Queen Mary
University of London

Friday 23rd February 2018 9:00 to 11:00 AM

ECS655U-ECS775P Security Engineering Midterm (20%) **Duration:** 120 minutes

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

Instructions: Enter your name and ID# on this page right away. This paper contains FOUR questions. **Answer ALL questions**. Cross out any answers that you do not wish to be marked.

Non-programmable calculators are permitted. Please state on your answer book the name and type of machine used.

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.

Full Name: .....

Student ID Number: .....

Question	Points	Score
1	25	
2	30	
3	30	
4	30	
Total:	115	

Leave this table blank.

Examiners: Dr Arman Khouzani, Dr Na Yao

Question 1

(a) Provide a short definition for each of the following security services:

[5 marks]

▷ Confidentiality:

▷ Data integrity:

(b) Does “data integrity” require “confidentiality”? Support your answer with a brief explanation.

[5 marks]

(c) For each of the following security service, determine whether or not a “digital signature” scheme can provide it. Support your claim with a brief explanation.

[5 marks]

▷ Confidentiality:

▷ Detection of Accidental Changes (e.g. due to channel noise):

(d) Provide two similarities and two differences between “Message Authentication Codes (MAC)” and “digital signatures”.

[10 marks]

▷ Two similarities:

▷ Two differences:

Question 2

(a) Consider the following symmetric encryption scheme:

- ▷ Consider a secret key K of 16 bytes, expressed in binary format (1 byte = 8 bits).
- ▷ break up the message m into blocks of 16 bytes each, applying necessary padding if need be: $m = (m_1, m_2, m_3, ...)$
- ▷ bitwise XOR each block of the message with the key block to get the ciphertext: $c = (m_1 \oplus K, m_2 \oplus K, m_3 \oplus K, ...)$

Recall: the truth table for the XOR operation is as follows (on each bit):

x	y	$x \oplus y$
0	0	0
1	0	1
0	1	1
1	1	0

(i) What is the key-space of this cryptosystem? Also what is the size of the key-space? Provide a brief description of how you arrived at your answer.

[5 marks]

(ii) Provide the corresponding decryption algorithm.

[5 marks]

(iii) Describe a method to "break" this cipher that is better than exhaustive key-search, i.e., is better than brute-force attack. (Amazingly, a similar "simple XOR cipher" was the cryptosystem used in early wireless keyboards!)

[5 marks]

(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.

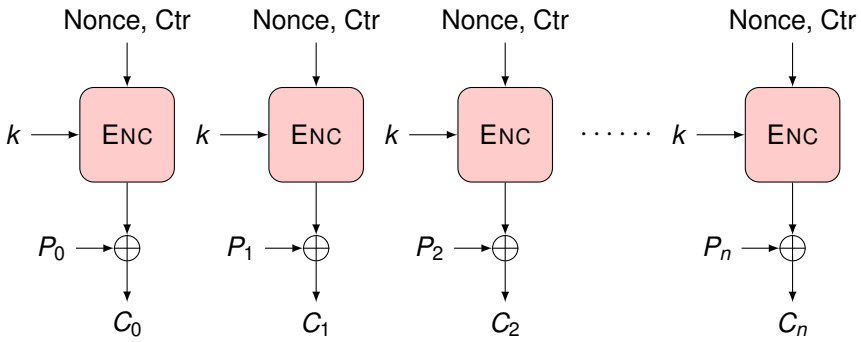

Figure 1: Q. 2-(b). Notations: $P_0,\ldots,P_n$: blocks of plaintext. "Nonce, Ctr": A counter that keeps incrementing starting from an initial value of "Nonce". $C_0,\ldots,C_n$: blocks of ciphertext. k: cryptographic key. ENC: an encryption block. $\oplus$: XOR (eXclusive OR) operator.

(i) Provide one advantage and one disadvantage of this mode of operation compared with the Electronic Code Book (ECB) mode.

[5 marks]

▷ Advantage:

▷ Disadvantage:

(ii) Draw the diagram of the corresponding decryption process.

[5 marks]

(iii) If there is an error in a single bit of the cipher text (e.g. due to noise in the channel), what would be the effect on the recovered plaintext at the receiver (using this mode of operation).

[5 marks]

Question 3

(a) Consider the following cryptographic protocol:

- Alice (the sender) and Bob (receiver) have established a symmetric key K. That is, K is "only" known by (both) Alice and Bob.
- Both parties have also already agreed on the choice of a strong cryptographic hash function H.
- Alice (the sender) construct the following message y from her plaintext message m, and sends y to Bob over a public channel:

$$y = m \| H(m) \| H(K)$$

Recall that the operator $\|$ represents concatenation (appending) of data together.

(i) 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.

[5 marks]

▷ Confidentiality:

▷ Data Integrity:

▷ Entity authentication:

(ii) Suppose the following modification is proposed: Alice first generates a random nonce n_A, and then constructs the message y from her message m as follows, and sends y to Bob:

$$y = m \parallel n_A \parallel H\big(m \| K \| n_A\big)$$

Describe the corresponding process that takes place in the receiver; i.e., what does Bob do to y upon receiving it?

[5 marks]

(iii) Now, answer part (i) for the modified protocol, that is, for each of the following security services, determine whether the modified protocol provides it. Again, each of your answers should be supported by a brief but clear justification.

[5 marks]

▷ Confidentiality:

▷ Data Integrity:

▷ Entity authentication:

(b) Here is a summary of the Diffie-Hellman key exchange algorithm:

- ▷ Both Alice and Bob (and anyone else!) know the values of two numbers: q a large prime number and α, where α has a special relation with q (it is a "primitive root" of q)
- ▷ Alice secretly selects a random number x_A less than q. She then computes $y_A = (\alpha^{x_A} \mod q)$, and sends y_A to Bob.
- ▷ Bob also secretly selects a random number x_B less than q, computes $y_B = (\alpha^{x_B} \mod q)$, and sends it to Alice.
- ▷ Alice, who has received y_B and knew X_A, computes $(y_B^{x_A} \mod q)$.
- ▷ Bob, who has received y_A and knew X_B, computes $(y_A^{x_B} \mod q)$.

(i) What is the equation that needs to hold in order for Alice and Bob to indeed reached the same value (which is their shared key).
Hint: the shared key is $(y_B^{x_A} \mod q)$ *which is at the same time equal to* $(y_A^{x_B} \mod q)$*, now just replace for* y_A *and* y_B*. You do not need to "prove" the equation!*

[5 marks]

(ii) Considering that transmission of the messages y_A and y_B happens over a public channel, and that both q and α are publicly known, why cannot an eavesdropper find out the value of the established key? (in other words, difficulty of which specific computation prevents an eavesdropper to get to the established key?)

[5 marks]

(iii) The Diffie-Hellman described as above is vulnerable to Man-in-the-Middle (MITM) attack. Describe exactly how to enhance the algorithm using public key certificates and digital signatures to be safe against MITM.

[5 marks]

Question 4

(a) Describe the “collision resistance” property of a cryptographic hash function.

[5 marks]

(b) The following is proposed as an improvement to public key certificates as a way to enable easier entity authentication: besides the digital signature of the Certificate Authority, the owner of the public key also digitally signs the certificate, as a proof that she is in possession of the private key corresponding to the public key included in the certificate. What is the problem with this proposition?

[5 marks]

(c) Explain why the following simple attack does not work on digital signatures: "although the attacker does not have access to the signing key, she can just copy/paste the digital signature of a message m_1, and append it to a message of her own m_2 as its digital signature."

[5 marks]

(d) In the SSL/TLS protocol, after the "handshake protocol" is done and a master key is established, a key derivation function is used to create many symmetric keys. List four of these symmetric keys (based on what they are used for during the "record" protocol). **[5 marks]**

(e) Recall that HTTPS is just running HTTP over TLS. It is often argued that HTTPS is not required for static websites used for streaming, or holding some public information. The argument is that since there is no sensitive data being transmitted from a client to the server, and the secrecy of the information is not needed, then a HTTP suffices. What is your analysis of this argument?

[10 marks]

End of questions