DATA SCURITYE QUESTIONS

- 1. What are the goals of cryptographic systems? Describe various attacks compromising these goals.
- 2. What are the goals of cryptography? Explain anyone in detail.
- 3. What are active and passive attacks?
- 4. Discuss types of attacks.
- 5. Classify the different types of attacks and explain them with example
- 6. Give an example of substitution cipher.
- 7. Give an example of transposition cipher.

DATA SCURITYE QUESTIONS

- 8. Explain DES with neat block diagram.
- 9. Give an example of black cipher.
- 10. Give an example of stream cipher.
- 11. Explain working of standard DES with suitable diagram.
- 12. Explain the double DES and the need for it. Also explain the meet in the middle attack.
- 13. Explain triple DES with two keys and meet in middle attack.
- 14. Explain working of triple DES with two and three keys.
- 15. Write short not on AES

NUMBER THEORY QUESTIONS

- 1. Define Fermat's little theorem .
- 2. State Fermat's little theorem and Euler's theorem. Illustrate with an example how FLT can be used to find modular inverse.
- 3. State Fermat's little theorem and Euler's theorem in modular arithmetic. What is Euler's totient function.
- 4. State Fermat's theorem with their application in cryptography.
- 5. State Euler's theorem with their application in cryptography.
- 6. Write a short note on chines remainder theorem.
- 7. State chines remainder theorem with their application in cryptography.
- 8. Explain chines remainder theorem with example.
- 9. Find the solution to the simultaneous equation x=2 mod 3, x=3 mod 5, x=2 mod 7

ASSYMETRIC KEY CRYPTOGRAPHY QUESTIONS

1. Explain RSA algorithm with an example
2. Explain the RSA encryption and decryption algorithm. Specifically explain why the decrypted message is the same as the plain text
3. Using modular arithmetic and theorem prove that decrypted text is same as plain text in the RSA algorithm
4. explain RSA in detail and also discuss attacks on RSA
5. What is significance of prime numbers in public key cryptography ? Explain RSA algorithm with suitable example

ASSYMETRIC KEY CRYPTOGRAPHY QUESTIONS

1. Write shory note on Deffe Hellmen key exchange
2. prove that the key exchanged between user A and B with Deffe Hellmen key exchange algorithm is the same
3. Explain Deffe Hellmen key exchange algorithm with an example. Also explain attack on Deffe Hellmen key exchange
4. Explain HASH and MAC functions with their role in cryptography
5. Write short note on HASH and MAC functions
6. What do you mean by secure HASH algorithm explain in detail what are the characteristics of secure HASH algorithm
7. What is message digest ? Explain HMAC algorithm
8. What is MDC and MAC ? Explain HMAC in detail
9. Explain hashed MAC with suitable diagram

ASSYMETRIC KEY CRYPTOGRAPHY QUESTIONS

1. What is digital signature ? How are they implemented
2. Write short note on digital signatures
3. Explain digital signature using RSA with example
4. Explain anyone digital signature algorithm in detail

SYSTEM SECURITY QUESTIONS

1. Write short note on intrusion detection system
2. What is intrusion detection system discuss the different techniques of implementing it ?
3. Explain intrusion detection system.
4. Write a short note on secure electronic payment system
5. Write short note on ethical hacking
6. Write short note on digital immune system
7. Write classification of firewall
8. Write a need of firewall
9. Explain operating process of biometric system
10. Explain types of biometric system

Thank You!

(vandanas@sies.edu.in)