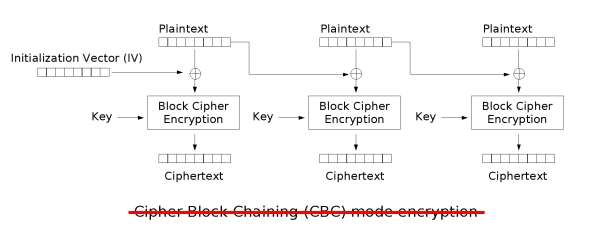
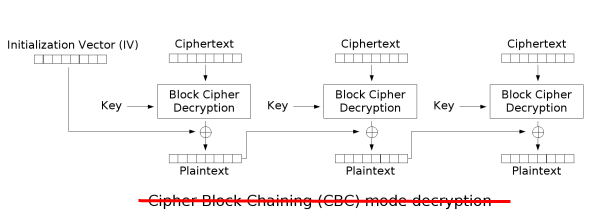
# Segurança Informática

## Série 1

1. Se a função de hash for usada num esquema de assinatura digital, o receptor irá considerar a mensagem como sendo enviada pelo emissor real.
2. 
   1. 
   2. O principal problema do ECB é que a existência de blocos iguais de texto em claro irão produzir blocos iguais de cifra, criando alguns padrões na cifra final. Não resolve o problema do ECB.
3. 1. Não. É necessário o Certificate Path completo.
   2. Porque o root certificate fará parte da máquina tendo de ser instalado pelo utilizador e comprometeria a segurança.
4. 1. Para provar ao TGS que é o possuidor da chave k.
   2. Não, porque um bilhete destina-se apenas à comunicação com um e só um servidor.