CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY

CRYPTOGRAPHY and NETWORK SECURITY [IT348]

Marks: 70 **Duration: 225 mins.**

A

Answer all the questions.

1 Find the multiplicative inverse of 23 in Z100. (2)

87 | 24 | 77 | Not Possible

2 A _____ takes place when one entity pretends to be a different entity. This attack usually includes one of the other forms of _____attack. (2)

Masquerade & Passive | DoS & Active | Masquerade & Active | Modification of messages & Passive

3 Calculate 11^110 mod 570= _____ (1)

121 | 120 | 122 | 119

4 Phi ϕ(187) = _____ (1)

160 | 158 | 186 | 159

5 Which of the following components of AES is self-invertible? (1)

AddRoundKey | SubByte | MixColumns | ShiftRows

6 Which of the following is/are desired properties of Block Cipher? (1)

Completeness & Avalanche Effect | Completeness only | Avalanche Effect only | None of the above

7 Use the Vigenere cipher with the keyword "HEALTH" to encipher the message "Life is full of surprises". (5)

SMFPBZMYLWHMZYPPKPZISMFPBZNYLWHMZYPPKPZISMFPBZMYLWHMZYPPKPYISMFPBZMYLWHMZYPPKPZJ | None of Above

8 The number of rounds in RC5 can range from 0 to _____ (1)

255 | 128 | 64 | 256

9 You receive an email with the following text message. "Microsoft and HP today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there is a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer. Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible." You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected. You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service". What category of virus is this? (2)

Virus Hoax | Spooky Virus | Stealth Virus | Polymorphic Virus

10 Which of the following is /are true for Virus?(i) The boot sector virus, the executable file infectors and the data file infectors are also called nano virus.(ii) Encryption , Oligomorphic, Polymorphic and Metamorphism are the types of virus based on concealment strategy. (2)

only (ii) is true | only (i) is true | Both are true | Both are false

11 Attacking well-known system defaults is one of the most common hacker attacks. Most software is shipped with a default configuration that makes it easy to install and setup the application. You should change the default settings to secure the system. Which of the following is NOT an example of default installation? (2)

Enabling firewall and antivirus software on the local system. | Many software packages come with "samples" that can be exploited, such as the sample programs on IIS web services. | Often, the default location of installation files can be exploited which allows a hacker to retrieve a file from the system. | Many systems come with default user accounts with well-known passwords that administrators forget to change.

12 Which of the following Intrusion detection techniques is based on comparing patterns to signify a known threat against the events that are observed? (1)

Signature Based Detection | Anomaly based detection | Stateful protocol analysis | None of the above

13 | Alice and Bob use Diffie hellman key exchange protocol to agree upon a shared secret key. They agree to use prime p=197 and a possible generator may be either 3 or 9. If Alice chooses her secret exponent as 98 and Bob chooses his secret exponent as 99, what are the numbers exchanged between Alice, Bob, and the final secret common key? (2)

1, 9, 1 | 196, 194, 196 | 194, 196, 217 | 1, 9, 196

14 | Bob chooses 17 and 11 as p and q. The value of e= 13 finds the value of d. (2)

37 | 38 | 40 | 31

15 | In diffie-hellman key exchange protocol, if two parties are not authenticated to each other then_____ can harm the security of the protocol. (1)

Man in the front attack | Ciphertext attack | Plaintext attack | Man in the middle attack

16 | Input size block size of MD4 and MD5 is of _____ bits. (1)

512 | 128 | 160 | 256

17 | Message Authentication code _____. (1)

generates a small block of data | generates a large block of data | does not generate data | is used for confidentiality

18 | To authenticate the data origin one needs_____. (1)

Message Detection code (MDC) | Message Authentication code (MAC) | Cipher text | Plain text

19 | Authentication means_____. (1)

verification of user's identification | verification of the data | All of above | None of above

20 | Digest created by a hash function is normally called a_____. (1)

Modification detection code | Modify authentication connection | Message authentication control | Message authentication cipher

21 | PGP offers _____ block ciphers for message encryption. (1)

AES | IDEA | CAST-128 | All of the above

22 | Outline the properties of Open PGP encryption standard. (1)

Modify email contents | Store sensitive information | Forward insensitive information | Transmit information across secure networks.

23 | _____is a popular session key creator protocol that requires an authentication server and a ticket-granting server. (1)

KDC | Kerberos | CA | None

24 | The cryptography algorithm/s used in S/MIME is/are_____. (1)

IDEA | CAST -128 | RSA, DES-3 | RC5

25 | For SSL connection, SSL Record protocol provides (1)

Confidentiality | Message integrity | Both | None of above

26 | A _____ provides privacy for LANs that must communicate through the global Internet. (1)

VPP | VNP | VNN | VPN

27 | _____ provides security at the transport layer. (1)

SSL | TLS | Both | None of the above

28 | SSL provides _____ (1)

Message integrity | Confidentiality | Compression | All of above

29			_____ operates in the transport mode or the tunnel mode. IPsec SSL PGP None of above	(1)

B

Answer all the questions.

30			Explain TRNG, PRNG and PRF in detail.	(5)
31			Calculate Mix column example of AES for the given data. $\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} ?? \\ 66 \\ 81 \\ e5 \end{bmatrix}$	(5)
32			Perform cryptanalysis on the given cipher text using column transposition. "ENMUODRASOWRFURTSHEOORUKBYWAMROCKYTA"	(5)
33			Consider an affine cipher (mod 26). Do a chosen plaintext attack using "HAHAHA". The ciphertext is "NONONO". Determine the encryption function.	(5)
34			Write a short on the firewall.	(5)
35			Write a short note on X.509 certificate revocation format.	(5)
[OR] 36			Explain preimage resistance, second preimage resistance and collision resistance in detail.	(5)

-----End-----