Program: BE Computer Engineering

Curriculum Scheme: Revised 2012

Examination: Final Year Semester VII

Course Code: CPC702 and Course Name: Cryptography and System Security

Time: 1hour Max. Marks: 50

==============================================================================

Note to the students:- All the Questions are compulsory and carry equal marks .

|  |  |
| --- | --- |
| Q1.  | According to the CIA Triad, which of the below-mentioned element is not considered in the triad? |
| Option A: | Confidentiality |
| Option B: | Integrity |
| Option C: | Authenticity |
| Option D:  | Availability |
|  |  |
| Q2. | A sender must not be able to deny sending a message that he or she, in fact, did send, is known as |
| Option A: | Message Nonrepudiation. |
| Option B: | Message Integrity. |
| Option C: | Message Confidentiality. |
| Option D: | Message Sending |
|  |  |
| Q3. | Which following security attack is threat to integrity  |
| Option A: | Snooping |
| Option B: | Masquerading |
| Option C: | Denial of service |
| Option D: | Traffic analysis |
|  |  |
| Q4. | 1. A cipher that scrambles letters into different positions is referred to as what?
 |
| Option A: | Substitution |
| Option B: | Stream |
| Option C: | Running key |
| Option D: | Transposition |
|  |  |
| Q5. | RC5 is a type of  |
| Option A: | Block cipher |
| Option B: | Plain cipher |
| Option C: | Stream cipher |
| Option D:  | Caesar cipher |
|  |  |
| Q6. | \_\_\_\_\_\_\_ is based on the idea of hiding the relationship between the cipher text and the Key  |
| Option A: | Confusion |
| Option B: | Diffusion |
| Option C: | stream cipher |
| Option D:  | block cipher |
|  |  |
| Q7.  | What encryption operation is used when AES uses S-boxes during the process of encryption?  |
| Option A: |  Chaining |
| Option B: |  Key generation  |
| Option C: |  Key exchange  |
| Option D:  |  Substitution |
|  |  |
| Q8.  | What characteristic of Digital Encryption Standard (DES) used in Electronic Code Book (ECB) mode makes it unsuitable for long messages?  |
| Option A: |  Block fragmentation causes message cipher instability.  |
| Option B: |  Weak keys will produce symmetrical message holes.  |
| Option C: |  Repeated message blocks produce repeated cipher text blocks |
| Option D:  |  Each message block produces a single cipher text block. |
|  |  |
| Q9. | The blowfish algorithm’s key expansion converts a key of at most 448 bits into several subkey arrays totaling \_\_\_\_\_\_\_\_\_\_\_ bytes.  |
| Option A: | 4096 |
| Option B: | 4608 |
| Option C: | 4168 |
| Option D:  | 4864 |
|  |  |
| Q10.  | 1. The Diffie-Hellman algorithm is primarily used to provide which of the following?
 |
| Option A: | Integrity |
| Option B: | Key exchange |
| Option C: | Confidentiality |
| Option D:  | Non-repudiation |
|  |  |
| Q11.  | 1. In RSA, Ф(n) = \_\_\_\_\_\_\_ in terms of p and q.
 |
| Option A: | (p)/(q) |
| Option B: | (p)(q) |
| Option C: | p+1)(q+1) |
| Option D:  | (p-1)(q-1) |
|  |  |
| Q12.  | 1. A hash function guarantees integrity of a message. It guarantees that message has not be
 |
| Option A: | Changed |
| Option B: | Replaced |
| Option C: | Over view |
| Option D: | Left |
|  |  |
| Q13. | 1. SHA-l has a message digest of
 |
| Option A: | 128 bits |
| Option B: | 255 bits |
| Option C: | 512 bits |
| Option D:  | 120 bits |
|  |  |
| Q14.  | 1. Digest created by a hash function is normally called a
 |
| Option A: | message authentication connection |
| Option B: | modification detection code (MDC). |
| Option C: | message authentication control. |
| Option D:  | message authentication cipher |
|  |  |
| Q15. | 1. \_\_\_\_\_\_\_\_\_\_ is a popular session key creator protocol that requires an authentication server and a ticket-granting server
 |
| Option A: | Authentication Header (AH) |
| Option B: | KDC |
| Option C: | Kerberos |
| Option D:  | CA |
|  |  |
| Q16.  | 1. Which is Internet Security Protocol?
 |
| Option A: | SSL |
| Option B: | Firewalls |
| Option C: | PGP |
| Option D:  | IDS |
|  |  |
| Q17. | 1. One of protocols to provide security at application layer is
 |
| Option A: | Pretty Good Privacy |
| Option B: | Handshake Protocol |
| Option C: | Alert Protocol |
| Option D: | Record Protocol |
|  |  |
| Q18. | What type of malware that is capable of infect a file with an encrypted copy of itself, then modify itself when decoded to make almost impossible to detect by signature-based virus scanner?  |
| Option A: | Computer worm |
| Option B: | Computer virus |
| Option C: | Trojan house |
| Option D:  | Polymorphic virus |
|  |  |
| Q19.  | What is one thing a Trojan does?  |
| Option A: | Logs your keystrokes |
| Option B: | Protects your computer from advertisements |
| Option C: | Causes your power supply to overheat |
| Option D:  | Improves virtual memory efficiency |
|  |  |
| Q20. | What is the basic need in protecting memory in multi-user environment? |
| Option A: | We need two registers one ‘start’ and other ‘end’ |
| Option B: | A fence register has to be used known as base register |
| Option C: | We need a variable register |
| Option D: | Users should be given just enough privileges to perform their tasks  |
|  |  |
| Q21. | \_\_\_\_\_\_\_ is responsible for using that the database remains in a consistent state despite system failure |
| Option A: | End user |
| Option B: | Transaction manager |
| Option C: | Sophisticated user |
| Option D:  | Storage manager |
|  |  |
| Q22.  | An analysis method used by some IDS that looks for instances that are not considered normal behavior. |
| Option A: | Stateful Inspection |
| Option B: | Pattern Matching |
| Option C: | Evasion |
| Option D:  | Anomaly Detection |
|  |  |
| Q23. | What is the payload length in Authentication header AH protocol? |
| Option A: | 4 bits |
| Option B: | 16 bits |
| Option C: | 8 bits |
| Option D:  | 32 bits |
|  |  |
| Q24.  | What is the role of internet key exchange (IKE) within the IPsec protocol?  |
| Option A: | Peer authentication and key exchange |
| Option B: | Enforcing quality of service |
| Option C: | Data signature |
| Option D:  | Data encryption |
|  |  |
| Q25. | **What is the purpose of a Denial of Service attack?** |
| Option A: | Exploit a weakness in the TCP/IP stack |
| Option B: | To overload a system so it is no longer operational |
| Option C: | To execute a Trojan on a system |
| Option D:  | To shutdown services by turning them off |