UNIVERSITY OF LONDON

GOLDSMITHS COLLEGE

Department of Computing

B. Sc. Examination 2020

IS53012B
Computer Security

Duration: 2 hours 15 minutes

Date and time:

This paper is in two parts: part A and part B. You should answer ALL questions from part A and TWO questions from part B. Part A carries 40 marks, and each question from part B carries 30 marks. The marks for each part of a question are indicated at the end of the part in [.] *brackets.*

There are 100 marks available on this paper.

Electronic calculators must not be programmed prior to the examination. Calculators which display graphics, text or algebraic equations are not allowed.

THIS PAPER MUST NOT BE REMOVED
FROM THE EXAMINATION ROOM

Part A

Question 1 All parts require an answer of True or False with justifications. You should read each statement carefully and then determine whether the statement is TRUE or FALSE. If the statement is true, explain why it is true or give a supportive example or reasoning. If it is false, give the correct answer or provide a counterexample or reasoning.

(a) A *security model* is a means for informally expressing the rules of the security policy in an abstract way. [5]

(b) A control is a potential to do harm. A vulnerability is a means by which a threat agent can cause harm. A threat is a protective measure that prevents a threat agent from exercising a vulnerability. [5]

(c) The product of two relatively simple ciphers, such as a *substitution* and a *transposition*, cannot achieve a high degree of security. This is because that ideally a substitution cipher contributes to the confusion property where as a transposition to the diffusion property. [5]

(d) A lattice is a mathematical structure that can be used to device a secure access control system. The system of all subsets of a finite set, under the operation "subset of" ($\subseteq$) forms a lattice. [5]

(e) A well designed block cipher should have a large blocksize (alphabet size) to prevent exhaustive search attacks, and a small keysize to prevent statistical analysis attacks. [5]

(f) The traditional authentication methods are unsuitable for use in computer networks mainly because they do not use cryptographical techniques. [5]

(g) The *Chosen-ciphertext-only attack* is the type of attack where an analyst has the least amount of information to work with. [5]

(h) "$f(X) = 2X$ is a one-way function as it is 'easy to compute one way and difficult to invert'. If $X = 500$, for example, it is easy to compute that $f(500) = 2 \times 500 = 1000$ but if given $f(X) = 1000$, it is hard to compute the X since there can be many possibilities of X." [5]

Part B

Question 2

(a) Bob wants to minimise the total number of transmission bits after encrypting his secret plaintext message to Alice. He therefore compresses the ciphertext before sending it off. Comment on Bob's approach in the context of security and give your reasons. [3]

(b) In conventional cryptology literature in Computer Security, two characteristic names, *Alice*, and *Bob* are used to refer to the sender and receiver of messages. It is assumed that Alice and Bob are physically separate and that they can communicate with each other over some *insecure* channel. Give two reasons to explain why the channel must be assumed to be insecure. [6]

(c) What is the *congruence relation* for $4 \equiv 17(\text{ mod } 13)$? Rewrite the expression in its modular arithmetic notation. [3]

(d) Suppose Alice generates a one pad key $k = 010001$, and uses it to encrypt two messages $m_1 = 011011$ and $m_2 = 110101$ using `XOR` and sent to Bob the ciphertexts c_1 and c_2 respectively. Demonstrate by intercepting c_1 and c_2, how Charlie, the analyst can work to get closer to the original plain texts. [8]

(e) The cipher text "`WKLV PHVVDJH LV QRW WRR KDUG WR EUHDN`" was produced using a Caesar cipher on a message consisting of only the uppercase English letters plus a 'blank' character which was translated to itself. Demonstrate how clues from the ciphertext can be used to determine the shift value and recover the plaintext. Briefly explain your approach and show all your work. [10]

Question 3

(a) Describe how the *two-phase commit* protocol works in distributed database systems. [6]

(b) Explain what it is meant by a *generator for prime p* when the discrete logarithm problem is discussed for a cryptographic protocol. Demonstrate why 2 is not a generator for prime 7. [7]

(c) Demonstrate how a *one-time key pad* of a certain length may be generated iteratively without a cycle using the XOR operator $\oplus$ and the initial key 1011. Describe briefly the algorithm that you use. [5]

(d) Explain what is the main disadvantage of the *one-time key pad* despite offering perfect secrecy. [4]

(e) Consider each of the scenarios below and write down yourself advice, as a security expert to the general public, on what to do in each of the situations. Justify your answers, and, if necessary, add assumptions to ease your discussion.

i. You received an urgent request from your line-manager who lost his login password at an important overseas conference and asking you for the password. [4]

ii. You have to send one password to a remote site. [4]

Question 4

(a) Demonstrate how the Vernam cipher works, using the example of
the plaintext "`1110 0110 1110 111`" and
the one-time key pad 1111 0101 1001 000,
applying the `XOR` (addition modular 2) operation. [6]

(b) Describe the Fermat's Little Theorem and demonstrate how the theorem can be used to determine 4^{11} mod 11. What is the value of 3^7 mod 8? Show all your work. [5]

(c) Alice would like to receive a secret message $m = 5$ from Bob using the El Gamal public key encryption scheme. She was advised to set up keys first and was given the following algorithm to generate her keys:

(1) Choose a prime number p
(2) Choose a random number g (less than p)
(3) Choose a random number a (less than p)
(4) Compute $y = g^a$ mod p.

Following the advice, Alice chose $p = 11, g = 3, a = 8$, but was told later by her friend that both the given algorithm and her chosen values are flawed.

i. Identify the errors in the key-generation algorithm and write your corrections. [5]
ii. Explain which value chosen by Alice is wrong. Suggest a correct value for Alice. Justify your answer and show all your work. [5]
iii. Determine y. Write the public key and private key. [3]
iv. Bob now can encrypt the (short) message $m = 5$. Assume Bob chooses $k = 9$. Devise the $ciphertext(m)$. [6]