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.