Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Licenciatura em Engenharia Informática, Redes e Telecomunicações

Segurança Informática

Primeira série de exercícios, Semestre de Inverno de 19/20

Entregar até 21 de outubro de 2019

---

1. Quais as semelhanças e as diferenças entre um esquema assimétrico de assinatura digital e um esquema MAC? Quais os critérios de decisão para selecionar um deles?

2. Considere a função de *hash* H(m) definida por:

   - Seja $E_p(k)(b)$ uma primitiva de cifra em bloco que usa chaves k de n bits e blocos b de n bits
   - Seja $m = m_1, m_2, \ldots, m_L$ a divisão da mensagem em blocos de n bits. Assuma que a dimensão das mensagens é sempre múltipla de n.
   - Seja $y_i = E_p(m_{i-1})(m_i)$, para $i = 2, \ldots, L$, com $y_1 = m_1$.
   - O valor de hash é $H(m) = y_L$.

   Explique porque motivo é computacionalmente fazível, dado m, obter $m' \neq m$ tal que $H(m') = H(m)$.

3. Apresente uma forma de atacar uma implementação de um esquema de cifra assimétrica cujo algoritmo de cifra, $E_a(k)(m)$, seja determinístico (isto é, se $x = y$ então $E_a(k)(x) = E_a(k)(y)$).

4. Os sistemas $\mathcal{A}$ e $\mathcal{B}$ cifram mensagens usando, respetivamente, as primitiva DES (chaves com 56 bits úteis) e AES (chaves de 128 bits). Admitindo o uso de chaves aleatórias, porque motivo os criptogramas produzidos por $\mathcal{A}$ podem ser mais difíceis de criptoanalisar do que os produzidos por $\mathcal{B}$?

5. Na biblioteca *Java Cryptography Architecture* (JCA), como é que as *engine classes* (ex: `Cipher`, `Signature`, `Mac`) possibilitam a aplicação incremental das respetivas proteções? Qual a vantagem de aplicar proteções incrementalmente?

6. Considere os certificados X.509 e as infraestruturas de chaves pública (PKI):

   6.1. De que forma a resistência à segunda pré-imagem de uma função de *hash* contribui para garantir a autenticidade da chave pública de um certificado.

   6.2. Considere o certificado folha C e os intermédios $I_1, I_2, \ldots, I_n$. Alguma das chaves privadas dos certificados intermédios é usada para validar o certificado C?

7. Considere o laboratório sobre cifra simétrica dos *Labs for Security Eduction* (SEED) [1]. Realize o ponto "*2.4 Task 4: Padding*". Na alínea 1 indique os modos que usam *padding* explicando as experiências efetuadas. Na alínea 2 realize a experiência com a primitiva AES em modo CBC e indique, para cada dimensão de ficheiro, os valores de *padding*.

8. Pretende-se desenvolver uma aplicação para geração e verificação de cifra autenticada do tipo *MAC-then-encrypt*. A cifra autenticada (AE) da mensagem m é definida por $AE(m, k_1, k_2) = E(k_1)(m||T(k_2)(m)))$.

   8.1. Defina a função de decrifra e verificação.

   8.2. Implemente a aplicação usando a JCA.

9. Usando a JCA realize uma aplicação para cifrar e decifrar ficheiros usando um esquema híbrido. Este tipo de esquema usa cifra assimétrica para transportar uma chave simétrica (gerada pela aplicação) que cifra o conteúdo do ficheiro.

   Independentemente da operação a realizar, a aplicação recebe como *input*: i) nome de ficheiro (com mensagem em claro ou cifrada); ii) a operação a realizar (`cifra` ou `decifra`). No modo `cifra` recebe o certificado do destinatário e produz i) ficheiro com mensagem cifrada (C_f); ii) ficheiro com metadados (IV e chave simétrica cifrada com a chave pública do destinatário). No modo `decifra` recebe: i) C_f; ii) metadados; iii) Chave privada do destinatário (ficheiro .pfx). e produz ficheiro com o texto em claro.

   Apresente tempos de execução para cifrar e decifrar o PDF do enunciado usando 2 algoritmos simétricos diferentes, em combinação com o algoritmo assimétrico RSA. Use o material criptográfico presente no anexo `certificates-keys.zip`

Referências

[1] `https://seedsecuritylabs.org/Labs_16.04/PDF/Crypto_Encryption.pdf`

ISEL, 18 de setembro de 2019.