Introdução à Criptografia – Prova II

Critérios para avaliação: Clareza, corretude, rigor, e concisão (i) A redação das respostas deve ser clara. (ii) Todo o raciocínio desenvolvido na resposta deve estar correto. (iii) O nível de rigor nas respostas deve ser próximo ao usado na bibliografia básica. (iv) As respostas não devem ser mais longas que o necessário.

Atenção: não há uma pontuação "por questão". A nota da prova pretende aferir a compreensão, de forma ampla, do conteúdo.

Ex. 1 — Mostre como implementar o esquema de acordo de chaves Diffie-Hellman para três participantes (os tres, A, B e C, devem terminar com as mesmas chaves). Não se preocupe com o ataque de homem-no-meio.
Comentário:

1. $A \to B, C : g^a$
2. $B \to C : (g^a)^b = g^{ab}$
3. $C \to B : (g^a)^c = g^{ac}$
4. $B \to C : g^b$
5. $C \to A : (g^b)^c = g^{bc}$
6. B calcula $\left(g^{ac}\right)^b = g^{abc}$
7. C calcula $\left(g^{ab}\right)^c = g^{abc}$
8. A calcula $\left(g^{bc}\right)^a = g^{abc}$

Ex. 2 — Porque o esquema de assinaturas de Lamport só pode ser usado uma única vez para cada par de chave pública/privada? Mostre detalhadamente o que um atacante poderia fazer se pudesse obter assinaturas de duas mensagens à sua escolha, m_1 e m_2 (mantendo o mesmo par de chaves).
Comentário: Porque a verificação da assinatura conssite em abrir partes da chave privada.
Sejam $m_1 = 0010$ e $m_2 = 1101$, e seja a chave secreta

$$X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \end{pmatrix}$$

e a chave pública

$$Y = \begin{pmatrix} F(x_{11}) & F(x_{12}) & F(x_{13}) & F(x_{14}) \\ F(x_{21}) & F(x_{22}) & F(x_{23}) & F(x_{24}) \end{pmatrix}$$

Ao assinar as mensagens m_1 e m_2, preciso abrir *todos* os valores da chave privada, depois disso qualquer um poderá assinar mensagens com minha chave.

Ex. 3 — Suponha que ao invés da Construção HMAC descrita em aula, usemos o seguinte:
Seja $(\mathtt{Gen}', H^s)$ uma função de hashing obtida via transformação de Merkle-Damgård. Então construímos

- $\mathtt{Gen}(1^n)$ (sem mudanças)
- $\mathtt{Mac}_k(m) = H^s(k||m)$
- $\mathtt{Vrf}_k(m, t)$ verifica se $\mathtt{Mac}_k(m) = t$.

Mostre que esta construção não é segura.
Comentário: Suponha que eu tenha gerado o rótulo de m:

$$t = \mathtt{Mac}_k(m) = H^s(k||m)$$

Um atacante pode facilmente, <u>*sem a chave* k</u>, gerar o rótulo de $m||m'$, para qualquer m'.

$$\begin{aligned} t' &= H^t(m') && \text{(hash de } m'\text{, usando } t \text{ como iv.)} \\ &= H^s(k||m||m') \end{aligned}$$

Isso funciona porque dissemos que a função de hashing é uma construção de Merkle-Damgård.