# University of Mumbai

Program: **Department of Information Technology**

Curriculum Scheme: Rev 2019

Examination: TE Semester: V

Course Code: ITC502 and Course Name: Computer Network Security

| **Q1.** | **Choose the correct option for following questions. All the Questions are compulsory and carry equal marks** |
|---|---|
| 1. | A firewall is a network security system ______based that controls incoming and outgoing network traffic based on a set of rules: |
| Option A: | Hardware |
| Option B: | Software |
| Option C: | Both hardware or software |
| Option D: | None of These |
| | |
| 2. | IPSec defines two protocols: _______ and ________. |
| Option A: | AH; SSL |
| Option B: | AH; ESP |
| Option C: | PGP; ESP |
| Option D: | PGP; SSL |
| | |
| 3. | A method for determining a solution to a problem by sequentially testing all possible solutions. |
| Option A: | brute force |
| Option B: | relative frequency |
| Option C: | cipher |
| Option D: | paired keys |
| | |
| 4. | Which is the principle of the encryption using a key? |
| Option A: | The key indicates which funcion is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown. |
| Option B: | The key contains the secret function for encryption including parameters. Only a password can activate the key. |
| Option C: | All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption. |
| Option D: | The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption. |
| | |
| 5. | In the DES algorithm the round key is __________ bit and the Round Input is ____________bits. |
| Option A: | 48, 32 |
| Option B: | 64,32 |
| Option C: | 56, 24 |
| Option D: | 32, 32 |
| | |
| 6. | In AES the 4×4 bytes matrix key is transformed into a keys of size __________ |
| Option A: | 32 words |

| | |
|---|---|
| Option B: | 64 words |
| Option C: | 64 words |
| Option D: | 44 words |
| | |
| 7. | What is the maximum length of the message (in bits) that can be taken by SHA-512? |
| Option A: | 2^64 |
| Option B: | 2^256 |
| Option C: | 2^192 |
| Option D: | 2^128 |
| | |
| 8. | SSL provides __________. |
| Option A: | message integrity |
| Option B: | confidentiality |
| Option C: | compression |
| Option D: | All the above |
| | |
| 9. | What is a Denial of Service (DoS) attack? |
| Option A: | A tool that prevents hackers from using network services. |
| Option B: | Any attack that intends to prevent users from using digital resources. |
| Option C: | A type of network attack that allows a hacker to remotely power down a computer. |
| Option D: | A computer used to attack hackers. |
| | |
| 10. | A Digital Signature is |
| Option A: | a bit string giving identity of the correspondent |
| Option B: | an authentication of an electronic record by tying it uniquely to a key only a sender knows |
| Option C: | a unique identification of the sender |
| Option D: | an encrypted signature of the sender |

| **Q2.** | **Solve any Four out of Six** **5 marks each** |
|---|---|
| A | *What is significance of digital signature on a certificate? Justify.* |
| B | *Write short note on Email Security.* |
| C | *Write short note on Honeypots.* |
| D | *Explain Play Cipher with the help of example.* |
| E | *Compare between steganography and cryptography.* |
| F | *What is asymmetric key cryptography? Discuss RSA Algorithm.* |

| **Q3.** | **Solve any Two Questions out of Three** **10 marks each** |
|---|---|
| A | *What are block cipher modes? Explain in detail.* |
| B | *Explain Kerberos Protocol in detail.* |
| C | *Perform encryption and decryption using RSA algorithm with* $p = 7$, $q = 11$, $e = 17$ *and* $M = 8$. *Explain each step in detail.* |

| **Q4.** | ***Please delete the instruction shown in front of every sub question*** |
|---|---|
| A | **Solve any Two** **5 marks each** |
| i. | *Compare SNMPv1, SNMPv2 and SNMPv3.* |
| ii. | *Describe Dos and DDoS attack in detail.* |
| iii. | Explain steps to implement NAC solution. |
| B | **Solve any One** **10 marks each** |
| i. | *Why there is a need of firewall? Explain different types in detail and the limitations of firewall.* |
| ii. | *Compare and contrast AES and DES.* |