**RELATÓRIO**

**SI-1011-1**

GRUPO: *G14N*

ALUNOS:

*32223, Paulo Pires*

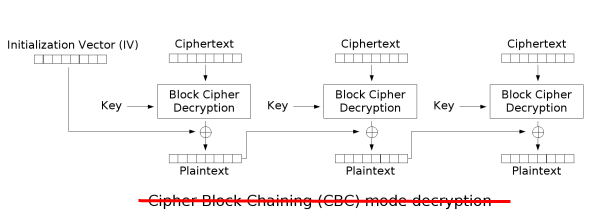
*31768, Ricardo Romão*

**ÍNDICE**

[1 Resolução 1](#_Toc276303195)

# Resolução

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.
3. 1. Esquema de decifra.



* 1. 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. O esquema proposto não resolve o problema do ECB.

2. 1. Não. O certificado terá de estar válido, ou seja, estar dentro do prazo de validade, não fazer parte das lista de revogação e é necessário os certificados intermédios e raízes de confiança.
   2. O certificado raíz não faz parte da CertPath pois tem de estar instalado na máquina do utilizador, pois o contrário traria grandes problemas de segurança.
4. 1. O autenticador de A é necessário nas mensagens trocadas com o TGS para provar que A é possuidor da chave k de encriptação fornecida pelo AS.
   2. Não, porque um bilhete destina-se apenas à comunicação com um e só um servidor.