l'autenticità di un documento firmato digitalemente da una persona (Alice) bisogna effettuare i seguenti passaggi:

- **Decifrare il message digest** del documento con la chiave pubblica di Alice
- **Calcolare l'hash** del documento ricevuto
- **Confrontare il message digest** decifrato con la chiave pubblica di Alice con il digest ottenuto in precedenza. Se i digest risultano uguali allora è garantito che il documento è stato firmato da Alice.

Il certificato digitale è un documento che attesta in maniera univoca l'associazione di una chiave pubblica con un soggetto, è principalmente costituito da:

- L'anagrafica del soggetto
- Chiave pubblica del soggetto
- Nome dell'ente che ha rilasciato il certificato, CA
- Scadenza del certificato
- Firma digitale della CA

Il formato più comune dei certificati è X.509 (proposto dall'ITU). Per ottenere un certificato digitale bisogna, inzialmente, generare una CSR (**Certificate Signing Request**), una richiesta di certificato che contiene la chiave pubblica e le informazioni del soggetto che ha fatto richiesta. La CSR dovrà essere mandata alla RA (**Registration Authority**) che si occuperà di verificare l'identità del soggetto e di verificare se il soggetto è idoneo per la ricezione del certificato. Se tutti i controlli effettuati dalla RA vanno a buon fine, la RA inoltrerà la richiesta alla CA (**Certificate Authority**) e tale genererà il certificato digitale firmandolo digitalmente. Uno strumento da riga di comando, che consente di eseguire una serie di operazioni legate alla sicurezza è openSSL. In questa esperienza di laboratorio verrà utilizzato openSSL per firmare digitalmente un documento e verificarlo.



- - - SVOLGIMENTO RELAZIONE - - -

Prefissati gli obiettivi dell'esperienza di laboratorio si procede con la generazione di una richiesta di certificato (CSR) attraverso l'uso del seguente comando:

openssl req -new -newkey rsa:2048 -nodes -keyout pri.pem -keyform PEM -out richiestaCertificato.csr

Questo comando creerà una chiave privata a 2048 bit utilizzando RSA, salvata nel file *pri.pem* e la richiesta di certificato salvata nel file *richiestaCertificato.pem.* Tutte le informazioni del soggetto chieste in input dal comando, possono essere pre-inserite attraverso l'uso del tag -subj.

La richiesta di certificato (richiestaCertificato.csr) dovrà essere presentata alla RA, che si occuperà di verificare se il soggetto che ha richiesto il certificato sia idoneo. La RA, non appena verifica che il soggetto sia idoneo, manda la richiesta di certificato alla CA. La CA dovrà generare il certificato e firmarlo digitalmente, tutto questo viene fatto attraverso l'uso del seguente comando:

openssl x509 -req -in richiestaCertificato.csr -CA ca.cert -CAkey ca.key -CAcreateserial -out Certificato.pem -days 365 -sha256 -keyform PEM

Attraverso questo comando la CA genera e firma digitalmente il certificato (in formato X.509). La firma del certificato avverrà utilizzando la chiave privata della CA (ca.key) e la funzione hash sha256.

Ottenuto il certificato digitale dalla CA, si procede con la firma digitale di un documento. Il documento di testo in questione riguarda la circolare di una scuola, la creazione del documento viene effettuatta attraverso il seguente comando:

echo 'In data 21/11/2024 le lezioni saranno sospese' > circ_21_11_2024.txt

Al documento si dovrà applicare una funzione di hash che genererà un message digest. Per fare l'hash del documento si utilizza il seguente comando:

openssl dgst -sha256 < circ_21_11_2024.txt > circ_21_11_2024.hash

Questo comando genererà il message digest utilizzando l'hash sha256 del documento di testo circ_21_11_2024.txt. Il message digest verrà salvato nel file circ_21_11_2024.hash.

Per firmare il documento si procede con l'esecuzione del seguente comando:

openssl rsautl -sign -inkey pri.pem -keyform PEM -in circ_21_11_2024.hash > firma_21_11_2024

Il file firma_21_11_2024 rappresenta la firma digitale del documento

circ_21_11_2024.txt, ossia il message digest cifrato con la chiave privata del firmatario del documento. Attraverso la chiave pubblica del firmatario del documento è possibile verificare la firma. La chiave pubblica si trova all'interno del suo certificato digitale, per estrarla si utilizza il seguente comando:

openssl x509 -in Certificato.pem -pubkey -noout > pub.pem

Per proseguire con la verifica della firma, viene decifrato il file firma_21_11_2024 con la chiave pubblica appena ottenuta:

openssl rsautl -verify -inkey pub.pem -keyform PEM -pubin -in firma_21_11_2024 > verifica_21_11_2024

Infine viene calcolato l'hash del documento e confrontato con quello appena decifrato:

openssl dgst -sha256 < circ_21_11_2024.txt > circ_21_11_2024.hash.ver

diff -s verifica_21_11_2024 circ_21_11_2024.hash.ver

Il comando diff, con il tag -s , manda a video un messaggio se i due file risultano uguali.
Per visualizzare i certificati è stato utilizzato il seguente comando:

openssl x509 -in Certificato.pem -text -noout

Per visualizzare la richiesta di certificato è stato utilizzato il seguente comando:

openssl req -in richiestaCertificato.csr -text -noout

NOTA:
L'esercitazione è stata svolta utilizzando il certificato della CA già rilasciato, assieme alla sua chiave privata, di nomi:

- ca.cert → certificato della CA
- ca.key → chiave privata della CA

* * * CONCLUSIONI * * *

L’esercitazione è stata svolta correttamente, seguendo passo dopo passo i comandi descritti nella sezione relativa allo svolgimento della relazione. Il certificato digitale (di cui si è fatta richiesta) è servito per poter ricavare la chiave pubblica di chi ha firmato il documento in digitale, consentendone la decrifratura della firma digitale e di conseguenza il confronto tra l’hash decifrato e l’hash del documento. In questa maniera è stato possibile verificare una firma digitale di un documento attraverso l’uso di openSSL.