1.1. ECB. Cifra a mensagem em blocos, todos de forma independente, embora aplique a mesma operação.

1.2.

a) Com o modo ECB, os padrões presentes no texto em claro repetem-se, uma vez que cada bloco é cifrado de forma independente dos outros e pela mesma ordem, enquanto que no modo CBC a cifra é feita a partir do resultado das mensagens cifradas anteriormente e apenas a partir de cada bloco isolado. Isto faz com que neste modo os padrões não se repitam.

b)

No modo ECB há paralelização da cifra e no modo CBC apenas na decifra, uma vez que neste último a cifra final depende de todos os blocos anteriores e, se se alterar um bit nesta operação, o resto da mensagem cifrada é afetada, contrariamente ao ECB, em que cada bloco é cifrado de forma independente.

2. Utilizam-se os dois tipos de chave, para garantir que o recetor pretendido é o único capaz de ver a mensagem. A decifra da chave privada é feita através de uma chave pública do recetor, para depois esta (chave privada) ser usada para decifrar a mensagem.

3.

3.1. Os Métodos de geração de assinatura são os seguintes:

- update: byte[] → void – continua a operação incremental
- sign: void → byte[] – finaliza operação incremental, retornando a assinatura

A função sign é responsável pela geração da assinatura sendo ela usada para finalizar a operação incremental.

INitVerify- inicia o objeto para verificação

Initsign- inicia o objeto para assinar

Sign – retorna a assinatura final da mensagem num array de bytes este método é usado depois da utilização do método update que recebe parte da mensagem.

3.2. Como sabemos que dois objetos partilham o mesmo hash, é possível obter ambos (os objetos). A partir daí, conseguimos calcular a chave privada de cada um, pois a chave pública e a chave privada partilham os mesmos dois números primos. Com isso, conseguimos inicializar novas assinaturas utilizando a chave privada (initSign)

4.

4.1. Quando o certificado é auto assinado ou seja raiz de confiança.

4.2. Se fosse utilizado o esquema MAC na proteção de integridade dos certificados é porque o mesmo para autenticar mensagem utiliza sempre a mesma chave (chave simétrica) logo qualquer entidade seria capaz de criar mensagens autenticadas.

4.3. um ficheiro .pfx possui tanto a chave publica como a chave privada associada ao certificado enquanto um ficheiro .cer só possui a chave publica.