crypto1104

Quiz for hash

姓名

1. Assume we want to use a hash function with output length as small as possible, subject to being collision resistant against a birthday attack running in time 2^{192}. Which hash function would be the best choice? 【多选题】

□ A、MD5.

□ B、SHA-1.

☑ C、SHA-3 with 384-bit output.

□ D、SHA-2, with output truncated to 192 bits.

2. Let H, H' be collision-resistant hash functions. Which of the following functions H'' is NOT necessarily collision-resistant? 【多选题】

□ A、H''(x) = H(x)|| H'(x), where || denotes concatenation.

☑ B、H''(x) = H(x) ⊕ H'(x).

□ C、H''(x) = H(H'(x)).

□ D、H''(x) = H(x) || 0...... 0.

3. Which of the following is the most appropriate primitive for achieving message integrity between two users sharing a key? 【多选题】

□ A、Collision-resistant hash function.

□ B、Block cipher.

□ C、Private-key encryption scheme.

☑ D、Message authentication code.

4. Which of the following is an example of a message authentication code used widely in practice? 【多选题】

□ A、CBC-mode encryption.

☑ B、HMAC.

□ C、SHA1.

□ D、AES.

5. Assume a sender and receiver use basic CBC-MAC but authenticate/accept messages of different lengths. Which of the following is a valid attack? 【多选题】

□ A、 Obtain tag t_1 on message m_1, and tag t_2 on message m_1, m_2. Then output the tag t_1 on the message t_2 ⊕ m_2.

☑ B、Obtain tag t_1 on message m_1, and tag t_2 on message m_1, m_2. Then output the tag t_2 on the message t_1 ⊕ m_2.

□ C、Obtain tag t_1 on message m_1, and tag t_2 on message m_2, m_1. Then output the tag t_2 on the message m_1, m_2.

□ D、Obtain tag t_1 on message m_1, and tag t_2 on message t_1, m_2. Then output the tag t_2 on the message m_1 ⊕ m_2.

6. Assume a sender and receiver use the encrypt-and-authenticate approach for variable-length messages, using CTR-mode encryption and a variant of CBC-MAC secure for authenticating variable-length data (and independent keys for each). Which of the following statements is true? 【多选题】

□ A、The combination is not CPA-secure, and it does not provide integrity because the CTR-mode encryption allows the attacker to forge a tag in the CBC-MAC.

☑ B、The combination is not CPA-secure, but it does provide integrity.

□ C、The combination is CPA-secure, but it does not provide integrity.

□ D、The combination is not CPA-secure, and it does not provide integrity because CTR-mode encryption is malleable.

7. Let F be a block cipher with n-bit block length. Consider the message authentication code for 2n-bit messages defined by Mac_k(m_1, m_2) = F_k(m_1 ⊕ m_2). Which of the following gives a valid attack on this scheme? 【多选题】

☑ A、 Obtain tag t on message m_1, m_2 (with m_1 ≠ m_2), and then output the tag t on the message m_2, m_1.

□ B、Obtain tag t on message m, 0...... 0, and then output the tag t ⊕ (1......1) on the message m, 1......1.

□ C、Obtain tag t on message m, ... 0 (with m ≠ 0...... 0), and then output the tag t on the message 0...... 0, 0......0.

□ D、Obtain tag t on message m, m, and then output the tag 0......0 on the message 0......0, m.

提交

举报