BTECH CSE SEM 5 AUTUM 2024-25 INFORMATION SECURITY QUESTION BANK

Introduction:

1. Mention and briefly explain the most prominent information security objectives and their corresponding mechanisms to achieve them.
2. Explain the importance of CIA triad.
3. Which is the most important element/aspect of information security which needs utmost security? Justify your answer.
4. Why has the importance of information security so much increased since last 5-10 years?

Cryptography/Confidentiality:

1. Explain what is meant by message confidentiality.
2. Explain the general model of working of a typical symmetric block cipher with diagram.
3. Classify ciphers on different criteria, along with examples for each classification.
4. Is it possible to encrypt multimedia like sound, video, etc.?
5. Differentiate between cryptography and steganography.
6. Mention some of the most popular symmetric block ciphers along with their supported block size/s and key size/s.
7. Explain the working of Caesar cipher with example.
8. Explain the working of Mono-alphabetic Cipher with example. Explain how this cipher can be attacked, apart from Brute Force Attack.
9. Explain the working of columnar transposition cipher with example.
10. Explain 'Avalanche Effect' with respect to ciphers.
11. Compare and Contrast DES, 3DES and AES on various parameters/criteria.
12. Mention and briefly explain the major design parameters for a symmetric block cipher.
13. What are the major application areas of symmetric block ciphers?
14. Write a short note on: Cryptanalytic Attacks
15. Explain 'Brute Force Attack' with reference to ciphers.
16. Explain the need for OPERATIONAL MODES in symmetric block ciphers. Explain how CBC mode is better than ECB mode in achieving confidentiality.

Asymmetric Ciphers:

1. Explain the general working of RSA algorithm with a block diagram to achieve confidentiality.
2. What is the role of public key and private key in RSA?
3. Why is RSA called as an asymmetric cipher?
4. Explain how RSA can be utilized to achieve authentication along with a block diagram.
5. What are the typical key sizes involved in RSA?
6. Explain in detail, with the help of an example, the RSA key generation process.
7. Explain in detail, with the help of an example, the working of the RSA algorithm, assuming that the required public/private key pairs are already generated.
8. Mention the major application areas of RSA.
9. The key sizes used in RSA are significantly higher than even the most secure symmetric block ciphers. Does this automatically render all symmetric block ciphers useless and obsolete? Give your opinion and justify your stand.
10. Explain, in detail, how an RSA based digital signature can be used. What is the use/application area of digital signatures?
11. Write a short note on: Digital Signature Certificates: Concept, Operations and Application

BTECH CSE SEM 5 AUTUM 2024-25 INFORMATION SECURITY QUESTION BANK

Message Integrity/Password based Authentication

1. Explain what is meant by message integrity.
2. Is it possible to prevent violation of message integrity? If yes, how. If no, why not.
3. Explain the concept/working of message digest, using a block diagram.
4. Mention and briefly explain the major properties of a cryptographic hash function or a message digest. (eg. Collision resistance, etc.)
5. Mention some of the popular message digest algorithms along with their code sizes.
6. Explain, with the help of a block diagram, how message digest can be used, for verifying message integrity.
7. Mention the major application areas of message digests.
8. Explain the role of message digests in password based authentication system.
9. What are the characteristics of a good password?
10. Explain how a weak password can be easily cracked using brute force based approach, with example.

Security Models/Access Control/Biometric Authentication

1. Explain in detail the working and application of Bell LaPadula Security Model.
2. Explain in detail the working and application of BIBA Security Model.
3. Explain what is 2FA with example.
4. Explain what is multi factor authentication.
5. Explain the different approaches to biometric authentication.
6. Explain: DAC, MAC and ABAC with reference to access control.
7. Explain what is ACL and Access Control matrix.
8. What is the role of captcha in web applications? Explain different types of captcha.

Firewalls/NIDS

1. Explain the working a basic packet filtering firewall. Which criteria are normally used by such firewalls for packet filtering?
2. Explain the different types of firewalls.
3. Explain perimeter network and demilitarized zone with reference to firewalls.
4. Explain the use of internal and external firewall with block diagram.
5. What is the use of an NIDS?
6. What is the difference in functionality of an NIDS and a firewall?
7. Explain different types of NIDS systems.
8. Explain: True Positive, True Negative, False Positive and False Negative with reference to an NIDS.
9. What are honeypots and what is their use?
10. What is the importance of Logs in NIDS? Mention the typical/generic format of logs to be maintained in an NIDS.
11. Mention some free and popular software based NIDS.

Network Attacks/Web Application Attacks

1. Differentiate between a vulnerability, a threat and an attack.
2. Differentiate between active and passive attacks. Give examples of each.

3. Briefly explain: IP Spoofing, DNS Spoofing, ARP Spoofing attacks
4. Explain DoS and DDoS attacks with example.
5. Explain : SQL Injection Attack, XSS attack, CSRF attack, Different types of Phishing attacks, Buffer Overflow Attack, Salami Attack, TCP SYN flood attack

Virus/Malware

1. Explain the working of Virus.
2. Mention and explain the modus operandi of some of the popular/famous virus attacks in past.
3. Explain the working of Logic Bomb.
4. Explain the working of Trojan Horse.
5. Explain the working of key loggers. Explain how modern day web applications try to protect their users from key loggers.
6. What is a ransom ware attack?
7. What is session hijacking?

-x-x-x-x-x-