8E5002

8E5002

B. Tech. VIII Semester (Main/Back) Examination-2015

COMMAN for #8CS & IT2

INFORMATION SYSTEM SECURITY

Time : 3 Hours Min. Passing Marks : 24 Maximum Marks : 80

Instruction to Candidates :

Attempt any five questions, selecting ***one*** *question from* ***each*** *unit. All questions carry* ***equal*** *marks. (Schematic diagrams must be shown wherever necessary. Any data you feel missing suitably be assumed and stated clearly. Units of quantities used/calculated must be stated clearly.)*

Unit-'I'

1. (*a*) Explain Euler's theorem in Detail. **[6]**

 (*b*) Write short note on:

 (i) Groups and Field

 (ii) Entropy and Unicity Distance **[5×2=10]**

OR

1. (*a*) Use Chinese remainder theorem to solve the simultaneous equation

 $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$ **[8]**

 (*b*) Find the result of the following:

 (i) $5^{-1} \bmod 13$

 (ii) d, if $7d \equiv 1 \pmod{30}$

 (iii) $15^{18} \bmod 17$

 (iv) $21^{24} \bmod 8$ **[4×2 = 8]**

Unit-'II'

2. (*a*) Explain IDEA with all its steps and sub-key generation in detail. **[10]**

 (*b*) Write short note on:

 (i) Substitution and Transposition techniques.

 (ii) Key Distribution in Symmetric Encryption. **[3×2 = 6]**

OR

2. (*a*) Explain DES with Triple DES with all its steps in detail. **[10]**

 (*b*) Explain all block cipher modes of operation with neat diagram. **[6]**

Unit-'III'

3. (*a*) Explain RSA in detail with security analysis of RSA. **[8]**

 (*b*) Write short note on:

 (i) Principles of Public key cryptosystems.

 (ii) RSA exponentiation in Modular Arithmetic. **[4×2 = 8]**

OR

3. (*a*) Explain with all Diffie-Hellman key Exchange steps in detail. **[8]**

 (*b*) Write short note on:

 (i) Distribution of public keys.

 (ii) Distribution of secret keys using public key cryptosystems. **[4×2 = 8]**

Unit-'IV'

4. (*a*) Why is message authentication required? Explain various authentication protocols. **[6]**

 (*b*) Explain SHA-1 algorithm in detail. **[6]**

 (*c*) Write short note on:

 (i) Birthday attack

 (ii) Digital signature **[2×2 = 4]**

OR

4. (*a*) What is message authentication code (MAC)? Explain types of MAC. **[8]**

 (*b*) Write short note on:

 (i) Model of Authentication Systems

 (ii) Elgamal signatures and undeniable signatures. **[4×2 = 8]**

Unit-'V'

5. (*a*) Explain X-509 Authentication procedure with X-509 versions in detail. **[8]**

 (*b*) Explain Pretty Good Privacy (PGP) with general structure of private and public key rings. **[8]**

OR

5. Write short note on:

 (*a*) S/MIME

 (*b*) IPSec

 (*c*) AH and ESP in Transport and Tunnel Mode

 (*d*) SSL **[4×4 = 16]**