Esercitazione 5 - Rsa/cifratura a chiave pubblica

Parte 1 - generare chiave pubblica e privata.

openssl genrsa -out *myKey.pem* ***-des3 1024****:*

genera la chiave segreta di 1024 bit.

more *myKey.pem:*

mostra a schermo la chiave

openssl rsa -in *myKey.pem* ***-text****:*

decifra e mostra a schermo la chiave privata

openssl rsa -in *mykey.pem* ***-pubout -out*** *pub.key:*

genera la chiave pubblica associata alla nostra chiave privata e la salva in un file.

Parte 2 - cifrare e decifrare un file.

*Creiamo un file di testo e lo chiamiamo "****plaintext.txt****".*

openssl rsautl -encrypt -pubin -inkey *pub.key* ***-in*** *plaintext.txt* ***-out*** *ciphertext.txt:*

cifra il file di testo utilizzando la chiave pubblica del destinatario.

openssl rsautl -decrypt -inkey *myKey.pem* ***-in*** *ciphertext.txt* ***-out*** *de_ciphertext.txt:*

decifriamo il file cifrato con la chiave privata del destinatario.

open *de_cipher.txt:*

apre il file decifrato per vedere se combacia con l'originale di partenza

Parte 3 - generare un message digest (codice hash) di un file.

echo *Bob. Buy 1000 IBM shares signed Alice* ***>*** *buyorder.txt:*

genera un file di testo.

openssl dgst -sha1 *buyorder.txt:*

genera l'SHA1 digest del file.

sha1sum *buyorder.txt:*

controlla lo SHA digest.

Parte 4 - firmare il message digest

openssl dgst -sha1 -sign *myKey.pem* ***-out*** *buyorder.txt.sha1 buyorder.txt:*

firmiamo il digest con la chiave privata del mittente.

openssl enc -base64 -in *buyorder.txt.sha1:*

per vedere la firma binaria nel formato base 64(formato ".pem").

openssl dgst -sha1 -verify *pub.key* ***-signature*** *buyorder.txt.sha1 buyorder.txt:*

il destinatario utilizza la chiave pubblica del mittente per verificare la sua firma.

Modifichiamo il file di testo ("buyorder.txt") a piacere e notiamo che se rieleggiamo la verifica essa non andrà più a buon fine.