VIT
Vellore Institute of Technology

School of Information Technology and Engineering

Winter Semester 2022-2023

Continuous Assessment Test – I

Programme Name & Branch	:	MCA
Course Name & code	:	ITA6007 & Network and Information Security
Class Number	:	VL2022230500249 & VL2022230500274
Slot	:	D2+TD2
Faculty Name (s)	:	Dr.C. NAVANEETHAN Dr.A. ANBARASA KUMAR

Exam Duration: 90 Min. **Maximum Marks: 50**

Q.No.	Question	Max Marks
1.	Identify the types of Security Attack occurred in the following scenarios a) Passive Attack (5 Marks) b) Active Attack (5 Marks)	10
2.	Classify the five categories of security services. a) Access Control b) Authentication c) Confidentiality d) Integrity e) Non repudation	10
3.	a) What is threat? And list out its various types. (5 Marks) b) State the difference between threats and attack. (5 Marks)	10
4.	a) With a neat block diagram, Explain the DES algorithm for 64 bit data and 64 bit key size. In DES algorithm we have **8 S boxes** Substitution boxes [S box]:. Input for S box is 48bit. and output from S box is 32 bit. The input 48 bit will be divided equally to 8 s boxes from s1, s2, … s8. So each s box will get 48/8= 6 bits as input. This Each S box reduce 6 bits to 4 bits. i.e input for each S box is 6 bits and output is 4 bits. How the 6 bits is reduce to 4 bits? Let you consider 6 bits 1 0 0 1 1 0. Find the position of 2nd row in 3rd column for S1. (5 Marks)	10

S1

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

	b) Explain Public Key Cryptography and when is it preferred. (5 Marks)	
5.	With a neat block diagram, Explain in detail the key generation, Input Array, State Array and Output Array in AES Algorithm and its expansion format.	10

VIT
Vellore Institute of Technology

School of Information Technology and Engineering
Winter Semester 2022-2023

Continuous Assessment Test – II

Programme Name & Branch	:	MCA
Course Name & code	:	ITA6007 & Network and Information Security
Class Number	:	VL2022230500249 & VL2022230500274
Slot	:	D2+TD2
Faculty Name (s)	:	Dr.C. NAVANEETHAN Dr.A. ANBARASA KUMAR

Exam Duration: 90 Min. **Maximum Marks: 50**

Q.No.	Question	Max Marks
1.	Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7. a) If user A has private key of 5, evaluate is A's public key Y_A? b) If user B has private key of 12, estimate B's public key Y_B? c) What is the shared secret key?	10
2.	a) Find private key'd' for RSA algorithm where public key <e,n> is given by n = 11363 and e = 211. Factorize 'n' to find the random numbers 'p' and 'q'. (5 Marks) b) In RSA algorithm if p= 5, q = 11 and e =13 then what will be the value for d? (5 Marks) i. Calculate the value of n = p x q, where p and q are prime numbers ii. Calculate φ (n) = (p-1) x (q-1) iii. Consider d as public key such that φ (n) and d has no common factors iv. Consider e as private key such that (e x d) mod φ (n) = 1 v. Cipher text c = message i.e. m^d mod n vi. Message m = cipher text i.e. c^e mod n	10
3.	Evaluate and verify the signature using Digital signature algorithm for the following inputs. p = 11, q = 5, w = 20, h = 2, x = 3, k = 3	10
4.	Explain the password controls in place for Banking Transaction Management and access to critical applications. Examine the factors influencing the transaction failures and the approach to enhance the success rate of transaction by reducing the illegal activities carried out during the transaction management.	10
5.	Consider the threat of "theft/breach of proprietary or confidential information held in key data files on the system." One method by which such a breach might occur is the accidental/deliberate e-mailing of information to a user outside to the organization. A possible countermeasure to this is to require all external e-mail to be given a sensitivity tag in its subject and for external email to have the lowest sensitivity tag. Identify the components and architecture that would be need to do this?	10

VIT
Vellore Institute of Technology

Final Assessment Test – June 2023

Course: ITA6007 - Network and Information Security
Class NBR(s): 0249 / 0274 Slot: D2+TD2
Time: Three Hours Max. Marks: 100
Faculty Name : Prof. ANBARASA KUMAR A / Prof. NAVANEETHAN C

KEEPING MOBILE PHONE/SMART WATCH, EVEN IN "OFF"POSITION IS TREATED AS EXAM MALPRACTICE

Answer ALL Questions
(10 X 10 = 100 Marks)

1. a) Suppose you have a file that contains sensitive information that only certain users should be able to access. How can you ensure that unauthorized users while still maintaining its confidentiality do not maliciously alter the file? Discuss the relevant concepts for the situation in detail. [5]

   b) Explain about active attacks and passive attacks in detail. [5]

2. a) State the difference between Denial of Service (DoS) and Distributed Denial of Service (DDoS). [5]

   b) An attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it. Explain the various types of DoS attacks and Organizations how can implement several measures to prevent from DoS attacks. [5]

3. a) Illustrate the following access control structures: [5]
   Role Based Access control with its benefits and example.

   b) An ABC Organization wants to restrict access to a particular file containing sensitive information, and the grant or restrict object access via an access policy determined by an object's owner group and/or subjects. Illustrate this situation with the features available in Discretionary Access Control mechanism. [5]

4. Explain why identity access management is important, as safety threats rise and users need to be protect. There are several kinds of password controls in place for banking transaction management and access to critical applications. Some of these controls include implementing strict controls for system-level and shared service account passwords, using one-time passwords (OTP) sent to the user's phone after successfully authenticating using a username and password. It helps ensure that only authorized users have access to specific resources or data. Justify the answer for the same.

5. a) Explain Data Encryption Standard (DES) in detail. How is Substitution operation handle in DES algorithm? Explain the concept in detail for the input 0 1 1 0 1 0 with the help of S1 Box given below. [5]

S1															
12	3	11	1	2	17	11	8	3	10	6	12	5	9	0	4
2	15	0	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	19	8	13	6	2	11	15	12	9	7	3	10	5	5
13	12	6	2	4	9	1	7	5	11	3	14	10	0	6	11

b) Describe the RSA algorithm and express the steps involved in the key generation. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and M=8. [5]

i) Calculate the value of n = p x q, where p and q are prime numbers
ii) Calculate ϕ (n) = (p-1) x (q-1)
iii) Consider d as public key such that ϕ (n) and d has no common factors
iv) Consider e as private key such that (e x d) mod ϕ (n) = 1
v) Cipher text c = message i.e. m^d mod n
vi) Message m = cipher text i.e. c^e mod n

6. The cyber-criminal emailing you while pretending to be your relative. In the email, they may try to get you to divulge personal information such as your address, birthday, login credentials, or more. Identify the attack with your answer in detail for given scenario.

7. The attacks such as 'Browser Attack' and 'Man-in-the-Middle Attack' disturbs the web security. Discuss how the efficiency of SSL features would counter all these attacks, in detail.

8. Intrusion Detection and Prevention (IDP) systems used to identify potential incidents, log information about them, attempt to prevent them and alert the administrators responsible for security. IDP systems use numerous incident detection techniques. Summarize the three primary classes of detection methodologies are signature-based, anomaly-based and stateful protocol analysis in detail.

9. In an Organization, Security departments must actively monitor networks to prevent from malware before it can cause extensive damage. Therefore, here prevention of malware and understanding what kind of malware attack is very critical. Discuss your answer with possible malware attacks that are applicable to above scenario.

10. As many organizations are adopting cloud computing, attackers exploit the cloud to obtain unauthorized control on the valuable data stored in it. Evolution of traditional computing to cloud has led to many security challenges for both customers and service providers. Discuss about different types of services are providing by trusted cloud providers over the Internet by using many technologies, which arises different security threats. Explain about cloud security issues, threats and related attacks in detail.

⇔⇔⇔