THE CATHOLIC UNIVERSITY OF EASTERN AFRICA

A. M. E. C. E. A

P.O. Box 62157

00200 Nairobi - KENYA

Telephone: 891601-6

Ext 1022/23/25

Fax: 254-20-891084

MAIN EXAMINATION

MAY – AUGUST 2021

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE

REGULAR PROGRAMME

CMT 447: WEB APPLICATION SECURITY

Date: AUGUST 2021	**Duration: 2 Hours**
INSTRUCTIONS: Answer Question ONE and any TWO Questions	

Q1.

a) Consider the following **security attack** where an evil server attempts to impersonate a good server:

- The evil server obtains the certificate for the good server(available publically from certificate authorities).
- The evil server uses an active network attack to arrange for traffic from a particular browser intended for the good server to be sent to the evil server instead.
- When a client attempts to open an HTTPS connection to the good server, the evil server receives the connection open request and behaves just like the good server, returning the good server's certificate at the appropriate point in the protocol.

Assuming that the evil server can obtain a valid certificate and mount an active network attack; can the client's security be compromised? Explain your answer.

(4 Marks)

b) *Discuss* the THREE types of Cryptographic **Algorithms** used in Computer security stating where each is **suited**.

(6 Marks)

c) You have recently been appointed Systems/Network administrator at Co-operative bank, Kisumu branch. *Outline* the **measures**, **policies** and **procedures** you would put in place to ensure *security* and *integrity* of customer's data. **(6 Marks)**

d) **Show** how the RSA algorithm generates the private-public key pair using p=137 and q=181.

(6 Marks)

e) In the Diffie-Hellman protocol where q = 23, a = 9, *compute* the value of the following clearly showing your workings:

i. The **symmetric** key, K_{AB}? **(4 Marks)**

ii. The **public keys** $\mathbf{Y_A}$ and $\mathbf{Y_B}$ **(4 Marks)**

Q2.

a) *Explain* the concepts of **authentication**, **privacy**/**confidentiality**, **integrity** and **non-repudiation**.

(8 Marks)

b) By means of a valid example/illustration, show how a man-in-the-middle attack against the Diffie-Hellman key agreement protocol would be carried out.

(6 Marks)

c) Using examples/illustrations, **explain** the following terminologies as used in computer security:

i. SQL injection **(2 Marks)**

ii. Key logger **(2 Marks)**

iii. Digital signature **(2 Marks)**

Q3.

a) *Discuss* the concepts of intrusion **prevention** and **detection**. **(4 Marks)**

b) *Differentiate* between an **attack** and **threat** in information security. **(4 Marks)**

c) *Differentiate* between a **Distributed Denial of Service** (DDoS) from a **Denial of Service** (DoS) attack **(4 Marks)**

d) **explain** any FOUR *values* or *ideals* that should be included in the proposed **IT code of ethics**. **(8 Marks)**

Q4.

a) What are **honeypots**? **How** can they help in *securing* a network? **(4 Marks)**

b) Describe how PGP uses a *web of trust* for **key management** **(6 Marks)**

c) *Discuss* the information security **challenges** posed by social networking sites such as Facebook and LinkedIn. **(6 Marks)**

d) *Explain* any TWO measures you would put in place to **protect** your home Wireless Access Point (Wi-Fi). **(4 Marks)**

Q5.

a) *Define***information security**. *Discuss* the multiple **layers** of security.**(6 Marks)**

b) *Discuss* any THREE ways that can be used to **authenticate** a computer system user.

(6 Marks)

c) Using examples *differentiate* between **Symmetric** and **Asymmetric** encryption.

(4 Marks)

d) A Michelangelo **worm** has been detected on your uncle's system but unfortunately he is far away from you and he does not have the technical knowledge to eradicate it. His anti-virus software is not available. What sensible **precaution** would you advise him to *take*? **(4 Marks)**

END