Sistema criptogràfic

Aquesta pràctica consisteix a combinar primitives criptogràfiques per tal d'implementar un sistema de comunicacions segur, amb garanties de privacitat, integritat, autenticitat i no-repudi de la informació intercanviada entre els usuaris del sistema.

1 Xifrar/Desxifrar

Xifrar `fitxer clauXifrat`

entrada: `fitxer` fitxer a xifrar;
`clauXifrat` fitxer amb la clau secreta per xifrar;
sortida: `fitxer.enc` fitxer xifrat amb el material necesari per desxifrar.

Desxifrar `fitxer.enc clauXifrat`

entrada: `fitxer.enc` fitxer xifrat amb el material necesari per desxifrar;
`clauXifrat` fitxer amb la clau secreta per desxifrar;
sortida: `fitxer` fitxer desxifrat.

2 Claus

RSAkey `n`

entrada: `n` nombre de bits de la clau RSA a generar;
sortida: dos fitxers, en format PEM, un que contingui la clau pblica RSA i un altre amb la clau privada RSA.

ECCkey `corba`

entrada: `corba` nom de la corba amb la que és generarà la clau ECC (podeu fer servir la comanda `openssl ecparam -list_curves` per obtenir el llistat de corbes);
sortida: dos fitxers, en format PEM, un que contingui la clau pública ECDH i un altre amb la clau privada ECDH.

3 Signatura/Verificació signatura

Signar `fitxer clauSignatura`

entrada: `fitxer` fitxer a signar;
`clauSignatura` fitxer amb la clau per signar, en format PEM;
sortida: `fitxer.signature` fitxer amb la signatura.

Verificar `fitxer fitxer.signature clauVerificació`

entrada: `fitxer` fitxer del que es vol verificar la signatura;
`fitxer.signature` fitxer amb la signatura a verificar;
`clauVerificació` fitxer amb la clau per verificar la signatura, en format PEM;
sortida: `True` o `False`.

4 Enviar/Rebre un missatge.

Quan un usuari (l'emissor) vol enviar un missatge M a un altre (el receptor) procedeix de la manera següent:

1. Firma el missatge en clar M amb la seva clau privada, afegint-li els bytes corresponents a la firma; diguem $M\|F$ al missatge amb la seva signatura.
2. Genera una clau de sessió KS. Denotem per KSE la informació per que el receptor pugui obtenir KS.
3. Amb KS, xifra el missatge $M\|F$ fent servir un algorisme de clau secreta. Notarem per $E(M\|F)$ el missatge xifrat.
4. Concatena KSE amb $E(M\|F)$ i envia el resultat $KSE\|E(M\|F)$ al receptor.

Quan el receptor rep el criptograma $KSE\|E(M\|F)$ procedeix en sentit invers per tal de recuperar el missatge en clar i verificar la signatura:

1. Primer descompon la informació rebuda en dos troços corresponents a KSE i $E(M\|F)$.
2. Recupera la clau de sessió KS fent servir KSE.
3. Desxifra el missatge $E(M\|F)$ amb la clau de sessió KS, obtenint $M\|F$.
4. Recupera el missatge M i verifica la firma F amb la clau pública de l'emissor.

enviarMissatge `M clauDeFirma clauPublica clauPrivada`*

entrada: `M` nom del fitxer a xifrar, el contingut es tractarà com una llista de bytes;
`clauFirma` nom del fitxer que conté la clau privada de firma del firmant;
`clauPublica` nom del fitxer que conté la clau pública del receptor del missatge;
`clauPrivada` *(si és necessari)* nom del fitxer que conté la clau privada per generar la clau de sessió (KS);

sortida: un fitxer binari amb $KSE\|E(M\|F)$.

rebreMissatge `C clauVerificacioDeFirma clauPrivada clauPublica`*

entrada: `C` nom del fitxer a desxifrar,
`clauVerificacioDeFirma` nom del fitxer que conté clau pública de verificació de firma del signant;
`clauPrivada` nom del fitxer que conté la clau privada corresponent a la clau pública feta servir per xifrar el missatge;
`clauPublica` *(si és necessari)* nom del fitxer que conté la clau publica per generar la clau de sessió (KS);
sortida: dos fitxers (un que contingui M i un altre amb F) i un missatge indicat la validesa de la signatura.

Per llegir

Suite B Cryptography / Cryptographic Interoperability,
http://www.nsa.gov/ia/programs/suiteb_cryptography/