Queen Mary
University of London

Friday 29 March 2019 9:00 to 10:50 AM

**ECS655U Security Engineering Midterm (20%)** **Duration:** 110 **minutes**

**YOU ARE NOT PERMITTED TO READ THE CONTENTS OF THIS QUESTION PAPER UNTIL INSTRUCTED TO DO SO BY AN INVIGILATOR.**

**Instructions:** Please write down your student ID on this page. This paper contains FOUR questions. **Answer all questions**. Cross out any answers that you do not wish to be marked.

Calculators are not permitted in this examination.

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately.

**Exam papers must not be removed from the exam room.**

Student ID Number: ........................................

| Question | Points | Score |
|---|---|---|
| 1 | 30 | |
| 2 | 30 | |
| 3 | 30 | |
| 4 | 30 | |
| Total: | 120 | |

Leave this table blank.

Examiner: Dr Arman Khouzani

**Question 1**

(a) Provide an advantage and a disadvantage of symmetric key cryptography versus public key cryptography.

**[5 marks]**

- Advantage:

- Disadvantage:

(b) Provide two similarities and two differences between a Message Authentication Code (MAC) and a Digital Signature scheme.

**[10 marks]**

- Two similarities:

- Two differences:

(c) This question is regarding a generic “digital signature” scheme. Using the following notations, answer each question.

(i) Provide the “correctness” conditions for this digital signature scheme. That is, what relation needs to hold for this digital signature scheme to be “correct”? Your answer can be very briefly stated in terms of the notations in the table. But if you cannot, express it in words using as much of the notations in the table as you can.

**[5 marks]**

| Notation | Description |
|---|---|
| $m$ | A message |
| $(\sigma_i, \omega_i)$ | A signing-verification key pairs |
| $sig = S(m, \sigma)$ | Signing algorithm applied to message $m$ (the first argument) using signing key $\sigma$ (the second argument), the output is a digital signature *sig*. |
| $V(m, sig, \omega)$ | Verification algorithm applied to message $m$ (the first argument) and signature *sig* (the second argument) using the verification key $\omega$ (the third argument). The output is boolean (passed/failed). |
| $\forall$ | A logic symbol which means "given any", or "for all". For example: $\forall m, \sigma$ means given any message $m$ and signing key $\sigma$ (i.e., for any given $m$ and any given $\sigma$) |

(ii) Does the following statement hold for a correct digital signature? That is, does a digital signature scheme have to satisfy the following property? Provide a brief reasoning.

**[5 marks]**

$$\forall(\sigma_i, \omega_i), m_1, m_2 : \quad m_1 \neq m_2 \Rightarrow V\left(m_1, S(m_1, \sigma_i), \omega_i\right) \neq V\left(m_2, S(m_2, \sigma_i), \omega_i\right)$$

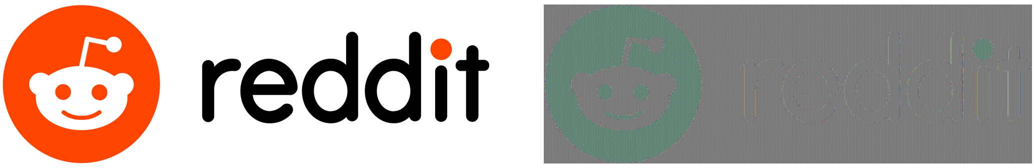
(iii) Answer the above question about the following statement. Again, is the following property necessary for a digital signature scheme? Support your answer with a brief reasoning.

**[5 marks]**

$$\forall m, \sigma_1, \sigma_2 : \quad \sigma_1 \neq \sigma_2 \Rightarrow S(m, \sigma_1) \neq S(m, \sigma_2)$$

**Question 2**

(a) Figure 1a shows an image in a format in which each pixel is represented by one byte. Figure 1b shows the result of encryption of that image using a mode of operation of a (symmetric key) block cipher like AES. Note that we can see a pattern of the original image in the encrypted image. For each of the following modes of operation, elaborate (in some detail) whether the image in Fig. 1b can be the result of encryption using that mode of operation?



(a) plaintext (b) ciphertext

Figure 1: Encryption of pixel-encoded image (a) using a mode of operation of a block cipher has given us (b) where the trace of the original picture can be seen.

**[10 marks]**

- Counter Mode (CTR)

- Cipher Block Chaining (CBC)

(b) Consider the following diagram describing the encryption algorithm in a particular mode of operation of a block cipher like AES, and answer the subsequent questions.

(i) Draw the diagram of the corresponding decryption process (with clear labels). Hint: this mode of operation was not explicitly presented in class, but you should be able to answer this question from basic principles. Start from $C_0$ and try to recover $P_0$ from it, and then $P_1$, $P_2$, and from there a general $P_i$. **[10 marks]**

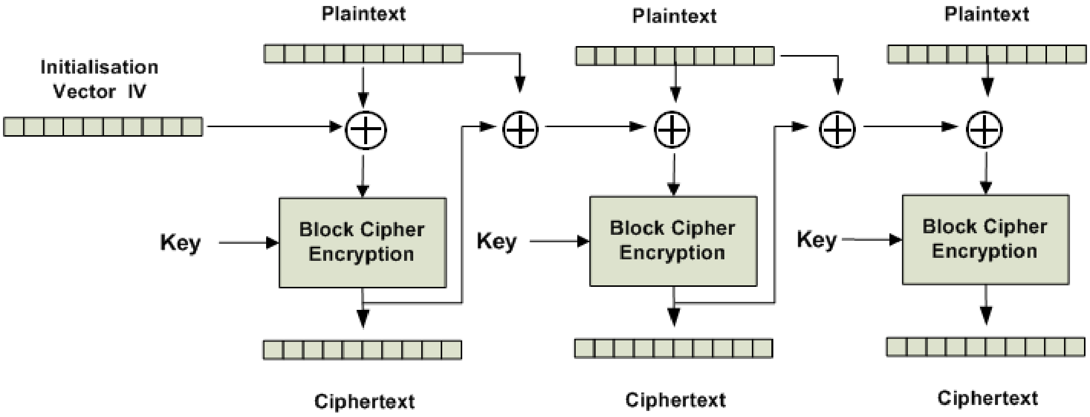


Figure 2: Q2(b) Notations: $\oplus$: XOR (eXclusive OR) operator.

(ii) Analyse the “error-propagation” of this mode of operation (in Figure 2). That is, if a single bit of the ciphertext is flipped (e.g. due to noise in the channel), what would be the effect on the recovered plaintext at the receiver.

**[5 marks]**

(iii) Provide two disadvantages of this mode of operation compared to the CTR (i.e., Counter) mode. **[5 marks]**

**Question 3**

(a) The following is the output of a SHA-256 cryptographic function applied to the string “ECS655U” in hex format (64 hexadecimal characters/digits):

```
11b8f8a636a335a7c74d0c6138e912db67380eda4767de0bc8d74d8077462caa
```

(i) On average, how many random inputs should you compute with SHA-256 in order to find another input other than “ECS655U” that gives you this specific output with at least 50% chance?

**[5 marks]**

(ii) On average, how many random inputs should you compute with SHA-256 in order to find two different inputs other than “ECS655U” that gives you this specific output with at least 50% chance?

**[5 marks]**

(b) When a cryptographic hash function is used for securely storing passwords, which one of the properties (pre-image resistance, second pre-image resistance, collision resistance) are we relying on? Explain your answer.

**[5 marks]**

(c) Does “Data Origin Authentication” prevent against Replay attacks? Briefly explain your answer. **[5 marks]**

(d) Suppose I have two friends Alice and Bob and I want to tell them the secret food recipe to eternal life! But I don't want any of them to find out anything about the secret recipe on their own! In other words, I want to force them to cooperate!

Here is the scheme someone suggests to me. Suppose the secret food recipe, encoded in some text encoding, like utf-8, is $m$.

- Generate a random sequence of bits, call it $k$, which has the same length as the binary representation of $m$.
- Compute the XOR of this random bits with the message, to get $c$, i.e., $c = (m \oplus k)$.
- Give $k$ to Alice and $c$ to Bob.

(i) Explain whether this scheme achieves my goal. That is, each of them on their own should not be able to get to the secret but together they can (by providing the exact procedure they need to follow in order to recover the secret).

**[5 marks]**

(ii) Suppose now that I have three friends, Alice, Bob and Cathy, that I want to share the secret recipe with, but making sure neither of them on their own, or any two of them, can get any information about the secret, and only if all of them cooperate can get it. Modify the above scheme to achieve this goal.

**[5 marks]**

**Question 4**

(a) Name at least 7 components that a public key certificate may contain (essential or non-essential).

**[5 marks]**

(b) Consider the following cryptographic protocol:

- Alice (the sender) and Bob (receiver) have established a symmetric key $K$, which is only known by (both) Alice and Bob.
- Both parties have already agreed on the choice of a strong symmetric-key encryption algorithm $E$, and a strong digital signature scheme with signing and verification algorithms $S$ and $V$ respectively, and a strong cryptographic hash function $H$.
- Alice has a "signing" key $\sigma_A$ that is only known by her. Associated with this signing key is a verification key $\omega_A$ which is known publicly. Similarly, Bob has a "signing" key $\sigma_B$ that is only known by him, and associated with this signing key is a verification key $\omega_B$ which is publicly known.
- Alice (the sender) performs the following on her message $m$, and sends the output $y$ to Bob over a public channel:

$$y = E_K(m) \| H\left(S(m, \sigma_A)\right)$$

For each of the following security services, determine whether our protocol provides it. Each of your answers should be supported by a brief but clear justification:

► Confidentiality

► Prevention against accidental changes

► Non-repudiation

**[15 marks]**

(c) Suppose we are visiting a specific article on the wikipedia using https and our browser (firefox, chrome, etc). For example, we are visiting *https://en.wikipedia.org/wiki/Transport_Layer_Security*.
Suppose that our employer has an application proxy, and all traffic has to go through this application proxy (a computer in the middle). For this question, you can think of the application proxy as an eavesdropper on the channel. For each of the following, determine whether or not it is visible to the eavesdropper. Provide a brief reasoning with each of your answers.

**[10 marks]**

- Source IP address (our computer)
- Destination IP address (of Wikipedia's server or load balancer)
- The URL of the page we are visiting.
- The text of the article we are reading.
- Where in the article we have scrolled to at each moment.

**End of questions**