This exam contains two sections:

Section 1 consists of questions 1 & 2;

Section 2 consists of questions 3 & 4.

Attempt one question from each section.

Please note that this differs from the usual structure of Computer Science exams.

If you are in any doubt as to what you should do, then *please ask an invigilator*.

CS-M18 Section 1: Cryptography – May/June 2006

(Attempt either Question 1 or Question 2)

Question 1.

(a.) (Block encryption systems)

i) The underlying structure of the Data Encryption Standard (DES) encryption algorithm is a Feistel network. Briefly list the main characteristics of a Feistel network and name the main cryptographic operations used in the DES algorithm.

[8 marks]

ii) DES is not considered to be secure anymore. Explain why. Name two significant differences between DES and the Advanced Encryption Standard (AES) algorithm. What were the main criteria applied by NIST (National Institute of Standards and Technology) when choosing AES?

[5 marks]

(b.) (Cryptographic check values)

i) What properties need to be fulfilled by a cryptographic hash function in general?

[3 marks]

ii) What are the differences between modification dectection codes and message authentication codes?

[2 marks]

Consider the following hash algorithm H applied to a message M consisting of n 64-bit blocks $M_1, \dots, M_n$.

$$\begin{aligned} H_0 &:= \text{Initial value} \\ H_i &:= E_{M_i}(H_{i-1}) \\ V &:= H_n \quad \text{(hash value)} \end{aligned}$$

where E_{M_i} denotes the use of a symmetric encryption algorithm E with M_i as key. The corresponding decryption algorithm with key M_i will be denoted by D_{M_i}.

Assume Alice has intercepted the message M and its hash value V_M and is interested in generating a new message which has the same hash value. To this end, she chooses a message M' (with her desired content) consisting of $n-2$ blocks, computes H_{n-2} (i.e. the hash algorithm applied to the $n-2$ blocks) and searches for two blocks X and Y such that $E_X(H_{n-2}) = D_Y(V_M)$.

iii) How should Alice extend her message M' to obtain a message with the same length and the same hash value as M? Justify your answer.

[3 marks]

iv) Jill, a friend of Alice, suggests a different method to Alice. Alice should freely choose a message with $n-1$ blocks (instead of $n-2$) and then search for a block M'_n such that the hash value of the new complete message is the same as that of M. Which of the two approaches is more feasible?

[4 marks]

Question 2.

(a.) Name and explain the two most important computer security goals.

[4 marks]

(b.) i) Explain (e.g., by using a diagram) how symmetric/asymmetric encryption works in general.

ii) A drawback when using a block encryption system is that two identical plaintext blocks result in the same ciphertext. How can this be avoided?

iii) Assume we are using a symmetric block encryption system which allows keys of different lengths. Which is more secure with respect to brute force attacks: sequential encryption using two 64 bit keys, or using one key of length 128? Justify your answer.

[7 marks]

(c.) Why should a onetime pad (or a key-stream in a stream cipher) not be used twice? Describe first a scenario where a plaintext/ciphertext pair and a second ciphertext (which was encrypted with the same key/key-stream) is known, and second a scenario in which only two ciphertexts are known to the attacker.

[4 marks]

(d.) i) What is the discrete logarithm to the basis 2, modulo 11, of 7?

ii) Alice and Bob want to exchange a key using the Diffie-Hellman Key exchange scheme. They agree on the prime number $p = 11$ and the primitive root $g = 2$. Moreover, A chooses $r_A = 5$ and B chooses $r_B = 4$. What is the common key both will have after the exchange?

iii) Eve wants to 'influence' the conversation between Alice and Bob. What kind of attack can she do and what is necessary in order for her to be able to perform the attack?

[5 marks]

(e.) Consider the following non-complete version of the Needham-Schröder protocol:

(1) $A \rightarrow S$: (A, B, N_A)
(2) $A \leftarrow S$: $\{N_A, B, k_{AB}, \{k_{AB}, A\}^{k_{BS}}\}^{k_{AS}}$
(3) $A \rightarrow B$:
(4) $A \leftarrow B$:
(5) $A \rightarrow B$:

Complete steps (3) – (5) and discuss what information is known to A and B after each step.

[5 marks]

CS-M18: Section 2: Security in Practice – May/June 2006

(Attempt either Question 3 or Question 4)

Question 3.

(a.) Discuss each of the following statements, saying whether you think it is valid or not, and defending your position.

i) "Security is a process, not a product."

ii) "Two-factor authentication is a useful tool for protecting local logins."

iii) "OpenBSD's *StackGap* buffer overflow prevention technique may be defeated by the use of a *NO-OP sled*." (It is not necessary to describe buffer overflows, NO-OP sleds, or StackGap in detail.)

[5 marks]

(b.) i) What is the purpose of a *port scan*?

ii) How do *TCP SYN* scans and *TCP ACK* scans help an attacker, and how may they be defended against?

iii) Given the existence of powerful dedicated vulnerability scanners such as `nessus`, why would anyone still use a port scanner such as `nmap`?

[6 marks]

(c.) In the context of password cracking:

i) Compare & contrast *brute force*, *dictionary* & *brute dictionary* attacks.

ii) *Rainbow tables* 'trade off' time vs memory in order to make fast password cracking feasible under certain circumstances. How do they work?

iii) Explain the use of *salt* in password encryption. Specifically, what is salt, and what benefits does it give?

[8 marks]

(d.) *Public Key Infrastructure* (*PKI*) and *Web of Trust* are two approaches to solving the *public key distribution problem.*

i) Briefly outline the key features of a PKI.

ii) Briefly outline the key features of a Web of Trust.

iii) For each approach, state one advantage it has over the other.

[6 marks]

Question 4.

(a.) Discuss each of the following statements, saying whether you think it is valid or not, and defending your position.

i) "Biometrics are useful for authentication."

ii) "Heap based buffer overflows are less dangerous than stack based buffer overflows."

iii) "If your web browser warns you that it can't authenticate a site's certificate, that means a hacker is performing a Man-In-The-Middle attack."

[5 marks]

(b.) Two users, Alice and Bob, both use the `ssh` utility to activate an interactive shell session on the remote host `dragon.example.com`. Alice is asked to supply the password for `alice@dragon.example.com`, but Bob is asked to supply a *passphrase* instead and doesn't type `bob@dragon.example.com`'s password at all.

i) What's happening here? Why weren't they both asked for a password? Where are the password and passphrase being checked, and against what?

ii) Briefly discuss the advantages and disadvantages of each of these methods of authentication, in terms of both security and usability.

[5 marks]

(c.) i) Outline the principle of a *Virtual Private Network* (*VPN*).

ii) Describe the use of IPSec *tunnel mode* to create a VPN.

ii) Why would you not use IPSec *transport mode* in order to create a VPN?

[5 marks]

(d.) The *principle of least privilege* states that users and processes should have the minimum privileges necessary in order to achieve their tasks.

Describe two techniques used by OpenBSD for achieving least privilege for *processes.*

[4 marks]

(e.) Until 2001, *Wired Equivalent Privacy* (*WEP*) was the main standard for securing 802.11 wireless networks. What are the flaws in WEP's confidentiality mechanisms?

[6 marks]