INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

SEGURANÇA INFORMÁTICA

LICENCIATURA ENGENHARIA INFORMÁTICA E COMPUTADORES

FASE DE EXERCÍCIOS
Fase 1

Autores:
43552 - Samuel Costa
43320 - André Mendes

Docente:
José Simão

29 de Dezembro de 2018

Conteúdo

1 Introdução

O trabalho realizado para este fase pretende que os temas desenvolvidos durante as aulas sejam postos em prática. Para esta fase os exercícios focaram essencialmente a primeira parte da matéria.

- Esquemas e Primitivas Criptográficas
- Java Cryptographic Architecture (JCA)
- Certificados digitais e Infraestrutura de Chave Pública
- Protocolo Criptográfico Transport Layer Security (SSL/TLS)

Neste trabalho prático pretendemos responder aos vários exercícios propostos e implementar uma demonstração dos pontos referidos.

2 Primeira série de exercícios

2.1 Exercício 1

Ambos os esquemas criptográficos visam garantir a autenticidade da mensagem adicionando à própria mensagem um numero de bits de forma a identificar o emissor da mesma, no caso do MAC uma marca ou uma assinatura no caso da assinatura digital, sendo essa autenticidade verificada no recetor. Ambos os esquemas utilizam chaves privadas para "marcar" a mensagem, sendo que no caso da assinatura digital é usado uma chave publica para autenticar essa mesma mensagem, já no esquema MAC é usada a chave privada do emissor.

2.2 Exercício 2

A função de hash obriga a uma mensagem de tamanho variável m para uma redução da mesma de tamanho n ou seja, a dimensão do yL = dimensão de $m1$, logo n bits = dimensão de um bloco "shiftado" da dimensão da mensagem, pelo que existe m e m', tal que $H(m) = H(m')$.

2.3 Exercício 3

Um algoritmo de cifra determinístico indica que a cifra de uma mensagem pode se repetir, ou seja, caso a mensagem seja um padrão a cifra irá se repetir também, logo o atacante tendo acesso à cifra e à chave publica pode através de força bruta repetir uma mensagem até encontrar a cifra, pois se for igual aquela que o atacante então a mensagem é equivalente à original.

2.4 Exercício 4

Analisando os dois tipos de esquemas seria expectável que a primitiva AES é sempre mais dificil de criptoanalizar que um sistema com primitiva DES, no entanto essa analise tem de ser feita também relativamente ao modo de operação que cada uma pode usar, como por exemplo no caso especifico de um sistema AES ter usado um modo de operação ECB (Electronic Code Book) e a sua mensagem ser de alguma forma curta e padronizada pode mais facilmente ser quebrada que uma DES que usou o mode de operação CBC (Cipher Block Chain).

3 Conclusão