Roll No. □□□□□□□□

B.E (FT) END SEMESTER EXAMINATIONS – APR /MAY 2024

Computer Science and Engineering
VI SEMESTER
CS6007 INFORMATION SECURITY
(Regulation 2018 - RUSA)

Time: 3 Hours   Answer ALL Questions   Max. Marks 100

PART-A (10 x 2 = 20 Marks)

1. "Information we receive involves transforming from one format to other" State how a person receive information?
2. Tabulate the difference between phishing and pharming. (Any Two)
3. A program you have downloaded as a free trial might stop working after 15 days, because you were told that when you downloaded it. Do you consider this as logic bomb? Are logic bombs always malicious? Comment.
4. Clarke Wilson Security model is considered to be highly secured model. State the 3 integrity goals associated with.
5. What are the five types of risk involved in software project management.
6. Comment: Zero-Day Exploit.
7. Write a short note on Multi-Factor OTP Authenticators.
8. What are the prime objectives of modern cryptography?
9. What are considered to be constraints while designing an application with biometric security.
10. List down the four types of SSL certificate.

PART – B (8 x 8 = 64 marks)

(Answer any 8 questions)

11. List down the steps performed at each step of software development process. Explain each step in detail how risk is managed in the SDLC conceptual model.

12. Tabulate the security and information model focusing on the key features, access control, kind of organization / domain which suits the model with its limitation.

13 The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted. List the top 10 (2021) security risk. Explain any one of the security risk attack with its overview, description about the attack with example of the attack scenario.

14. Formulate in detail about the importance of Physical Security.

15. With neat illustration explain Advanced Encryption Standard algorithm (AES).

16. Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2.

    a) If user "A" has public key YA=9, what is A"s private key XA.

    b) If user "B" has public key YB=3, what is shared secret key K.

17. Explain RSA algorithm. Using RSA algorithm perform encryption and decryption using p=17, q=11, e=7 and M=88.

18. What is Kerberos? Explain how it provides authenticated service

19. Perform encryption and decryption using RSA Alg. for the following. P=17; q=11; e=7; M=88. Discuss the basic idea behind the RSA algorithm.

20. Explain the 4 phases of security certification and accreditation process with a neat diagram.

21. Consider any threat model (Stride / PASTA / Trike / Vast / attack tree / Octave /Dread / QTTM / CVSS etc.). Identify and classify threats in a tabular format with the name of the threat and the property violated with its definition. Explain with an example with a data flow diagram (DFD) considering its strengths and weakness.

22. What is SSL session? Can a session be shared among multiple connections? What are the parameters that define a session state?

PART – C (2 x 8 = 16 marks)

23. Alice used an alphabet with 30 characters from A to Z and 0, 1, <,>, <!>. Each of the letters is encoded as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z	0	1	,	!
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

The plaintext is divided into consequent subwords of length 4 that are encrypted independently via the same encryption (2 × 2)-matrix F with elements from Z30. For example, let the j-th subword be WORD and the encryption matrix F be equal to

$$F = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix}.$$

The matrix that corresponds to WORD is denoted by Pj and the matrix that corresponds to the result of the encryption of WORD is Cj and calculated as follows:

$$C_j = F \cdot P_j = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix} \cdot \begin{pmatrix} 22 & 17 \\ 14 & 3 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ 22 & 7 \end{pmatrix} \pmod{30}.$$

that is the j-th subword of the ciphertext is IWEH.

Eve has intercepted a cipher text that was transmitted from Alice to Bob:

CYPHXWQE!WNKHZ0Z

Also, she knows that the third subword of the plaintext is FORW. Will Eve be able to restore the original message? Find the plain text.

24 What are the characteristics of an ideal biometric? Brief the errors in biometrics

I. Fraud rate

II. Insult rate

III. Equal error rate