UNIVERSITY OF LONDON

BSc EXAMINATION 2019

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

IY2760/IY2760R : Introduction to Information Security
PAPER FOR FIRST SITS/RESIT CANDIDATES

Time Allowed: **TWO** hours

Answer **ALL** questions
Calculators are NOT permitted

Answer **ALL** questions.

1. Introduction and concepts

(a) State Kerckhoffs' Principle [2 marks]

(b) The following substitution cipher is to be used to encrypt and decrypt plaintext (top row) to cipher text (lower row):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	Y	N	B	R	G	M	T	Z	S	C	O	A	W	K	F	I	X	P	V	D	Q	U	H	J	E

Figure Q1.

(i) Encrypt the plain text BROKE [1 mark]

(ii) Decrypt the cipher text RLPV [1 mark]

(iii) Is this a simple Caesar cipher? Why not? [3 marks]

(iv) How many possible keys are there for this type of cipher? [1 mark]

(v) What can we do to enhance an alphabetic based cipher? Give 2 examples. [3 marks]

(vi) What are the 3 characteristics required to make these ciphers practically unbreakable? [3 marks]

(c) Explain the key ideas used in cryptanalysis of mono or polyalphabetic ciphers. Include example data characteristics from the English language in your answer.

[5 marks]

(d) Introduce the two types of adversary that we typically assume will engage with a cryptographic protocol. For each adversary identify their capabilities and limitations.

[6 marks]

NEXT PAGE

2. Cryptography

(a) Stream Ciphers

(i) Describe, preferably with the aid of a block diagram, how a stream cipher encrypts data. [4 marks]

(ii) Discuss the speed of encryption and the error propagation properties of stream ciphers. [2 marks]

(iii) Briefly outline the three main properties that a stream cipher keystream generator must satisfy in order to be considered as secure. [3 marks]

(b) Block Ciphers

(i) Describe, preferably with the aid of a block diagram, how a block cipher operates during encryption, identifying typical block sizes etc. [4 marks]

(ii) Name up to 3 different modes of operation for a block cipher (e.g. consider the modes available for DES) and describe with the aid of a block diagram one of these modes of operation for the process of encryption. [7 marks]

(c) Message Authentication Codes (MACs)

(i) Identify what property MACs typically provide with respect to the CIA triad. [1 mark]

(ii) Let $M = m_1 \,||\, m_2 \,||\, m_3$ be plaintext, where m_1, m_2, m_3 are each 64 bit blocks and $||$ denotes concatenation of the blocks. Describe how to compute a MAC value for M using the CBC-MAC mode. You may use a diagram in your answer. [4 marks]

NEXT PAGE

3. Authentication and protocols

(a) Briefly define the term 'Information Security Policy' and what would one typically include? [3 marks]

(b) Describe two reasons why *Passwords* and *Personal Identification Numbers* (PINs) are considered weak authentication mechanisms. Give three examples of mechanisms that can be applied in a computer system that could be used to enhance the use of passwords or pins. [5 marks]

(c) Specify the five component modules that are seen in typical biometric systems for personal authentication. For each module describe its role. [10 marks]

(d) Consider the following protocol for two pass authentication from ISO/IEC 9798-1 where a symmetric cryptographic algorithm with a single shared key K_{AB}, is used between Alice (A) and Bob (B) to encrypt and decrypt messages used to authenticate A to B (or vice versa).

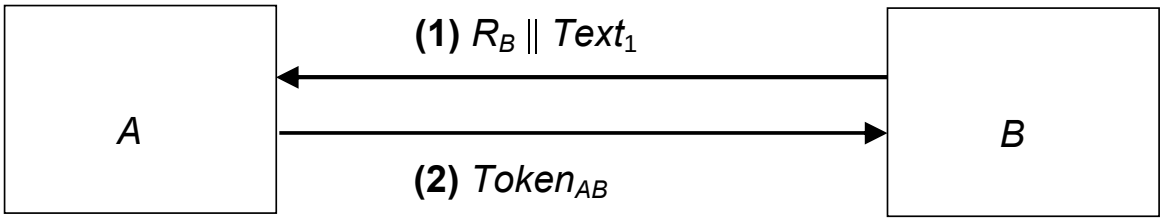

Figure Q.3 Two pass authentication protocol.

(i) What are the typical components that we would see in $Token_{AB}$ and what are their significance (or contribution) in the protocol? [3 marks]

(ii) How could this protocol be extended to provide three pass authentication? In your answer provide an example of the information exchanged. [4 marks]

NEXT PAGE

4. Network and Computer Security

(a) The Diffie-Hellman protocol can be used by two communicating parties to establish a shared secret key for use with a cipher to provide confidentiality during a communication session.

(i) Describe the operation of the Diffie-Hellman protocol, covering what the participants generate, what they send, and how the final shared key is calculated.

[7 marks]

(ii) Explain how the Diffie-Hellman protocol is vulnerable to an attack by an active adversary.

[3 marks]

(iii) Outline how active attacks on the Diffie-Hellman protocol might be prevented by using digital signatures.

[2 marks]

(b) SSL/TLS are the default protocol for communicating between applications such as web browsers.

(i) List the three goals of the TLS Handshake Protocol. [3 marks]

(ii) Explain the MAC-Encode-Encrypt operation performed in the TLS Record Protocol, detailing the structure of the data that is handled.

[6 marks]

(iii) Name and briefly discuss an attack on the TLS Record Protocol.

[4 marks]

END

 PK