CNS Semester Questions

CNS MAY 2023

Q1a: Explain Security Services and mechanisms to implement it.
Q1b: Compare HMAC and CMAC
Q1c: Explain different NAC enforcement methods
Q1d: Explain SSH protocol stack in brief

Q2a: Explain Playfair cipher with example
Q2b: Describe different Block Cipher modes

Q3a: State firewall design principles and its types with advantages.
Q3b: Describe different types of protocol offered by SSL.

Q4a: What is Network access control? Discuss the elements present in this context.
Q4b: Explain Kerberos Protocol in detail.

Q5a: Explain the working of IPsec in its different mode.
Q5b: What is Network Management Security? Explain SNMP V3.

Q6a: Explain IDS and its types in detail.
Q6b: Define Malware. Explain at least five types with example.

CNS DEC 2023

Q1a: Describe RC5 algorithm with an example.
Q1b: Explain the purpose of keylogger and rootkit.
Q1c: Explain Playfair Cipher with an example.
Q1d: Explain how VPN can be used to encrypt your personal data.

Q2a: Explain Public Key Cryptography and RSA algorithm. Given modulus n=91 and public key e=5, find the value of p, q, phi(n) and d using RSA. Encrypt M=25.
Q2b: List and explain all types of Malware in detail. Differentiate between Virus and Worms.

Q3a: Explain Kerberos protocol in detail. Show how a Kerberos protocol can be used to achieve single sign-on in distributed systems.
Q3b: Explain the OSI Security Architecture and Network Security Model.

Q4a: Explain Email security process. Explain how S/MIME can be used for Digital Signature and verification operations on email messages.
Q4b: Explain the implementation of Network Access Control with one use case.

Q5a: Explain how Network Management security is implemented using SNMP v3.
Q5b: What is an Intruder Detection System? Explain its types in detail.

Q6: Write Short Notes on ANY 4:

- Firewall design principles
- Block Cipher Modes of Operation
- HMAC and CMAC
- Steganography and its applications
- SHA 256 and SHA 512
- SSL Architecture

CNS MAY 2024

Q1a: Distinguish between passive and active security attacks
Q1b: Differentiate between virus and worm
Q1c: Explain SSH protocol stack in brief
Q1d: Write short note on :Email Security

Q2a: Discuss classical encryption techniques with example
Q2b: Explain different types of denial of service attacks

Q3a: What are Block cipher modes. Describe any two in detail
Q3b: Given modulus n=221 and public key e=7 find the values of p, q, phi(n) and d using RSA encrypt M=5

Q4a: Discuss various NAC enforcement methods
Q4b: Design sample digital certificate and explain each field of it

Q5a: Show how a Kerberos protocol can be used to achieve single sign on in distributed systems
Q5b: Explain the different types of protocol offered by SSL

Q6a: Why there is a need of a firewall? Explain the different types of firewalls
Q6b: How does IPSec help to achieve authentication and confidentiality? Justify the need of AH and ESP

CNS DEC 2024

Q1a: Enlist security goals. Discuss their significance
Q1b: Compare and contrast DES and AES.
Q1c: Explain the purpose of keylogger and rootkit
Q1d: SHA provides better security than MD5 Justify

Q2a: Encrypt "This is the final exam" with Play fair cipher, the key is 'Guidance'
Q2b: What is the significance of a digital signature on a certificate ?Justify

Q3a: How does IPSec help to achieve authentication and confidentiality? Justify the need of AH and ESP
Q3b: What Is PKI. Explain PKI architecture in detail

Q4a: Show how a Kerberos protocol can be used to achieve single sign on in distributed systems
Q4b: What is network access control? Discuss the elements present in this context

Q5a: Explain different types of denial of service attacks
Q5b: Explain network management security with respect to SNMP protocol

Q6a: Explain different methods of IDS? State capabilities and challenges in IDS

Q6b: Explain transposition ciphers with illustrative examples