International Islamic University Chittagong

Department of Computer Science and Engineering

B. Sc. in CSE

Final Exam, Autumn 2022

Course Code: **CSE 4743** Course Title: **Computer Security**

Time: 2 hours 30 minutes Full Marks: 50

(i) The figures in the right-hand margin indicate full marks

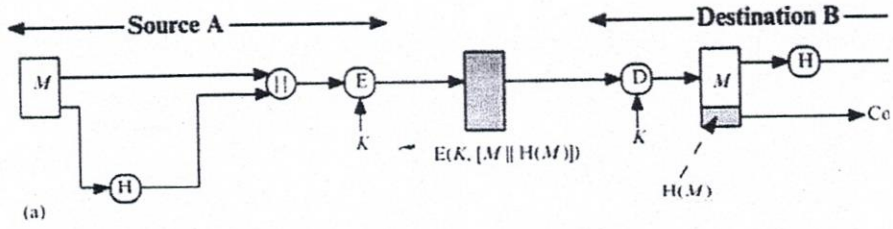
(ii) Course Outcomes and Bloom's Levels are mentioned in additional Columns

---

Part A

[Answer the questions from the followings]

					Marks
1.	a)	Write the purpose of encryption with private key and encryption with public key in Public key cryptosystems. **OR** Explain symmetric secret key distribution between two parties ensuring confidentiality and authentication.	CO1	U	5
	b)	Draw a block diagram and briefly explain the working steps of Intrusion Prevention Systems (IDS). Compare the benefits and drawbacks of IPS with IDS.	CO2	App	5
2.	a)	Explain the process given in figure:	CO1	U	5



	b)	In the Kerberos authentication shown below, why are ID_c, AD_c and ID_v included included in the encrypted ticket, why ticket is encrypted with K_V?	CO2	App	5

(1) C → AS: $ID_C \| P_C \| ID_V$

(2) AS → C: $Ticket$

(3) C → V: $ID_C \| Ticket$

$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$

OR

	b)	Design a Hash function that uses the XOR operation of inputs to get the bits of the output hash. Does such a hash function fulfill the Pseudorandmoness requirement?	CO2	App	5

Part B

[Answer the questions from the followings]

3.	a)	Explain the social engineering attack cycle. List the organizational and technical defense mechanisms against social engineering attacks.	CO3	R	4
	b)	What are the desired attributes of a cryptographic hash function? Use examples if required.	CO2	U	3
	c)	Explain how non-repudiation is ensured by using a digital signature.	CO2	App	3
4.	a)	Explain the steps of the Kerberos authentication protocol with necessry figures.	CO1	E	5
	b)	What is a digital signature? Why it is used? If a person **P** signs message **M** with signature **S(P, M)**, what are the desired properties from the security perspective?	CO1	R	5
5.	a)	Discuss some intrusion detection methods.	CO4	U	4
	b)	Show with example and explain why it is extremely difficult to insert a fake block of transaction into a block chain.	CO3	An	6

OR

5.	a)	Demonstrate some packet filtering policies that are configured in your firewall.	CO4	App	4
	b)	Explain Proof of work in Blockchain. Why is it an expensive process? What is the benefit of having such a process in Blockchain.	CO3	U	6