United International University (UIU)

Dept. of Computer Science & Engineering (CSE)

Final Exam Year: 2021 Trimester: Fall
Course: CSE 4531 Computer Security
Total Marks: 40, Time: 2 hours (plus 15 additional minutes for upload/download)

There are THREE questions. Answer all of them. Figures in the right-hand margin indicate full marks.

Any examinee found adopting unfair means will be expelled from the trimester / program as per UIU disciplinary rules

---

1. a) Suppose you want to communicate with the Surokkha (website for Covid Vaccination) webserver. Surokkha stores your sensitive information, hence a **secure session** needs to be established between your browser and the server before exchanging information. During the session establishment your browser gave you a '**bad certificate**' warning, but you ignored it. [8]

Does accepting invalid certificate enable any attack on integrity and confidentiality? If not, explain your answer. If yes,

I. Explain how this attack may take place.

II. Why does the attack compromise integrity and confidentiality?

b) Explain why **RSA** is not allowed in **TLS v1.3** for key exchange. [4]

2. a) Let **p = 11; q = 5; e = 3; m = 3** be the values for **RSA** encryption/decryption algorithm. *Show the Key generation and Encryption steps*, i.e., generate the keys and encrypt the message **m = 3** with the keys to generate a ciphertext. *Also, show the steps to demonstrate that you can successfully decrypt the ciphertext.* [5]

b) Suppose you need to get your bank's **Public Key**, but your browser does not know the CA which issued the certificate for your bank. [4]
How can your browser be sure that the certified Public Key belongs to the bank, not to an attacker?

c) Suppose **Alice** wants to send a message **M** to **Bob**. Different cryptographic approaches can be used by **Alice** and **Bob**. For describing the approaches, the following terminologies are used: [2*2=4]

M	Plaintext Message
PK_A **SK_A**	**Public Key** of **Alice** Corresponding **Private Key** of **Alice**
PK_B **SK_B**	**Public Key** of **Bob** Corresponding **Private Key** of **Bob**
E_{PK}	Encryption using **RSA** with the **public key PK**
$Sign_{SK}$	Signature using **RSA** with **private key SK**

Let us consider that **Alice** and **Bob** want their communication to achieve the following security properties: **Integrity** and **Confidentiality**. *For each of the following approaches, identify which property/properties will hold. Justify your answer.*

a. ***Alice*** *sends to* ***Bob***: $\mathbf{E_{PK_A}(M)}$, $\mathbf{Sign_{SK_A}(M)}$

b. ***Alice*** *sends to* ***Bob***: $\mathbf{E_{PK_B}(M)}$, $\mathbf{Sign_{SK_A}(M)}$

3. a) Suppose XYZ Company is facing several security threats and they have come up with the following table while trying to perform quantitative risk analysis. [5]

Asset	**Threat**	**Asset Value (BDT)**	**Exposer Factor**	**Frequency of Occurrence**
Customer Database	Hacked	43,25,000	0.74	1 per 2 years
Data files	Information Theft	5,00,000	0.17	1 per year
E-commerce Website	DDoS	2,30,900	0.44	2 per year

There is a security system available in the market that costs **BDT 10,00,000** a year. But it is **70%** effective.

Would it be worth investing in that security system? Justify your answer.

b) Suppose you have deployed **Kerberos** in your system. There is a **printer** as a service provider in the system and it shares a secret key $\mathbf{K_v}$ with the **TGS**. One day, an attacker compromises the printer and steals the key $\mathbf{K_v}$, but does not change the key. [4]

Can the printer still authenticate itself to a client? Justify your answer.

c) Suppose you have an e-commerce company in the European Union which sells electronic gadgets online. A customer needs to do registration before purchasing an item. However, your company is required to comply with the **General Data Protection Regulation (GDPR).** [3*2=6]

Identify whether each of the following cases is ***GDPR*** *compliant. Justify your answer. If non-compliant, suggest how compliance can be achieved.*

I. *The website contains your company's name and contact address to identify the company.*

II. *Customer 'requires' to give consent on the following: "I consent to having my data processed for the purpose of administering my purchase and I consent to marketing emails from various electronic gadget manufacturers".*

III. *Customers' Personal Data got stolen and this incident is notified to the Data Protection Commissioner after 96 hours of being identified.*