Instituto Superior de Engenharia de Lisboa
Licenciatura/Mestrado em Engenharia Informática e de Computadores
Segurança Informática
Primeira série de exercícios, Semestre de Inverno de 13/14
Data de entrega: 21 de Outubro de 2014

---

1. Considere um esquema de cifra simétrica baseado numa primitiva de cifra em bloco com $n = 128$ (dimensão do bloco) e $l = 256$ (dimensão da chave) que utiliza o modo de operação CBC com *padding* PKCS#5. Qual a dimensão do criptograma resultante da cifra duma mensagem com 256 *bits*.
2. A obtenção simultânea de integridade e autenticidade pode ser conseguida através da utilização de esquemas MAC e de cifra simétrica, usando uma das seguintes técnicas: *Encrypt-then-Authenticate* ou *Authenticate-then-Encrypt*. Qual destas técnicas é imune ao ataque de *Vaudenay*?
3. Quais as semelhanças e as diferenças entre um esquema assimétrico de assinatura digital e um esquema MAC? Quais os critérios de decisão para seleccionar um deles?
4. No contexto das infra-estruturas de chave pública, apresente uma técnica para proteger as *end-entities* de ataques às autoridades de certificação.
5. No contexto das infra-estruturas de chave pública baseadas em certificados X.509
   5.1. Qual a relação entre a chave pública presente num certificado e a chave usada na assinatura deste?
   5.2. Quais as consequências se uma aplicação consumidora de certificados ignorar a extensão *basic constraints*?
   5.3. Em que circunstância um certificado X.509 contém uma chave privada?
6. Seja $h_k : \{0,1\}^* \to \{0,1\}^k$ a função de *hash* definida por

$$h_k(x) = y_1 \dots y_k$$

   onde $y_1 \dots y_{160} = \mathbf{SHA1}(x)$.

   Sejam m_1 e m_2 os programas Java definidos nos ficheiros `BadApp.java` e `GoodApp.java` (presentes em anexo ao enunciado). Dois programas m e m' dizem-se equivalentes ($m \equiv m'$) se a sua execução produz o mesmo resultado observável.

   6.1. Calcule $h_k(m_1)$ e $h_k(m_2)$ para $k = 8, 16, 32$.
   6.2. Realize uma aplicação para encontrar um programa m' tal que $h_k(m') = h_k(m_2)$ e $m' \equiv m_1$. Considere $k = 8, 12, 16$. Qual o número médio de operações h_k necessário para encontrar a colisão?
   6.3. Realize uma aplicação para encontrar um par (m'_1, m'_2) tal que $h_k(m'_1) = h_k(m'_2), m'_1 \equiv m_1$ e $m'_2 \equiv m_2$. Considere $k = 8, 16, 32$. Qual o número médio de operações h_k necessário para encontrar a colisão?
7. Realize uma aplicação consola para assinar e verificar objectos *JSON Web Token* (JWT) [1], transportados numa estrutura *JSON Web Signature* (JWS) [2]. A aplicação deve no mínimo suportar assinatura digital com os algoritmos "RS256" e "HS256" [3].

Referências

[1] https://tools.ietf.org/html/draft-ietf-oauth-json-web-token-27, visitado 30 setembro 2014.

[2] https://tools.ietf.org/html/draft-ietf-jose-json-web-signature-33, visitado 30 setembro 2014.

[3] http://tools.ietf.org/html/draft-ietf-jose-json-web-algorithms-18#page-52, visitado 30 de setembro 2014.

ISEL, 30 de Setembro de 2014.