Sample Questions

Class & Sem: TE- VI Subject: CSS (Cryptography and System Security)

Multiple Choice Questions

|  |  |
| --- | --- |
|  | Choose the correct options for following questions. All the questions carry equal marks. |
|  | The assurance that a given entity is involved and currently active in a communication session is called as \_\_\_\_\_\_\_\_ |
| Option A. | Message authentication |
| Option B. | Entity Authentication |
| Option C. | Authentication |
| Option D. | All of the above |
|  |  |
|  | The Application Layer includes which protocol. |
| Option A. | ICMP |
| Option B. | UDP |
| Option C. | SMTP |
| Option D. | ARP |
|  |  |
|  | How many algorithms does digital signature consist of? |
| Option A. | 2 |
| Option B. | 3 |
| Option C. | 4 |
| Option D. | 5 |
|  |  |
|  | A cryptographic hash function is an equation used to verify the \_\_\_\_ of data. |
| Option A. | variety |
| Option B. | validity |
| Option C. | veracity |
| Option D. | None of the above. |
|  |  |
|  | The DES Algorithm Cipher System consists of \_\_\_\_\_\_\_\_\_\_\_\_rounds (iterations) each with a round key. |
| Option A. | 12 |
| Option B. | 18 |
| Option C. | 9 |
| Option D. | 16 |
|  |  |
|  | Which is not a component of Public key infrastructure(PKI)? |
| Option A. | Client |
| Option B. | CRL |
| Option C. | CA |
| Option D. | KDC |
|  |  |
|  | The method of converting plaintext into cipher text by using an algorithm and a key is called as \_\_\_\_\_\_\_\_ |
| Option A. | Eavesdropping |
| Option B. | Encryption |
| Option C. | Decryption |
| Option D. | Cryptography |
|  |  |
|  | The \_\_\_\_\_\_\_\_\_ cipher is a symmetric-key based encryption technique that uses digraph Substitution cipher. |
| Option A. | p[layfair |
| Option B. | Hill |
| Option C. | Vignere |
| Option D. | Keyed |
|  |  |
|  | In symmetric-key cryptography, the key locks and unlocks the box is |
| Option A. | same |
| Option B. | shared |
| Option C. | private |
| Option D. | public |
|  |  |
|  | An algorithm used in encryption is referred to as cipher. |
| Option A. | True |
| Option B. | False |
|  |  |
|  | A small program that changes the way a computer operates. |
| Option A. | worm |
| Option B. | trojan |
| Option C. | bomb |
| Option D. | virus |
|  |  |
|  | Which of the following is not a transport layer vulnerability? |
| Option A. | mishandling of undefined , poorly defined |
| Option B. | the vulnerability that allows fingerprinting & other enumeration of host information |
| Option C. | overloading of transporting layer mechanisms |
| Option D. | unauthorized network access |
|  | TCP/IP model does not have \_\_\_\_\_\_ layer but OSI model have this layer |
| Option A. | session layer |
| Option B. | transport layer |
| Option C. | application layer |
| Option D. | network layer |
|  |  |
|  | Which one is the strong attack mechanism? |
| Option A. | chosen plaintext attack |
| Option B. | chosen cipher text |
| Option C. | brute force attack |
| Option D. | man in the middle attack |
|  |  |
|  | Which layer filters the proxy firewall? |
| Option A. | application |
| Option B. | network |
| Option C. | transport |
| Option D. | none of the above |
|  |  |
|  | GCD(a,b) = GCD(b,a mod b) |
| Option A. | true |
| Option B. | false |
| Option C. | cannot be determined |
| Option D. | none |
|  |  |
|  | Does the set of residue classes (mod 3) form a group with respect to modular addition? |
| Option A. | yes |
| Option B. | no |
| Option C. | cant say |
| Option D. | insufficient data |
|  |  |
|  | Public key encryption is advantageous over Symmetric key Cryptography because of \_\_\_\_\_\_\_ |
| Option A. | speed |
| Option B. | space |
| Option C. | key exchange |
| Option D. | key length |
|  |  |
|  | Rail Fence Technique is an example of |
| Option A. | substitution |
| Option B. | transposition |
| Option C. | product cipher |
| Option D. | ceasar cipher |
|  |  |
|  | Which one of the following can be considered as the class of computer threats? |
| Option A. | DoS attack |
| Option B. | Phishing |
| Option C. | Soliciting |
| Option D. | Both A and C |
|  |  |
| 21. | Which of the following is considered as the unsolicited commercial email? |
| Option A. | Virus |
| Option B. | Malware |
| Option C. | Spam |
| Option D. | All of the above |
|  |  |
| 22. | It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the\_\_\_\_\_\_\_ |
| Option A. | Antivirus |
| Option B. | Firewall |
| Option C. | Cookies |
| Option D. | Malware |
|  |  |
| 23. | Which one of the following refers to the technique used for verifying the integrity of the message? |
| Option A. | Digital Signature |
| Option B. | Decryption Algorithm |
| Option C. | Protocol |
| Option D. | Message Digest |
|  |  |
| 24. | Which of the following is not a type of scanning? |
| Option A. | Xmas Tree Scan |
| Option B. | Cloud Scan |
| Option C. | Null Scan |
| Option D. | SYN Stealth |
|  |  |
| 25. | The field that covers a variety of computer networks, both public and private, that are used in everyday jobs. |
| Option A. | Artificial Intelligence |
| Option B. | ML |
| Option C. | Network Security |
| Option D. | IT |
|  |  |
| 26. | Which of these is a part of network identification? |
| Option A. | User ID |
| Option B. | Password |
| Option C. | OTP |
| Option D. | fingerprint |
|  |  |
| 27. | Secure Hash Algorithm -1 (SHA-1) has a message digest of |
| Option A. | 160 bits |
| Option B. | 512 bits |
| Option C. | 628 bits |
| Option D. | 820 bits |
|  |  |
| 28. | A hash function guarantees the integrity of a message. It guarantees that the message has not been\_\_\_\_\_ |
| Option A. | replaced |
| Option B. | over view |
| Option C. | changed |
| Option D. | violated |
|  |  |
| 29. | A Digital Signature is required: |
| Option A. | for non repudiation of communication by a sender |
| Option B. | for all email sending |
| Option C. | for all DHCP Server |
| Option D. | for FTP transactions |
|  |  |
| 30. | \_\_\_\_\_\_\_\_\_ uses pretty good privacy (PGP) algorithm. |
| Option A. | Electronic Mails |
| Option B. | File encryption |
| Option C. | Both Electronic Mails and File Encryption |
| Option D. | None of the above |
| 31. | What is the gcd value of the pair (88 and 220) using Euclid algorithm. |
| Option A: | 22 |
| Option B: | 44 |
| Option C: | 11 |
| Option D: | 88 |
|  |  |
| 32. | What is the gcd value of the pair (400 and 60) and the values of s and t using  extended Euclidean algorithm. |
| Option A: | gcd = 20, s = 1, t = -7 |
| Option B: | gcd = 20, s = -1, t = -7 |
| Option C: | gcd = 20, s = 1, t = 7 |
| Option D: | gcd = 20, s = -1, t = 7 |
|  |  |
| 33. | What is the ciphertext after encrypting the plaintext "secure" with key value = 15 by using additive cipher technique. |
| Option A: | htrgjt |
| Option B: | hsrgjs |
| Option C: | hsrjgs |
| Option D: | htrjgt |
|  |  |
| 34. | What is the ciphertext after encrypting the plaintext "he is attacking" by using  keyword 'program' in Vigenere cipher technique. |
| Option A: | wv wy rtfpytoeg |
| Option B: | xw xz sugquzpfh |
| Option C: | wv wy rtfptyoeg |
| Option D: | vw yw sugquxmfh |
|  |  |
| 35. | What is the ciphertext after encrypting the plaintext "programmer" with keyword "network" by using playfair cipher technique. |
| Option A: | LATIKBPYYKAU |
| Option B: | LATIKBPVVKAU |
| Option C: | LATIKBPXXKAU |
| Option D: | LATIKBPVVKBV |
|  |  |
| 36. | \_\_\_\_\_\_\_\_ defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. |
| Option A: | X.800 |
| Option B: | X.809 |
| Option C: | X.832 |
| Option D: | X.802 |
|  |  |
| 37. | \_\_\_\_\_\_\_\_\_\_\_\_are fundamental to a number of public-key algorithms, including and the digital signature algorithm (DSA). |
| Option A: | Discrete logarithms |
| Option B: | Chinese remainder theorem |
| Option C: | Fermat’s theorem |
| Option D: | Miller and Rabin algorithm |
|  |  |
| 38. | Plain text message is: "meet me after the toga party" with a rail fence of depth 2. Compute cipher text. |
| Option A: | MEMATRHTGPRYETEFETEOAAT |
| Option B: | MEMATRHTGPRYETEFETFOAAT |
| Option C: | MEMATRHTHPRYETEFETEOAAT |
| Option D: | MEMATRHTGPRYETEFFTEOAOT |
|  |  |
| 39. | In\_\_\_\_\_\_ mode, the same plaintext value will always result in the same cipher text value. |
| Option A: | Cipher Block Chaining |
| Option B: | Cipher Feedback |
| Option C: | Electronic code book |
| Option D: | Output Feedback |
|  |  |
| 40. | DES encrypting the plaintext as block of \_\_\_\_\_\_\_ bits. |
| Option A: | 64 |
| Option B: | 56 |
| Option C: | 128 |
| Option D: | 32 |
|  |  |
| **41.** | \_\_\_\_\_\_ is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. |
| Option A: | AES |
| Option B: | RSA |
| Option C: | MD5 |
| Option D: | RC5 |
|  |  |
| **42.** | The number of rounds in RC5 can range from 0 to \_ |
| Option A: | 127 |
| Option B: | 63 |
| Option C: | 31 |
| Option D: | 255 |
|  |  |
| **43.** | How many rounds does the AES-192 perform? |
| Option A: | 10 |
| Option B: | 14 |
| Option C: | 16 |
| Option D: | 12 |
|  |  |
| **44.** | For the Knapsack: {1 6 8 15 24}, Find the cipher text value for the plain text 10011. |
| Option A: | 40 |
| Option B: | 15 |
| Option C: | 14 |
| Option D: | 39 |
|  |  |
| **45.** | Which of the following is not possible through hash value? |
| Option A: | Password check |
| Option B: | Data integrity check |
| Option C: | Data retrieval |
| Option D: | Digital signature |
|  |  |
| **46.** | Which of the following is not an element/field of the X.509 certificates? |
| Option A: | Issuer Name |
| Option B: | Serial Modifier |
| Option C: | Issue unique identifier |
| Option D: | Signature |
|  |  |
| **47.** | \_\_\_\_\_\_\_ is responsible for distributing keys to pairs of users (hosts, processes, applications) as needed |
| Option A: | Key distribution center |
| Option B: | Key analysis center |
| Option C: | UKey storing center |
| Option D: | HKey storing center |
|  |  |
| **48.** | A digital certificate system is |
| Option A: | uses third-party CAs to validate a user's identity |
| Option B: | uses digital signatures to validate a user's identity |
| Option C: | uses tokens to validate a user's identity |
| Option D: | are used primarily by individuals for personal correspondence |
|  |  |
| **49.** | Hashed message is signed by a sender using |
| Option A: | His public key |
| Option B: | His private key |
| Option C: | Receivers public key |
| Option D: | Receivers private key |
|  |  |
| **50.** | The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not |
| Option A: | Authenticated |
| Option B: | Joined |
| Option C: | Submit |
| Option D: | Separate |
|  |  |
| 51. | \_\_\_\_\_\_\_\_\_ operates in the transport mode or the tunnel mode. |
| Option A: | IPSec |
| Option B: | SSL |
| Option C: | PGP |
| Option D: | BGP |
|  |  |
| 52. | When a hash function is used to provide message authentication, the hash function value is referred to as |
| Option A: | Message Field |
| Option B: | Message Digest |
| Option C: | Message Score |
| Option D: | Message Leap |
|  |  |
| 53. | What is honey pot attack? |
| Option A: | dummy device put into the network to attract attackers |
| Option B: | single line threat |
| Option C: | Ip spoofing bypass |
| Option D: | recognition attack |
|  |  |
| 54. | Which of the following tool would NOT be useful in figuring out what spyware or viruses could be installed on a client’s computer? |
| Option A: | Wireshark |
| Option B: | Malware Bytes |
| Option C: | HighjackThis |
| Option D: | HitmanPro |
|  |  |
| 55. | Which of the following does authorization aim to accomplish? |
| Option A: | Restrict what operations/data the user can access |
| Option B: | Determine if the user is an attacker |
| Option C: | Flag the user if he/she misbehaves |
| Option D: | Determine who the user is |
|  |  |
| 56. | A person who enjoys learning details about computers and how to enhance their capabilities. |
| Option A: | cracker |
| Option B: | hacker |
| Option C: | app controller |
| Option D: | site controller |
|  |  |
| 57. | Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis. |
| Option A: | random polyalphabetic , plaintext , playfair |
| Option B: | random polyalphabetic, playfair , vignere |
| Option C: | random polyalphabetic , vignere , playfair , plaintext |
| Option D: | random polyalphabetic , plaintext , beaufort , playfair |
|  |  |
| 58. | The process of writing the text as rows and read it as columns is known as |
| Option A: | vernam cipher |
| Option B: | ceaser cipher |
| Option C: | transposition columnar cipher |
| Option D: | homophonic substitution cipher |
|  |  |
| 59. | What is the port number for HTTPS (HTTP Secure)? |
| Option A: | 43 |
| Option B: | 443 |
| Option C: | 445 |
| Option D: | 444 |
|  |  |
| 60. | The certificate message is required for any agreed key exchange method, except\_\_\_\_\_\_\_\_\_\_. |
| Option A: | Ephemeral Diffie-Hellman |
| Option B: | Anonymous Diffie-Hellman |
| Option C: | Fixed Diffie-Hellman |
| Option D: | RSA |

Descriptive Questions

|  |
| --- |
| In RSA system the public key of a given user e=7 & n=187  1) What is the private key of this user?  2) If the intercepted CT=11 and sent to a user whose public key e=7 & n=187. What is the PT?  3) Elaborate various kinds of attacks on RSA algorithm? |
| Explain IPSec protocol in detail. Also write applications and advantages of IPSec |
| Differentiate between i) MD-5 and SHA ii) Firewall and IDS. |
| How can we achieve web security? Explain with example. |
| What characteristics are needed in secure hash function? Explain the operation of secure hash algorithm on 512 bit block. |
| What is the need for message authentication? List various techniques used for message authentication. Explain any one of them . |
| Use Hill cipher to encrypt the text "short". The key to be used is "hill". |
| What are different types of viruses and worms? How do they propagate? |
| Explain different TCP/IP vulnerabilities layerwise. |
| Explain Working of DES. |
| What is digital signature. Explain RSA digital signature algorithm. |
| Compare packet sniffing and packet spoofing. Explain session hijacking attack. |
| A and B decide to use the Diffie Hellman algorithm to share a key. They choose p=23 and g= 5 as public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share. |
| Explain working of Kerberos in detail. |
| What is a digital certificate? How does it help to validate the authenticity of a user? Explain X.509 Certificate Format. |
| What are Denial of Service Attacks? Explain any three types of DoS attacks in detail. |
| Compare and Contrast (any two)  i) Block and Stream Ciphers  ii) Substitution cipher and transposition Cipher  iii) MD-5 and SHA-1 |

|  |
| --- |
| List and explain various types of attacks on encrypted message. |
| What is the purpose of S-boxes in DES? Explain the avalanche effect? |
| Why is the segmentation and reassembly function in PGP(Pretty Good Privacy) needed? |
| Give examples of replay attacks. List three general approaches for dealing with replay attacks. |
| With the help of suitable example compare and contrast monoalphabetic ciphers and polyalphabetic ciphers. |
| What are the properties of hash functions? What is the role of a hash function in security? |
| What are the different protocols in SSL? How do the Client and Server establish an SSL connection? |
| Explain the phases in life cycle of a virus. |
| Explain SQL Injection attack with examples. |
| What are the requirements of the cryptographic hash functions? Compare MD5 and SHA-1 hash functions. |
| Elaborate the steps of key generation using RSA Algorithm. |
| Explain with examples, Keyed and Keyless transposition Ciphers. |
| Encrypt the string “This is an easy task” using a playfair cipher with key “monarchy” |
| Given modulus n= 221 and public key, e= 7, find the values of p, q, phi(n) and d using RSA Algorithm and Encrypt M=5. |
| Find GCD of (2278,28) using the Euclidean Algorithm. |
| Explain Steps in MD5 Algorithm along with diagram. |
| What are the attacks on Digital Signature?Explain each of them. |
| A and B wish to use RSA to communicate securely. A chooses public key (e, n) as (7, 247) and B chooses public key (e, n) as (5, 221)   1. Calculate A's Private key. 2. ii. Calculate B's Private Key. 3. iii. What will be the cipher text sent by A to B, if A wishes to send M=5 to B |
| What is meant by DOS Attack? What are different ways mount DOS attacks? |
| How does ESP header guarantee confidentiality and integrity of packet payload? |
| Explain structure of DES wrt:   1. Fiestel structure and its significance 2. Significance of extra swap between left and right half blocks 3. Expansion 4. Significance of S-box 5. DES function |
| What is the need of SSL? Explain handshake mode of protocol. |
| Encrypt the given message using Autokey Cipher, Key=7 and the Message is: "The house is being sold tonight". |
| Explain man in the middle attack on Diffie Hellman. Explain how to overcome the same. |
| Use the playfair cipher with the keyword: "HEALTH" to encipher the message "Life is full of Surprises" |
| What are different types of firewall? How firewall is different than IDS? |
| Explain Kerberos authentication process in detail. |
| Why are digital certificates and signatures required? What is role of digital signature in digital certificates? Explain any one digital signature algorithm. |
| What are the different components of Intrusion Detection System? Compare signature based IDS to anomaly based IDS. |
| Explain Diffie Hellman key exchange algorithm. What types of attacks  are possible on it explain with example. |
| Explain briefly the following attacks with example  (I) Session hijacking (II) Salami Attack  (III) SQL injection (IV) Buffer overflow |
| What is Denial of Service attack? What are the different ways in which an attacker can mount a DOS attack on a system? |
| Elaborate the steps of key generation using RSA algorithm. In RSA system the public key (E, N) of user A is defined as (7,187). Calculate Ф(N) and private key 'D'. What is the cipher text for M=10 using the public  key. |
| What is OSI model? List few security services and Mechanisms for each layer. |
| Explain DES, detailing the Fiestel structure and S-block design. |
| Explain in detail block cipher mode of operation. |
| What is the need for message authentication? List various techniques used for message authentication. Explain anyone. |
| What is a digital certificate? How does it help to validate the authenticity of a user?  Explain the X.509 certificate format. |
| With a block diagram, describe SHA-1 and SHA-2 |
| A chooses public key as (7,33) and B chooses public key as (13,221). Calculate their private keys. A wishes to send message m=5 to B. Show the message signing and verification using RSA digital signature. |
| Explain different types of firewalls and mention the layer in which they operate. |
| With a block diagram give a brief Overview of SSL protocol. |
| What is Pretty Good Privacy (PGP)? Explain the concept of “Webb of Trust” |
| What are the different types of viruses and worms? How do they propagate? |
| Describe various botnet architectures. |
| What are the ways of detecting rootkits |
| Describe the various categories of authentication methods with examples. |
| Explain the working of DES Algorithm |
| Explain the working of AES Algorithm |
| Explain RSA Algorithm with an example |
| Explain the working of Kerberos. |
| *Define authentication and non-repudiation and show with examples how each one can be achieved.* |
| *List and explain various types of attacks on encrypted message.* |
| Why digital signature and digital certificates are required? |
| Explain with example keyed and keyless transposition cipher |
| Explain key rings in POP? |
| What are properties of hash function? Explain role of hash function in security |
| Using Chinese remainder theorem solve the following: x=2 (mod 3), x=3 (mod 5), x=2(mod 7), Find x? |
| How is firewall different from IDS? |
| Why is a digital signature and certificate required? |
| Encrypt “The Key is hidden under the door” using Playfair cipher with keyword “domestic” |
| Discuss any one transposition cipher with example. List their merits and demerits. |
| Write advantages and disadvantages of Symmetric Key Encryption. |
| Compare cryptography with steganography. |
| What is the purpose of S-boxes in DES? Explain the avalanche effect? |
| Explain with examples the CBC and ECB modes of block ciphers. |
| Compare AES and DES. Which one is bit oriented? Which one is byte oriented? |
| Explain the operation of secure hash algorithm on 512-bit block. |
| Compare MD5 and SHA Hash functions. |
| Explain working of Kerberos. |
| Explain any digital signature algorithm in detail. |
| What is Authentication header (AH)? How does it protect against replay attacks? |
| Write in brief about -IP spoofing. |
| Write in brief about IPSec protocols for security. |
| What is firewall? What are the firewall design principles? |
| List various Software Vulnerabilities. How Vulnerabilities are exploited to launch an attack? |
| Write short note on Buffer Overflow. |