Total No. of Questions: 6 *Total No. of Printed Pages:2*

Enrollment No......................................

MEDI-CAPS UNIVERSITY Knowledge is Power

Faculty of Engineering / Science
End Sem Examination May-2024
OE00073 Cyber Security Fundamentals

Programme: B.Tech./ B.Sc. Branch/Specialisation: All

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Caesar cipher is an example of- **1**
(a) Poly-alphabetic cipher (b) Mono-alphabetic cipher
(c) Multi-alphabetic cipher (d) Bi-alphabetic cipher

ii. What is the meaning of cipher in computer terminology? **1**
(a) An algorithm that performs encryption
(b) An algorithm that generates a secret code
(c) An algorithm that performs encryption or decryption
(d) A secret code

iii. In public key cryptosystem _____ keys are used for encryption and decryption. **1**
(a) Same (b) Different
(c) Encryption keys (d) None of these

iv. Which of the following algorithm is not used asymmetric key cryptography? **1**
(a) RSA (b) DSA
(c) Electronic code book algo (d) None of these

v. Which of the below does not constitute a cybercrime? **1**
(a) Refusal of service (b) Man in the middle
(c) Phishing (d) AES

vi. An act to injure, corrupt, or threaten a system or network is characterised as which of the below? **1**
(a) Digital crime (b) Threats
(c) System hijacking (d) Cyber Attack

vii. ______ gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs & infrared to affect mobile phones. **1**
(a) Worms (b) Antivirus (c) Malware (d) Multimedia files

P.T.O.

viii. Which of the following is not a security issue for PDAs? **1**
(a) Password theft (b) Data theft
(c) Reverse engineering (d) Wireless vulnerability

ix. What is the full form of ITA-2000? **1**
(a) Information Tech Act -2000
(b) Indian Technology Act -2000
(c) International Technology Act -2000
(d) Information Technology Act -2000

x. A digital signature is mathematical technique which validates? **1**
(a) Authenticity (b) Integrity
(c) Non-repudiation (d) All of these

Q.2 i. Explain steganography technique. **2**
ii. Draw and explain symmetric encryption model. **3**
iii. Key="hello" and plaintext="university" then write playfair matrix(table) and Encrypt message using playfair cipher. **5**
OR iv. Briefly introduce the different modes of operation in DES. **5**

Q.3 i. Write down application of hash function. **2**
ii. What is the difference between public key and private key cryptosystem? **3**
iii. Perform encryption and decryption using RSA algorithm for the following: P=7; q=11; e=17; M=8. **5**
OR iv. User A & B exchange the key using Diffie Hellman alg. Assume á=5 q=11 XA=2 XB=3. Find YA, YB, K. **5**

Q.4 i. Differentiate threat and attack. **2**
ii. Differentiate passive attack from active attack with example. **3**
iii. Classify cybercrimes. Explain with examples. **5**
OR iv. How the criminals plan the attacks? Explain with small example. **5**

Q.5 i. Explain proliferation of mobile and wireless devices. **4**
ii. Discuss about credit card frauds in mobile and wireless computing era. **6**
OR iii. Discuss different registry settings for mobile devices. **6**

Q.6 Attempt any two:
i. Why do we need cyber laws? Explain. **5**
ii. Discuss about digital signatures in cyber security. **5**
iii. Write about forensic investigations. **5**

******

Scheme of Marking
Cyber Security Fundamentals-OE00073

Q.1 i) Caesar Cipher is an example of **1**
b) Mono-alphabetic Cipher

ii) What is the meaning of cipher in computer terminology? **1**
c) an algorithm that performs encryption or decryption

iii) In public key cryptosystem _____ keys are used for encryption and decryption. **1**
b) Different

iv) A cryptographic hash function has variable output length. **1**
a) Electronic Code Book Algo

v) Which of the below does not constitute a cybercrime? **1**
d) AES

vi) An act to injure, corrupt, or threaten a system or network is characterised as which of the below? **1**
d) Cyber Attack

vii) ____________ gets propagated through networks and technologies like SMS, Bluetooth, wireless medium, USBs and infrared to affect mobile phones. **1**
c) Malware

viii) Which of the following is not a security issue for PDAs? **1**
c) Reverse engineering

ix) What is the full form of ITA-2000? **1**
d) Information Technology Act -2000

x) A digital signature is mathematical technique which validates? **1**
d) All of the above

Q.2 i. Explain Steganography technique. **2**
ii. Draw and Explain Symmetric Encryption model. **2,1**
iii. key=h̄ello_ and plaintext=u̲niversity_ then write playfair matrix(table) and Encrypt message using playfair cipher. **2,3**
OR iv. Briefly introduce the different modes of operation in DES? **5**

Q.3 i. Write down application of Hash function. **2**
ii. What is the difference between public key and private key cryptosystem? **3**
iii. Perform encryption and decryption using RSA Alg. for the following: P=7; q=11; e=17; M=8. **5**
OR iv. User A & B exchange the key using Diffie Hellman alg. Assume á=5, q=11, XA=2, XB=3. Find YA, YB, K. **5**

Q.4 i. Differentiate threat and attack. **2**
ii. Differentiate passive attack from active attack with example. **3**
iii. Classify Cybercrimes? Explain with examples? **3,2**
OR iv. How the Criminals Plan the Attacks? Explain with small example? **3,2**

Q.5 i. Explain Proliferation of Mobile and Wireless Devices. **2,2**
ii. Discuss about Credit card frauds in Mobile and Wireless Computing era? **6**
OR iii. Discuss different Registry Settings for Mobile Devices **6**

Q.6 Attempt any two:
i. Why do we need cyber laws? Explain? **5**
ii. Discuss about digital signatures in Cyber security. **5**
iii. Write about Forensics Investigations. **5**

Q.3. (iv) $a = 5$, $q = 11$, $X_A = 2$, $X_B = 3$

$Y_A = ?$ $Y_B = ?$ $K = ?$

→ user A's public key Y_A

$Y_A = a^{X_A} \bmod q$

$Y_A = 5^2 \bmod 11 \Rightarrow 25 \bmod 11$

~~Y~~

→ B's public key Y_B

$Y_B = a^{X_B} \bmod q$

$= 5^3 \bmod 11 = 125 \bmod 11$

1) For user ~~A =)~~ ~~$K = Y_A \wedge \{X_B\}$~~
A & B ↓

$$\begin{cases} K_A = Y_B^{X_A} \bmod q = 5 \\ K_B = Y_A^{X_B} \bmod q = 5 \end{cases}$$

Q.3. (iii) 1) $P=7$, $q=11$, $e=17$, $M=8$

↳ $N = P \times Q = 77$

2) $\phi(N) = (P-1) \times (Q-1) = 6 \times 10 = 60$

3) Choose (E)

$\gcd(17, 60) = 1$

4) calculate (D)

$D \times E = 1 \pmod{\phi(N)}$

$17D = 1 \pmod{60}$

$D = 53$

5) ENcryption publickey (E, N)

$C = M^E \pmod{N} \Rightarrow C \Rightarrow 8^{17} \pmod{77}$

~~Calculate C = C = N~~

~~8^{17} mod 77~~

Calculate $\boxed{C = 51}$ Ans cipher text

6) Decryption (D, N) Private key

$M = C^D \pmod{N} \Rightarrow M = 51^{53} \pmod{77}$

calculate M

$\boxed{M = 8}$ Decrypted msg = 8 Ans.