Definir modelo de adversário(MiM?), de acordo com a framework X.800

O atacante vai tentar compremeter/atacar as 3 propriedades definidas no enunciado

Pretende violar as propriedades de autenticidade(spoofing, forging), integridade(tampering, replaying) e confidencialidade(sniffing, eavesdropping)

PBE para proteger adicionalmente o ficheiro com as configurações de criptrografia

Individuo entra, e diz ao utilizador para dar a password(como se fosse login), dá a password e usa o PBE file para aceder aos dados criptrograficos.

**Fase 2**

Usar PBEncryption para a autenticação, pois assim impede o message replaying.

## Modos de Operação utilizados

CBC e CTR, permitem initialization vectors

ECB não é seguro e não permite IV

CFB não utilizador porque é focado em data stream.

## Algoritmos criptrográficos utilizados

AES, TripleDES, Blowfish, sendo o AES o melhor de todos

-DES, plaintext block 64bits, ciphered block 64bits, key size 56bits chave de (horrivel)

-TripleDES, plaintext block 64bits, ciphered block 64bits, key size 112/168bits(56\*2/56\*3)

-AES, plaintext block 128bits, ciphered block 128bits, key size 128/192/256 bits