A22648

Calculators permitted provided they are not capable of being used to store alphabetical information other than hexadecimal numbers.

UNIVERSITY OF BIRMINGHAM

School of Computer Science

MSc Computer Science
MSc Advanced Computer Science
MSc Cyber Security
MSc Human-Computer Interaction
Undergraduate Affiliate Computer Science/Software Engineering
Final Year – MSci Computer Science
Final Year – MEng Computer Science/Software Engineering
Final Year – MSci Computer Science with Industrial Year
Final Year – MEng Computer Science/Software Engineering with Industrial Year

**06 20008**

# Cryptography

Summer May/June Examinations 2017

Time allowed: 1 hour 30 minutes

[Answer ALL Questions]

1. DES is a block cipher with an effective key length of 56 bits (that is, there are $2^{56}$ distinct keys). 3DES is a block cipher defined in terms of DES. 3DES uses three DES keys $k_1$, $k_2$ and $k_3$. The encryption $c$ of a block $m$ using 3DES is given by $c = \mathsf{Enc}_{k_1}(\mathsf{Dec}_{k_2}(\mathsf{Enc}_{k_3}(m)))$.

   (a) Explain why 3DES is better than DES. **[7%]**

   (b) Explain why encryption with 3DES is defined as $\mathsf{Enc}_{k_1}(\mathsf{Dec}_{k_2}(\mathsf{Enc}_{k_3}(m)))$ and not $\mathsf{Enc}_{k_1}(\mathsf{Enc}_{k_2}(\mathsf{Enc}_{k_3}(m)))$. **[7%]**

   Joe is considering to use "2DES", which he defines using

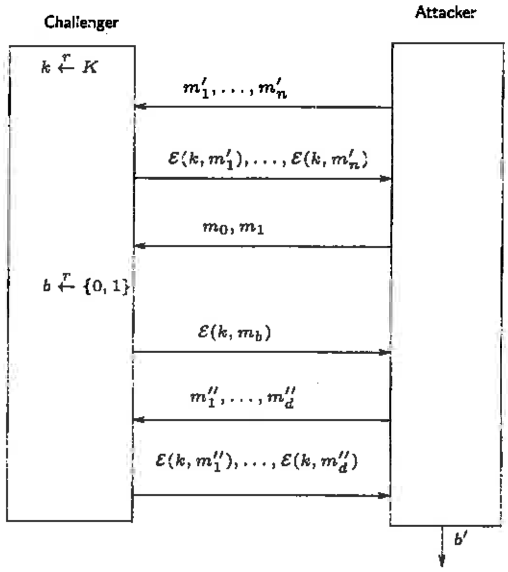
   2DES: $c = \mathsf{Enc}_{k_1}(\mathsf{Enc}_{k_2}(m))$

   (it uses only two DES keys). He hopes that this will give him approximately twice the bitlength security of DES.

   (c) Show that the equation (2DES) above may be equivalently written $\mathsf{Enc}_{k_2}(m) = \mathsf{Dec}_{k_1}(c)$, which has no nested Enc or Dec funcions. **[6%]**

   (d) Suppose an attacker has a plaintext message $m$ and the corresponding ciphertext $c$. Explain how it can find the keys $k_1$ and $k_2$ used by Joe, using a little more than $2^{56}$ operations (and way less than Joe's expected $2^{112}$ operations). **[5%]**

2. The figure below is to remind you of the IND-CPA game.




(a) What is the condition on the output $b'$ that indicates that the attacker has won the game? **[6%]**

For each of the following definitions of $\mathcal{E}(k,m)$ explain whether the attacker can expect to win the game.

(b) $\mathcal{E}(k,m)$ is defined as the encryption of a message $m$ using AES in counter mode, the key $k$, and a randomly-chosen IV. **[7%]**

(c) $\mathcal{E}(k,m)$ is defined as the HMAC of a message $m$ using SHA-256 as the underlying hash function, and the key $k$. **[7%]**

You are designing a system which will encrypt and save some information $m$ on a disk, and later retrieve and decrypt the information. You want to use *authenticated encryption.* You have an encryption function $\mathcal{E}$ satisfying IND-CPA and a MAC function $\mathcal{M}$ satisfying the MAC unforgeability game, and two secret keys $k_1$ and $k_2$.

(d) Which of the following ways to do it is better?

(i) Encrypt-then-MAC: encrypt the message, then compute MAC of ciphertext. The result may be written $\mathcal{E}(k_1,m)$, $\mathcal{M}(k_2,\mathcal{E}(k_1,m))$.

(ii) Encrypt and MAC: The result consists of the encryption of $m$ and the MAC of $m$, and may be written $\mathcal{E}(k_1,m)$, $\mathcal{M}(k_2,m)$.

Explain your answer. **[5%]**

3. Let us consider **RSA-D** = (Kg,Enc,Dec), a variant of the RSA public key encryption scheme.

- Key generation KG($\lambda$)
  - Generate two distinct odd primes $p$ and $q$ of same bit-size $\lambda$
  - Compute $N = p \cdot q$ and $\phi = (p-1)(q-1)$
  - Select two random integers $1 < e_1, e_2 < \phi$ such that $\gcd(e_1, \phi) = 1$ and $\gcd(e_2, \phi) = 1$
  - Compute the unique integer $1 < d_1 < \phi$ such that $e_1 \cdot d_1 \equiv 1 \bmod \phi$
  - Compute the unique integer $1 < d_2 < \phi$ such that $e_2 \cdot d_2 \equiv 1 \bmod \phi$
  - The public key is $PK = (N, e_1, e_2)$. The private key is $SK = (d_1, d_2)$
- Encryption Enc($PK, m$) a message $m \in \mathbf{Z}_N^\star$ proceeds as follows:
  - Generate a random integer $r$ in $\mathbf{Z}_N^\star$
  - Compute $c_1 = r^{e_1} \bmod N$
  - Compute $c_2 = m^{e_2} \cdot r^{e_1 \cdot e_2} \bmod N$
  - Output $C = c_1 || c_2$

(a) Give the corresponding decryption algorithm Dec($SK, C$). Prove your decryption algorithm is correct, i.e. that given a legitimate key pair $(PK, SK)$ it holds Dec($SK$, Enc($PK, m$)) $= m$ for any admissible $m$. **[10%]**

(b) Let us study the security of the asymmetric encryption scheme **RSA-D**:

(i) Describe in technical terms what the statement *"Breaking the RSA problem is hard"* means. **[5%]**

(ii) What is the definition of *one-wayness* for a public key encryption scheme? **[5%]**

(iii) Is **RSA-D** a one-way secure public key encryption scheme? Justify your answer. **[5%]**

(iv) Is **RSA-D** an IND-CPA (or semantically secure) public key encryption scheme? Justify your answer. **[5%]**

4. Let us consider ElGamal encryption parameters $(G, g, p, q)$ for large primes $p, q$, where $g$ is a generator of a subgroup $G$ of $\mathbf{Z}_p^*$ and $G$ has $q$ elements. Recall that in ElGamal every user chooses a random private key $x \in \mathbf{Z}_q$ and computes the public key $X = g^x \bmod p$. To encrypt a message $m \in G$ for a user with public key $X$, the sender chooses a random $y \in \mathbf{Z}_q$ and computes the ciphertext $(g^y, X^y \cdot m)$.

   (a) How is ElGamal encryption related to the Diffie-Hellman key exchange protocol? Describe the Diffie-Hellman (DH) protocol in detail. **[5%]**

   (b) Why is DH key exchange insecure against man-in-the-middle (MitM) attacks? Describe a MitM attack against the DH protocol in detail. **[5%]**

   (c) Present an improvement of the DH key exchange that prevents MitM attacks. Explain your answer. **[10%]**

**Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so**

## Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

**Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.**