C&O 487/687: Midterm test

Duration: 2 hours
Additional materials allowed: None.

Instructions: Please use *complete sentences* and try to be as *concise* as possible. Solutions that are neatly written and well organized will receive more partial credit than solutions that are untidy, disorganized, and unfocused. Please state and justify any assumptions you may make.

1. **Miscellaneous questions**

   (a) What is a *chosen-plaintext* attack on a symmetric-key encryption scheme? Describe a practical scenario where an attacker may be able to mount a chosen-plaintext attack on a symmetric-key encryption scheme.

   (b) Recall that Feistel ciphers are a class of block ciphers with parameters n (half the block length), h (the number of rounds), and l (the key size). Then $M = \{0,1\}^{2n}$ (the plaintext space), $C = \{0,1\}^{2n}$ (the ciphertext space), and $K = \{0,1\}^l$ (the key space). A key scheduling algorithm determines subkeys $k_1, k_2, \ldots, k_h$ from a key k. Each subkey k_i determines a function $f_i : \{0,1\}^n \to \{0,1\}^n$. Encryption takes h rounds:
   Plaintext is $m = (m_0, m_1)$, where $m_0, m_1 \in \{0,1\}^n$.
   Round 1: $(m_0, m_1) \to (m_1, m_2)$, where $m_2 = m_0 \oplus f_1(m_1)$.
   Round 2: $(m_1, m_2) \to (m_2, m_3)$, where $m_3 = m_1 \oplus f_2(m_2)$.
   ......
   Round h: $(m_{h-1}, m_h) \to (m_h, m_{h+1})$, where $m_{h+1} = m_{h-1} \oplus f_h(m_h)$.
   The ciphertext is $c = (m_h, m_{h+1})$.
   Give an algorithm for the decryption process.

   (c) Define what it means for a MAC scheme to be *secure*.

   (d) Suppose that $H : \{0,1\}^* \to \{0,1\}^n$ is a collision-resistant hash function. Define a new hash function $G : \{0,1\}^* \to \{0,1\}^n$ by $G(x) = H(H(x))$. Prove that G is also collision resistant.
   (Note: As mentioned in class, such statements are best proven using the contrapositive statements. That is, you should prove that if G is not collision resistant, then H is not collision resistant.)

   (e) Explain why, strictly speaking, non-repudiation cannot be achieved with a MAC scheme.

   (f) Suppose that Alice's RSA public key is $(n = 35,\ e = 7)$. Find her private key d.

2. Describe and analyze a polynomial-time algorithm for the problem of computing $a^m \bmod n$, given a positive integer n and integers $a, m \in [1, n-1]$. (You have to justify why the running time of the algorithm is polynomial-time.)

3. Recall that DES is a symmetric-key encryption scheme with a 56-bit key size, and 64-bit plaintext and ciphertext blocks. Consider the following proposal for a new symmetric-key encryption scheme based on DES. The secret key for the new scheme is $k = (k_1, k_2)$, where $k_1 \in_R \{0,1\}^{56}$ and $k_2 \in_R \{0,1\}^{64}$ (so k is a 120-bit key). Let $m \in \{0,1\}^{64}$ be a plaintext message. Then encryption is defined as follows:

$$E_k(m) = \mathrm{DES}_{k_1}(m \oplus k_2).$$

   (a) Give a formula for the decryption function.

   (b) Show how this encryption scheme can be totally broken—that is the secret key k can be recovered—by a known-plaintext attack using *roughly* 2^{56} DES encryption/decryption operations. Your attack should have very little space requirements. You may assume that you have a moderate number of plaintext-ciphertext pairs $(m_i, c_i = E_k(m_i))$. Justify why the number of such pairs you use is sufficient to uniquely determine the key with high probability.

4. Recall that the CBC block cipher mode of operation encrypts a message $m_1 m_2 \cdots m_n$ to the ciphertext $c_0 c_1 c_2 \cdots c_n$ where c_0 is chosen at random and

$$c_i = E_k(m_i \oplus c_{i-1}) \text{ for } 1 \leq i \leq n.$$

   (a) Explain how decryption is performed with CBC.

   (b) We define a new block cipher mode of operation known as UBC (Useless Block Chaining), with

$$c_i = E_k(m_i) \oplus c_{i-1} \text{ for } 1 \leq i \leq n.$$

   Show that UBC is, in fact, useless.

5. Let (n, e) be an RSA public key, where n is 2048 bits in length. The corresponding RSA private key is not known to anyone. Define a hash function $H : \{0,1\}^* \longrightarrow [0, n-1]$ as follows: $H(m) = \overline{m}^e \bmod n$, where $\overline{m}$ denotes the integer whose binary representation is m.

   (a) Is H preimage resistant? (Justify your answer.)

   (b) Is H second-preimage resistant? (Justify your answer.)

   (c) Is H collision resistant? (Justify your answer.)