UNIVERSITY OF LONDON

BSc EXAMINATION 2023

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

1. *Security concepts, elements of cryptography.*

(a) We say that a simple substitution cipher is not computationally secure against a ciphertext-only attack, given enough ciphertext.

i. Explain what is meant by “computationally secure”.

ii. Why is “given enough ciphertext” in the above statement important?

(Only brief answers are required. Do not write more than two or three lines.)

[12 marks]

(b) A binary block cipher has block size 128 bits and key length 56 bits.

i. What is the size of the key space?

ii. Do you regard this as sufficiently secure? Explain your answer briefly.

[10 marks]

(c) Suppose a Vigenère cipher is used to encrypt English plaintext. We use the conventional correspondence between letters of the alphabet and the numbers $0, \ldots, 25$:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Suppose the key chosen is “OK”. What is the correct encryption of the plaintext “FAB”?

[3 marks]

2. *Symmetric key cryptography, integrity mechanisms*

(a) Suppose you intercepted 8 bits of ciphertext encrypted using a stream cipher with a keystream of period 5:

$$c_0c_1c_2c_3c_4c_5c_6c_7 = 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1.$$

Suppose that you know that the first 3 bits of the corresponding plaintext are

$$p_0p_1p_2 = 0\ 1\ 1,$$

and suppose you found out that the 4th and 5th bits of the keystream are

$$k_3k_4 = 1\ 0.$$

Write down the first 5 bits of the plaintext $p_0p_1p_2p_3p_4$ and the first 5 bits of the key stream $k_0k_1k_2k_3k_4$.

[6 marks]

(b) Suppose we have a binary block cipher B with 80-bit block size and 128-bit key. The encryption algorithm uses an encryption function $e_k(x)$, where e takes as input a binary block x of size 80 and key k of size 64. The encryption function of $B_K(x)$ is as follows:

Write K as two bit strings of equal length, $K = k_1||k_2$, where k_1 and k_2 are 64-bit strings, and $||$ denotes concatenation. Then

$$B_K(x) = e_{k_2}(e_{k_1}(x)).$$

i. Given a plaintext-ciphertext pair, how many pre-computations are required, and how many decryptions are required, in a meet-in-the-middle attack? Pick the correct answer. (You only need to write down the letter corresponding to your choice.)

A. 2^{64} pre-computations, 2^{80} decryptions.
B. 2^{128} pre-computations, 2^{64} decryptions.
C. 2^{128} pre-computations, 2^{128} decryptions.
D. 2^{64} pre-computations, 2^{64} decryptions.
E. 2^{80} pre-computations, 2^{80} decryptions.
F. 2^{64} pre-computations, 2^{128} decryptions.

ii. How many bits is the perceived security of B? There is no need to justify your answer.

iii. How many bits is the effective security of B? There is no need to justify your answer.

[7 marks]

(c) Alice uses CBC-MAC without optional processing to compute message authentication codes. We write $MAC(m)$ to denote the message authentication code on a message m.

Oscar observed on one occasion that Alice sent (m_1, MAC_1) to Bob, where $MAC_1 = MAC(m_1)$, and on another occasion Alice sent (m_2, MAC_2) to Bob, where $MAC_2 = MAC(m_2)$.

Oscar now sends

$$(m_1',\ m_2', MAC')$$

to Bob, where $m_1' = m_1$, $m_2' = m_2 \oplus MAC_1$, and $MAC' = MAC_2$.

Explain why Bob accepts that $m_1',\ m_2', MAC'$ is from Alice.

[8 marks]

(d) Alice stores a file m on a disc and computes a hash $y = h(m)$ using the hash function h. She makes sure that the integrity of y is protected. Oscar observes y and m. He finds another file m' such that $h(m') = y$, and replaces Alice's file m with m'.

Precisely what property should h have so that Oscar cannot do this feasibly?

[4 marks]

3. *Public key cryptography, entity authentication, digital signature.*

(a) i. What hard computation problem does the RSA public key cryptosystem rely on?

ii. Name one randomised public key cryptosystem.

[5 marks]

(b) Consider the following authentication protocol:

We assume that Alice and Bob share a secret key K, and that this secret key is known only to Alice and Bob.

1. Bob → Alice: r_B
2. Alice → Bob: $e_K(r_A, r_B, i_B)$
3. Bob → Alice: $e_K(r_B, r_A)$

Here r_A, r_B are random numbers generated by Alice and Bob respectively, $e_k(x)$ denotes encrypting plaintext x with key k using encryption algorithm $e()$, and i_B is an identifier for Bob.

i. Does Alice authenticate herself to Bob in the protocol? Explain your answer by pointing out which part of which message(s) achieves this and why, if any.

ii. Which value assures Bob that this is a fresh run of the protocol with Alice and not a replay?

[12 marks]

(c) i. What is the main security service that digital signature provides?

ii. Consider Alice's RSA digital signature scheme with the following parameters:

$$N = 55,\ p = 5,\ q = 11,\ x = 27,\ y = 3,\ xy = 1 \bmod 40.$$

Suppose Alice's signing key is 3. Now, suppose Bob receives the message-signature pair $(18, 2)$.

How does Bob decide whether to accept this as a valid message-signature pair from Alice? (Write down the equation that must be satisfied using the numbers on the list above, but do not perform any calculation.)

[8 marks]

4. *Key management, computer and network security.*

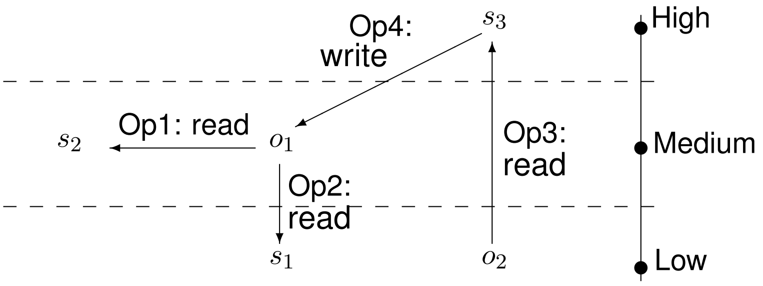
(a) The Diffie-Hellman key exchange protocol works as follows:

- Public parameters consist of a prime p and a primitive element α.
- Alice chooses secret x_A at random $(0 \leq x_A \leq p-2)$ and sends $y_A = \alpha^{x_A} \bmod p$ to Bob.
- Bob chooses secret x_B at random $(0 \leq x_B \leq p-2)$ and sends $y_B = \alpha^{x_B} \bmod p$ to Alice.
- The secret key shared between Alice and Bob is $k = y_B^{x_A} = y_A^{x_B} = \alpha^{x_A x_B} \bmod p$.

However, this protocol has a security weakness - it does not provide entity authentication. The Station-to-station (STS) protocol fixes this. Describe the STS protocol, including details about how it fixes the authentication problems.

[12 marks]

(b) A tactical IT system takes advantage of the information flow policy to manage user access (read and write operations) to its databases. The diagram below shows the security labels of the subjects (s_1, s_2, s_3), and the security labels of the data objects (o_1 and o_2). Which of the operations (Op1, Op2, Op3, Op4) are permitted and which ones are denied?



[8 marks]

(c) My organisation wants to make sure that any new attacks on our system can be detected by our intrusion detection system. What type of behaviour analysis should we opt for: signature-based or anomaly-based? Briefly justify your answer.

[5 marks]

END