A22648

Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers

THE UNIVERSITY OF BIRMINGHAM

THIS PAGE TO BE REPLACED BY OFFICE

06 00000

Cryptography

May 2016 1.5 hours

[Answer ALL questions]

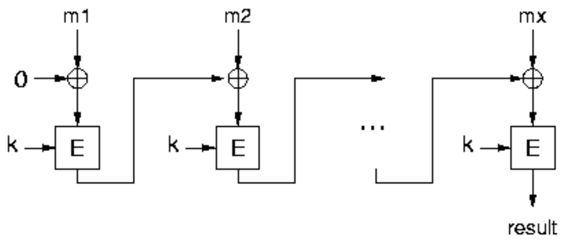
1. Let E be a secure block cipher, such as AES. E takes two arguments: a 128-bit key k, and a single 128-bit message m block. It returns a 128-bit ciphertext block $c = E(k, m)$.

   (a) Explain how to use the secure block cipher E in counter mode (also called CTR mode), in order to securely encrypt a message m that consists of multiple blocks, say $m_1, \ldots, m_n$. In your answer, you should give the definition of the ciphertext blocks $c_1, \ldots, c_n$.
   [10%]

   (b) Does encryption using a secure block cipher in counter mode guarantee message integrity? Explain your answer. **[5%, 10%]**

2. (a) Explain the concept of message authentication code (MAC). Briefly give an example of how it might be used. **[5%]**

   (b) As a reminder, a diagram showing the workings of CBC-MAC over a block cipher E is shown below.



   Suppose a message m consists of two blocks m_1 and m_2. Write down an expression which is the result of computing a CBC-MAC (over the block cipher E and key k) of $m = m_1||m_2$. **[10%]**

   (c) Again, let m_1, m_2 be message blocks, and suppose the attacker possesses just two message-tag pairs, namely (m_1, t_1) and (m_2, t_2).

      (i) Write down t_1 and t_2 in terms of m_1 and m_2 **[3%]**

      (ii) Let $m = m_1||(m_2 \oplus t_1)$. Write down the tag for m in terms of m_1, m_2 and t_1.
      [3%]

      (iii) Explain why this calculation shows that CBC-MAC is not secure without adding further restrictions to how it is used. **[4%]**

3. (a) Explain the concept of semantic security (IND-CPA security) for public key encryption (PKE). Discuss whether a PKE scheme with a deterministic encryption algorithm can be IND-CPA or not. **[5%,5%]**

   (b) Let RSA.PKE = (RSA.Kg,RSA.Enc,RSA.Dec) be the (plain) RSA public key encryption scheme. Let (E,D) be an IND-CPA symmetric encryption scheme using a 256-bit long secret key. Let H be a secure hash function, such as SHA-256.

      (i) Consider RSA.HybPKE = (RSA.Kg,RSA.HybEnc,RSA.HybDec), the combined PKE scheme obtained by defining RSA.HybEnc as follows:
      RSA.HybEnc(PK, m):
      - Choose a random plaintext R from RSA message space
      - Compute $c_0 =$ RSA.Enc(PK, R)
      - Compute $c_1 =$ E$(H(R), m)$
      - Output (c_0, c_1)

      (ii) Describe the corresponding decryption algorithm RSA.HybDec. **[5%]**

      (iii) Is RSA.HybPKE IND-CPA secure in the Random Oracle Model? Discuss your answer. **[5%,5%]**

4. (a) Explain the concept of existential unforgeability for digital signatures. **[8%]**

   (b) What is a *public key certificate* and why do we need them? **[7%]**

   (c) Let us recall the Schnorr digital signature scheme:

   - KG(λ)
     - choose a λ bit prime p and a 256-bit prime q, such that q divides $p-1$ and q is the order of a subgroup $G_q = \langle g \rangle$ of $\mathbf{Z}_p^\star$
     - a cryptographic hash function $H : \{0,1\}^\star \to \{0,1\}^{256}$ (e.g., SHA-256)
     - Choose a random x from $\{0, \ldots, q-1\}$ (i.e. from $\mathbf{Z}_q$)
     - Compute $y = g^x \bmod p$
     - Publish the public key $vk = (p, q, g, y, H)$
     - Retain the private key $sk = x$
   - Sign(sk, M). To sign a bit-string M do:
     - Choose a random r from $\{0, \ldots, q-1\}$
     - Compute $s = H(M \| g^r) \bmod q$
     - Compute $t = (r + x \cdot s) \bmod q$
     - Output signature $\sigma = (s, t)$
   - Verify(vk, σ, m) works as follows:
     - Parse σ as (s, t)
     - Accept the signature if $H(M \| g^t y^{-s}) = s$
     - Otherwise reject the signature

   Let us argue that randomness re-use while signing is insecure. To see this, show that if the same random $r \in \mathbf{Z}_q$ is used to create a signature (s, t) on a message M, and a signature (s', t') on a message M', then an attacker can recover from these two signatures the signing key x, as long as $M \neq M'$.

   [10%]