Queen Mary
University of London

SAMPLE FINAL **Examination Period: 2018**

ECS655U-ECS775P **Security Engineering** Duration: $2\frac{1}{2}$ hours

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

Instructions: 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.

Complete all rough workings in the answer book and cross through any work that is not to be assessed.

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.

It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the exam room.

Examiners: Dr Arman Khouzani, Dr Na Yao

Question 1

(a) (i) Define “data origin authentication” and “entity authentication” security services.

[5 marks]

(ii) Provide a practical example setting in which “data origin authentication” is required but not “entity authentication”. Similarly, provide another example practical scenario where specifically “entity authentication” is required.

[5 marks]

(b) Explain whether “non-repudiation” implies “entity authentication”.

[5 marks]

(c) Recall that the following describes the basic RSA public-key cipher, the encryption of the message “*m*”, and the decryption of the ciphertext “*c*”:

$$\text{Encryption: } \mathrm{Enc.}(m, e, N) = m^e \mod N$$

$$\text{Decryption: } \mathrm{Dec.}(c, d, N) = c^d \mod N$$

(i) For the cipher to be correct, the decryption process needs to recover the message. What mathematical equation needs to be satisfied for this to hold? *Hint:* You need to replace for the ciphertext “*c*” – the relation should not involve “*c*”.

[3 marks]

(ii) Consider the parameters to be $e = 3$, $d = 7$, $N = 33$. What is the encryption of the message *m* encoded as 5. That is, what is the ciphertext for the plaintext message $m = 5$.

Reminder: x $\mod$ *N means the “remainder” of diving x by N. e.g. 13* $\mod$ *6 = 1 because 13 = 2×6 + 1, i.e., 1 is the remainder after 13 is divided by 6.*

[3 marks]

(d) Consider the following diagram describing the decryption algorithm in a particular mode of operation of a block cipher like AES:

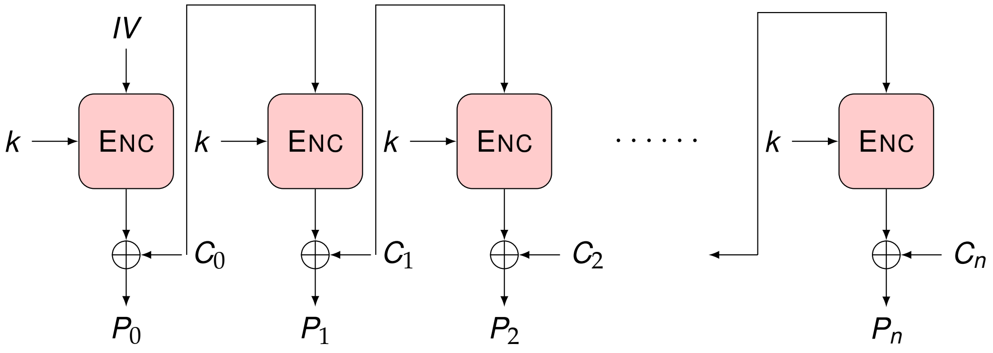

Figure 1: Q. 1-(d). Notations: $C_0,\ldots,C_n$: blocks of ciphertext. k: cryptographic key. IV: Initialization Vector. ENC: an encryption block. $\oplus$: XOR operator. $P_0,\ldots,P_n$: blocks of plaintext.

Draw the diagram of the corresponding encryption process.

[4 marks]

Question 2

(a) Consider the following cryptographic protocol:

- Alice and Bob have agreed on the use of a strong digital signature scheme, including the signing algorithm $\mathrm{sig}(\cdot)$ and the verification algorithm $\mathrm{ver}(\cdot)$;
- Alice and Bob each have their own signature keys k_1 and k_2, respectively;
- The public, including Alice and Bob, have access to a verification keys k_3 and k_4, corresponding to Alice's and Bob's signature keys, respectively;
- First Bob generates a random number n_B and sends it to Alice over the public channel;
- Alice wants to send her message m to Bob. Upon receiving n_B, she constructs the following and sends the output y to Bob over the public channel:

$$y = m \,\|\, \mathrm{sig}_{k_1}(m \| \mathrm{Bob} \| n_B)$$

A quick reminder on our notations:

- $\mathrm{sig}_k(x)$ represents the digital signature of x using the signing key k;
- and $x \| y$ represents simple concatenation (appending) of the two messages x and y together;
- "Bob" is just the public unique ID of Bob (e.g., his unique physical address).

(i) Describe the corresponding process in the receiver; i.e., describe what Bob does upon receiving y.

[3 marks]

(ii) Determine whether our protocol provides each of the following security services. Each of your answers should be supported by a brief but clear justification:

- Confidentiality
- Data origin authentication (on the message y)
- Entity authentication (of Alice for Bob)
- Non-repudiation (of Alice on the message y)

[7 marks]

(b) (i) Describe the pre-image resistance and second pre-image resistance properties of a cryptographic hash function.

[4 marks]

(ii) Suppose the following is proposed as a Hash algorithm to produce a byte-long hash of a message m:

- *Chop the message m into bytes, i.e., write the message as* $m = (X_0, X_1, \dots, X_{n-1})$ *where each* X_i *is a byte (pad* X_0 *with zeros to the left if shorter than a byte)*
- *Construct the hash of m as* $h(m) = X_0 \oplus X_1 \oplus \dots \oplus X_{n-1}$ *where* $\oplus$ *represents the bitwise XOR function.*

This hash function definitely satisfies the property of being easy to compute, but it is not suitable as a cryptographic hash function.

Explain why this hash function does not satisfy the pre-image resistance property.

[3 marks]

(iii) Explain why this hash function does not satisfy the second pre-image resistance property.

[4 marks]

(c) Answer only one of the following questions at your will:

[4 marks]

(i) Explain how brute-force attack on AES cryptosystem is different from a brute-force attack on RSA cryptosystem.

(ii) Explain how TLS/SSL complies with the principle of "key separation" principle in cryptography.

Question 3

(a) Provide an advantage and a disadvantage of Discretionary Access Control (DAC) against Mandatory Access Control (MAC).

[3 marks]

(b) Provide an advantage and a disadvantage of the “Bell-LaPadula” model (policy) against the “Biba” model (policy) in access control.

[3 marks]

(c) Recall that in the Access Control Matrix (ACM), each row is indexed by the subjects (users, processes, etc), and the columns are indexed by the objects (resources, programs, data), and the entries of the matrix are the access rights (permissions, capabilities) for the subject of that row on the object of that column. Also recall that Access Control List (ACL) correspond to the columns of the ACM, that is, there is an ACL for each object, each of which lists the pairs of subjects and their rights on that object. Also, Capability List (C-List) correspond to the rows of the ACM, that is, for each subject, we have a C-List that contains the pairs of objects and the rights of the user on that object for all the objects in the system. Given this reminder explanation, answer the following questions.

(i) Consider the following scenario: Arman can read and write to file `file1`, read file `file2` and has no access to `file3`. Na can read `file1`, read and write to `file2` and can execute `file3`. Provide the Access Control Matrix (ACM) that describes these access rights.

[2 marks]

(ii) Now, suppose an OS implements these access controls using ACLs. Provide the Access Control Lists (ACLs) that pertains to this scenario.

[3 marks]

(iii) Similarly, if we had implemented C-Lists, what would be the capability lists (C-Lists) describing the above access rights?

[3 marks]

(iv) For each of the following actions, determine which implementation of access control, ACL or C-List, is more efficient. Provide a brief reasoning for each of your answers.

- When a user wants to execute a file, and the OS needs to decide whether to grant access to that user.
- When we want to answer who are all the users that can read a certain file.
- When we want to revoke (cancel) all the access rights of a specific user.

[5 marks]

(d) Recall that one of the methods to prevent buffer overflows was using (stack) “canaries”. A stack canary is a specific pattern (e.g. a randomly selected integer) that the compiler adds to each function to demarcate its stack region and buffers, so that if the pattern is changed, this would be a sign that this border is overwritten as a result of a buffer/stack overflow. This will immediately stop the execution of the program (before going to the return address, which can be overwritten) and raises an exception which is eventually handled by OS's default exception handler.

(i) Explain why the "canary" values must be selected randomly.

[3 marks]

(ii) Explain whether an attacker that can overwrite the pointer of an exception handler of the program can bypass this defence.

[3 marks]

Question 4

(a) Describe the operational difference between stateless versus stateful firewalls? What is an advantage and a disadvantage of using a stateful vs a stateless firewall?

[3 marks]

(b) Consider the following sample packet filtering rule-set for a firewall that we are using to protect our webserver. Recall that a web server listens on port 80 for HTTP requests and listens on port 443 for HTTPS requests.

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	In	External	Internal	TCP	> 1023	80	Any	Permit
B	Out	Internal	External	TCP	80	> 1023	Yes	Permit
C	Either	Any	Any	Any	Any	Any	Any	Deny

Table 1: An example packet filtering rule-set related to problem Q4.part(b). Note: Src.: Source, Dest.: Destination, Addr.: (IP) Address.

(i) What is the role of rule B (second row in the table), i.e., why do we need to have that rule?

[3 marks]

(ii) After using this firewall, we noticed that our https webpages are not accessible! Fix the above firewall to also people to access our https pages.

[3 marks]

(c) What is DMZ (demilitarized zone) in computer security. Name 2 examples of services that are typically placed in DMZ.

[3 marks]

(d) Explain to what degree serving an application on https (http running on a secure channel created by TLS) can prevent against Cross-Site-Scripting (XSS) attacks.

[3 marks]

(e) Name and describe two different methods to defend against SQL-injection attacks.

[5 marks]

(f) Consider your company has some important IT assets and is hence considering to adopt a cyber-security plan. After running some penetration testing and risk analysis, expert A has recommended plan A, while expert B has independently suggested plan B. Provide your comparison of these two plans in terms of the trade-offs involved.

[5 marks]

Cyber-security Plan A	Cyber-security Plan B
Require all staff to go to monthly training sessions regarding social engineering attacks like phishing	Install an anti-spam/anti-phishing filter on the internal mail-server.
Require all passwords to be at least 18 characters long and be a combination of letters, numbers and special characters	Implement multi-factor authentication
Disable the right of any staff to install any new software on their machines	log the newly installed programs
Install all software patches as soon as they are released	Install only patches marked as critical every weekend
Install anti-malware software on all devices	blacklist (block access to) known malicious websites in the network firewall

End of questions