53 (CS 717) CRNS

2019

CRYPTOGRAPHY AND NETWORK SECURITY

Paper : CS 717

Full Marks : 100

Time : Three hours

The figures in the margin indicate full marks for the questions.

Question No. ***7*** *is* ***compulsory*** *and answer* ***any five*** *questions from the rest.*

1. Answer the following : 5×3=15

   (a) The following shows the remainders of powers of 10 when divided by 13.

   The pattern will be repeated for higher powers.

   $10^0 \bmod 13 = 1$, $10^1 \bmod 13 = -3$, $10^2 \bmod 13 = -4$

   $10^3 \bmod 13 = -1$, $10^4 \bmod 13 = 3$, $10^5 \bmod 13 = 4$

   Using the above information, find the remainder of an integer when divided by 13. Test your method with 691553672.

Contd.

(b) John is reading a mystery book involving cryptography. In one part of the book, the author gives a ciphertext 'CIW' and two paragraphs later tells the reader that this is a *shift cipher* and the plaintext is 'yes'. In the next chapter, the hero found a tablet in a cave with 'XVIEWYWI' engraved on it. John immediately found the actual meaning of the ciphertext. What type of attack did John launch here? What is the plaintext?

(c) Encrypt the message 'the house is being sold' using one of the following ciphers. Ignore the space between words. Decrypt the message using the ciphertext plaintext :

(i) *Vigenère cipher* with key : 'vigenère'

(ii) *Autokey cipher* with key = 7

2. Answer ***any three*** from the following : 5×3=15

(a) How many rounds of operations are used in the *DES cipher*?

(b) Why does the *DES function* need an expansion permutation?

(c) Why does the round-key *generator* need a parity drop permutation in Key generation? Present the key generation in *DES* with the help of a block diagram.

(d) What is *triple DES*? What is *triple DES with two keys*? What is *triple DES with three keys*?

3. Answer the following : 5×3=15

(a) What are *square roots* of 1 mod n if n is 17 (a prime)? Obtain the roots.

(b) Prove that there is *infinite number of primes* in the set of positive integers.

(c) What are the different *cryptanalytic techniques* that are applied to *DES*? Point out the technical differences. What are the difficulties when a brute force attack is applied in *DES*?

4. Answer the following : 5×3=15

(a) Distinguish between *message integrity* and *message authentication.*

(b) Define the *RSA digital signature* scheme and compare it to the *RSA cryptosystem.*

(c) Describe the *first criterion, the second criterion and the third criterion* for a *cryptographic hash function.*

5. 5×3=15

(a) Identify the application area of *Pretty Good Privacy (PGP).* How does *PGP* contribute to e-mail security?

(b) Distinguish between *security socket layer* and *transport layer security* in a TCP/IP protocol suite. Describe how *master secret* is created from *pre-master secret* in SSL.

(c) Describe the components of a *virus* code. Explain the purpose of the components of the *virus.* How does the *virus* protect itself from being detected by *anti-virus software*?

6. 5×3=15

(a) What are the different types of cryptanalytic attacks? Explain with the help of block diagrams.

(b) What are the two types of cryptanalysis techniques that are used in *DES*?

(c) Differentiate between the two and also explain the uses of the techniques in different cryptanalytic attacks.

7. 5+5+10+5=25

(a) What do you understand by *Asymmetric key cryptography*? Explain with the help of a block diagram.

(b) What are the advantages and disadvantages of *Asymmetric key cryptography*? Formulate a *digital envelope* using a *Symmetric* and *Asymmetric key cryptography.*

(c) Briefly explain the idea behind the *RSA Cryptosystem.* What is the *one-way function* in this system? What is the *trapdoor* in this system? Define the *public and private keys* in this system. Describe the *security* of this system.

(d) Why are two pair of keys required for each sender and receiver in a *Public key infrastructure*? Present the *digital signature algorithm* with help of a block diagram.
