UNIVERSITY OF LONDON

BSc EXAMINATION 2024

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

IY2760: Introduction to Information Security
IY2760R: Introduction to Information Security – for FIRSTSIT/RESIT CANDIDATES

Time Allowed: **TWO hours**

Please answer **ALL** questions

Calculators are not permitted

1. *Security concepts, elements of cryptography.*

   (a) Alice and Bob want to communicate securely over an insecure channel.

   Name one security service that might be provided to address the threat of information leakage. What security mechanism might be used to provide this security service?

   [6 marks]

   (b) Suppose Alice and Bob share a secret key K, and they use a symmetric key encryption system to encrypt their communication using this key.

   An adversary Oscar wants to launch an attack on their communication system.

   i. Under Kerckhoff's assumption, what information do we assume Oscar has?

   [4 marks]

   ii. State one possible goal of Oscar's attack.

   [4 marks]

   iii. Give one example of an active attack that Oscar might launch. What security service can be compromised if such an attack is successful?

   [6 marks]

   (c) Describe one aspect of the one-time pad that makes it impractical to use for frequent bulk communication.

   [5 marks]

2. *Symmetric/secret key cryptography, integrity mechanisms.*

   (a) With the aid of a diagram, describe a stream cipher and how it operates during encryption.

   [6 marks]

   (b) The CBC block cipher mode of operation encrypts n-bit plaintext blocks $m_1, m_2, \ldots, m_q$, resulting in ciphertext blocks $c_1, \ldots, c_q$, as follows:

   $$\begin{aligned} c_0 &= IV, \text{ an } n\text{-bit initialisation vector,} \\ c_i &= e_K(c_{i-1} \oplus m_i),\ i = 1, \ldots, q. \end{aligned}$$

   Here $e_K(x)$ denotes using the block cipher e to encrypt x using key K.

   If one ciphertext block c_j is transmitted in error, how many plaintext blocks will be affected in the decryption? Explain your answer briefly.

   [6 marks]

   (c) A hash function $h(\cdot)$ is used as part of a digital signature scheme: a message m is hashed, and a function based on the private signing key is applied to $h(m)$ to produce the signature. Explain what the property "collision resistance" means for hash functions, and why h should have this property in this application.

   [7 marks]

   (d) Suppose Alice and Bob share a secret key K and a message authentication code (MAC) algorithm f. Suppose Alice wants to send a message m to Bob with data origin authentication. She computes the MAC $f_K(m)$ on m, and sends $(m, f_K(m))$ to Bob.

   What steps must Bob take to gain assurance that this message m does indeed come from Alice?

   [6 marks]

3. *Asymmetric/public key cryptography, entity authentication, digital signature, key establishment.*

   (a) Suppose Alice and Bob use a public key encryption system, and Bob has public key PK_B and secret key SK_B.

   Now, suppose Alice generates a new secret key K for use in a block cipher to encrypt a long message m to Bob. Describe briefly how Alice might use Bob's key pair (PK_B, SK_B) to allow Bob to recover m. (We assume that Bob knows which block cipher Alice uses.)

   [5 marks]

   (b) Suppose Alice and Bob share a secret key K_{AB}, known only to them. Consider the following key establishment protocol:

   1. Bob $\rightarrow$ Alice: R_B
   2. Alice $\rightarrow$ Bob: $e_{K_{AB}}(k_s|R_B|i_B)$

   Here $e_K(x)$ denotes encrypting x using key K, R_B is a random number generated by Bob, i_B is a (public) identifier for Bob, and k_s is the session key generated by Alice.

   i. Does this protocol provide entity authentication of Alice to Bob? Explain your answer briefly.

   [5 marks]

   ii. Implicit key authentication is the assurance that no one other than the specified parties has access to the key. Does this protocol provide implicit key authentication with respect to the session key k_s? Explain your answer briefly.

   [5 marks]

   (c) i. What is meant by non-repudiation?
   ii. How does a digital signature scheme with appendix provide this service?
   iii. Does such a scheme also provide data integrity? (Answer yes or no.)
   iv. Does such a scheme also provide confidentiality? (Answer yes or no.)

   [10 marks]

4. *Computer and network security.*

(a) Give one reason why we use access control.

[6 marks]

(b) An access control matrix has rows indexed by subjects and columns indexed by objects. How is an access control list related to an access control matrix? State one disadvantage of access control lists.

[7 marks]

(c) Describe briefly one principle of secure software design. [6 marks]

(d) Name the following malware types:

i. This type of malware can look like a useful program but may allow an attacker unexpected access to some resources when invoked.

ii. This type of malware can collect user information from a computer by monitoring the user's web-browsing habits.

iii. This type of malware can replicate and insert itself into other pieces of code.

[6 marks]

END