T. T. es Gem-V Nov-2022 Regular. S.T. Q. A paper Not Available

Paper / Subject Code: 82904 / Information & Network Security

| N.B. 1) All questions are compulsory. 2) Figures to the right indicate marks. 3) Illustrations, in-depth answers and diagrams will be appred 4) Mixing of sub-questions is not allowed. Q. 1 Attempt All(Each of 1 Marks) (a) Multiple Choice Question i) Which of the following is not an example of a substitute a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher A deliberate attempt to evade security services is called a) threat b) attack | (15M |
|---|---------------------------------|
| 2) Figures to the right indicate marks. 3) Illustrations, in-depth answers and diagrams will be appred 4) Mixing of sub-questions is not allowed. Q. 1 Attempt All(Each of 1 Marks) (a) Multiple Choice Question i) Which of the following is not an example of a substitute a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher c) Rail Fence cipher d) Hill cipher d) A deliberate attempt to evade security services is called a) threat b) attack | (15M |
| 3) Illustrations, in-depth answers and diagrams will be appred 4) Mixing of sub-questions is not allowed. Q. 1 Attempt All(Each of 1 Marks) (a) Multiple Choice Question i) Which of the following is not an example of a substitute a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | (15M |
| 4) Mixing of sub-questions is not allowed. Q. 1 Attempt All(Each of 1 Marks) (a) Multiple Choice Question i) Which of the following is not an example of a substitute a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher i) A deliberate attempt to evade security services is called a) threat b) attack | (15M |
| Q. 1 Attempt All(Each of 1 Marks) (a) Multiple Choice Question i) Which of the following is not an example of a substitute a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | ntion cipher? |
| (a) Multiple Choice Question i) Which of the following is not an example of a substitution a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | ntion cipher? |
| (a) Multiple Choice Question i) Which of the following is not an example of a substitution a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | ntion cipher? |
| i) Which of the following is not an example of a substitution a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | |
| a) Caesar cipher b) Playfair cipher c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | |
| c) Rail Fence cipher d) Hill cipher ii) A deliberate attempt to evade security services is called a) threat b) attack | er |
| ii) A deliberate attempt to evade security services is called a) threat b) attack | |
| a) threat b) attack | |
| | |
| | |
| c) masquerade d) repudiation. | |
| iii) Which security protocol is used at the transport Layer? a) IPSec b) PGP | |
| c) SMIME d) SSL | |
| iv) A digital signature needs a(n) system. | |
| a) symmetric-key b) asymmetric-k | cey |
| c) private key d) session key | |
| v) Which of the following is a means to access a computer | program or entire computer |
| system bypassing all security mechanisms? | |
| a) Backdoor b) Masquerading | |
| c) Phishing d) Trojan Horse. | |
| vi) Passive attacks do not include | |
| a) modification of data stream b) obtaining the | |
| transmitted c) eavesdropping on transmission | d) the possibility of replay |
| attack in future. | |
| vii) Public - key encryption is also known as a) asymmetric encryption b) symmetric E | Engration |
| | |
| c) single encryption c) super encryption viii) PKI stands for . | ption |
| a) Parent Key Interface b) Public Key | Infrastructure |
| c) Protocol Key Infrastructure c) Private Key | |
| ix) AES has different configurations. | mirastractare |
| a) one b) three | |
| c) four c) five | |
| | e algorithm |
| | algorithm. |
| | |
| c) RSA d) RAA | • |
| | |
| (b) Fill in the blanks | |
| (hashing,64, 128, shared secret,steganography,cryptanalys | |
| i) ciphers hide the message by rearranging the | e letter order without altering |
| the actual letters used. | |
| ii) SHA is aalgorithm. | |

Paper / Subject Code: 82904 / Information & Network Security

| iii) | is an alternative to encryption which hides the very existence of a message | |
|------|--|---------|
| | by some means. | |
| iv) | DES is a non-Feistel cipher that encrypts and decrypts a data block of bits. | |
| v) | Private key cryptography uses a | |
| | ALL CHARLES (A THIREE)/E I COM IN | (1500) |
| Q. 2 | Attempt the following (Any THREE)(Each of 5Marks) | (15M) |
| (a) | What is the CIA triad? Explain in detail. | |
| (b) | Explain symmetric cipher model. Discuss different techniques used in traditional ciphers. | |
| (c) | Explain DES cipher in detail. Explain ECB block cipher mode of operation with its advantages and limitations. | |
| (d) | Explain the differences between symmetric and asymmetric cryptography. | |
| (e) | | |
| (f) | Discuss different categories of security services as per X-800 recommendations. | |
| Q. 3 | Attempt the following (Any THREE) (Each of 5Marks) | (15M) |
| (a) | Explain key generation process in Diffie-Hellman key exchange algorithm. | |
| (b) | Discuss different approaches of distribution of public key in public key cryptography. | |
| (c) | What is Message authentication? Discuss different approaches that can be used to achieve message authentication. | |
| (d) | Explain various characteristics of Hash function. | |
| (e) | Explain SHA algorithm. | |
| (f) | Explain basic digital signature model. What security requirements do you feel | |
| | can be achieved in digital communication by using digital signature? | |
| Q. 4 | Attempt the following (Any THREE) (Each of 5Marks) | (15M) |
| (a) | Discuss any one protocol which is used to add security in email applications. | (10111) |
| (b) | What is SSL? Discuss its protocol stack. | |
| (c) | What is a honeypot? How does it facilitate intrusion detection? | |
| (d) | What do you understand about malware? Explain any two types of malicious program. | |
| (e) | Discuss the significance and limitations of firewalls. | |
| (f) | What is the SET protocol? What business requirement does it fulfil? | |
| Q. 5 | Attempt the following (Any THREE) (Each of 5Marks) | (15M) |
| (a) | What is asymmetric key cryptography? Discuss its various applications. | (15111) |
| (b) | Explain rail fence cipher with proper example. | |
| (c) | Briefly explain Man in middle attack. | |
| (d) | What is kerberos? Explain its different components. | |
| (e) | Explain the key elements of public key infrastructure. | |
| (f) | Discuss IPSec protocol with its different modes of operation. | |
| (g) | What do you understand about security attacks? Discuss different types of attacks. | |
| (h) | Explain the process of encryption and decryption using caesar cipher for plaintext "attack at dawn". | |
| | | |