CS+IT

UL(7) — Crypto.

2020(A)

Time : 3 hours

Full Marks : 70

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

*Answer any **five** questions.*

1. (a) Explain the block cipher and stream cipher. 8

   (b) Explain double DES. What kind of attack on double DES makes it use less ? 6

2. (a) Find all multiplicative inverses in z_{10}. 7

   (b) Solve the following equation : 7

   $$10x \equiv 2 \pmod{15}$$

3. (a) Explain the type of Intrusion Detection Systems. 7

(b) Compare conventional encryption and public-key encryption. 7

4. (a) State and explain some advantages and some disadvantages of static and dynamic s-boxes. 7

(b) Compare DES and AES. Which one is bit-oriented ? 7

5. (a) Find the result of the following $(21)^{24}$ mod 8. 7

(b) State and explain the advantages and disadvantages of symmetric-key and asymmetric-key crypto system. 7

6. (a) List some features of the whirlpool cryptographic function. What kind of compression function is used in whirlpool ? 7

(b) Explain security goals. 7

7. Write short notes on any **two** of the following : 7+7 = 14

(a) Diffie Hellman

(b) Key Management

(c) SHA – 512

(d) Digital Signature