CO 487/687: Midterm test

Total marks: 40 | 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 make.

1. **Miscellaneous questions** (3 marks each)

   (a) Recall that RC4 is a stream cipher that, on input a secret key k, outputs a keystream RC4(k). The plaintext is then encrypted by addition (bitwise modulo 2) with the keystream. What is the danger in using the same keystream to encrypt two different plaintexts?

   (b) Let E denote the family of encryption functions for a block cipher where plaintext blocks, ciphertext blocks, and keys are each 128 bits in length. Let $H : \{0,1\}^* \to \{0,1\}^{128}$ be a hash function. Define a MAC scheme $\text{MAC}_k : \{0,1\}^{3072} \to \{0,1\}^{128}$ by $\text{MAC}_k(m) = E_k(H(m))$. Here, k is an 128-bit secret key. Is this MAC scheme secure? (Explain)

   (c) Recall that SHA-256 : $\{0,1\}^* \to \{0,1\}^{256}$ is a hash function. Recall also that AES is a block cipher where plaintext blocks, ciphertext blocks, and keys are each 128 bits in length. Explain why SHA-256 and AES are thought to have the same *security level*.

   (d) Describe two advantages of public-key cryptography over symmetric-key cryptography.

   (e) Suppose that Alice's RSA public key is $(n = 143, e = 7)$. Determine her private key d.

   (f) Recall that a party holding a 104-bit secret key k encrypts a WEP packet m as follows:

      (i) Select a 24-bit IV v.

      (ii) Compute a 32-bit checksum $S = \text{CRC}(m)$.

      (iii) Compute $c = (m\|S) \oplus \text{RC4}(v\|k)$.

      (iv) Send (v, c).

      i. Describe how the legitimate receiver processes (v, c).

      ii. Describe an attack which demonstrates that WEP does not provide a high degree of confidentiality.

   (g) Let (n, e) be an RSA public key, and let $c \in [1, n-1]$. Consider the following algorithm for computing the eth root of c modulo n:

      For m from 1 to $n-1$ do:

         Compute $r = m^e \bmod n$ using the repeated square-and-multiply algorithm.

         If $r = c$ then RETURN(m) and STOP.

      Is this a polynomial-time algorithm? (Explain)

   (h) Let (n, e) be Alice's RSA public key, and let d be the corresponding private key. let $H : \{0,1\}^* \to [1, n-1]$ be a hash function. Recall that in the RSA-FDH signature scheme (where FDH = Full Domain Hash), the signature on a message M is $s = H(M)^d \bmod n$.
   Suppose now that an attacker is able to find four distinct messages M_1, M_2, M_3, M_4 the product of whose hash values is 1 modulo n, i.e., $\prod_{i=1}^{4} H(M_i) \equiv 1 \pmod{n}$. Explain how the attacker can use this 4-tuple of messages to break the security of RSA-FDH.

2. **Hash functions** (2+2+2+3 marks)
Let $H : \{0,1\}^* \longrightarrow \{0,1\}^n$ be a hash function.

   (a) Define what it means for H to be 2nd preimage resistant.

   (b) Define what it means for H to be collision resistant.

   (c) Describe an application of hash function where 2nd preimage resistance is a necessary security requirement (and explain why 2nd preimage resistance is necessary).

   (d) Prove *one* of the following:

      (i) If H is 2nd preimage resistant, then H is collision resistant.

      (ii) If H is collision resistant, then H is 2nd preimage resistant.

3. **Symmetric-key encryption** (2+2+3 marks)
Recall that AES is a block cipher with plaintext and ciphertext blocks of length 128 bits, and key space $\{0,1\}^{128}$. Plaintext messages m that are longer than 128 bits are broken into blocks: $m = (m_1, m_2, \ldots, m_t)$ where each block m_i is 128 bits long. In the ECB mode of operation, m is encrypted one block at a time; that is, the ciphertext is $c' = (c'_1, c'_2, \ldots, c'_t)$ where $c'_i = \text{AES}_k(m_i)$ for $i = 1, 2, \ldots, t$ and k is the secret key. In the CBC mode of operation, m is encrypted by first selecting $c_0 \in_R \{0,1\}^{128}$ and then computing $c_i = \text{AES}_k(m_i \oplus c_{i-1})$ for $1 \leq i \leq t$; the ciphertext is $c = (c_0, c_1, c_2, \ldots, c_t)$. (Note that a new c_0 is selected each time a message is encrypted.)

   (a) Give a decryption algorithm for the CBC mode of operation.

   (b) Explain why CBC encryption is preferable to ECB encryption.

   (c) Show that CBC encryption is *not* semantically secure against *chosen-ciphertext attack*.