No. of Printed Pages : 4

MMTE–006

M. SC. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE) [M. SC.(MACS)]

Term-End Examination

December, 2024

MMTE-006 : CRYPTOGRAPHY

Time : 2 Hours *Maximum Marks : 50*

Note : (*i*) *There are six questions in this paper.*

(*ii*) *The* ***sixth*** *question is* ***compulsory****.*

(*iii*) *Do any* ***four*** *questions from Question Nos.* ***1*** *to* ***5****.*

(*iv*) *Use of calculator is not allowed.*

(*v*) *Show all the relevant steps. Do the rough work at the bottom or at the side of the page only.*

1. (a) Explain the concept of data integrity in Cryptography. Name any tool that is useful in achieving data integrity. 2

(b) Explain the Blum-Blum-Shub pseudo-random bit generator. Find the first four terms of the output for the primes 19, 23 and 3 as the initial integer. 4

(c) Explain the Diffie-Hellman key exchange. 4

2. (a) Decrypt the Vigenère cipher OQLTHEQTFBYZOL, where the keyword is "SMART". Is the Vigenère cipher a polyalphabetic or monoalphabetic substitution cipher ? Justify your answer. 4

(b) Calculate the multiplicative inverse of $x^5 + x^3 + 1$ in $\mathbf{F}_2[x]/\langle x^8 + x^4 + x^3 + x + 1\rangle$. 4

(c) Factorise 221 using the Fermat factorisation method. 2

3. (a) Generate the first ten terms of the LFSR sequence with characteristic polynomial $x^5 + x^3 + 1$, with starting values $(x_0, x_1, x_2, x_3, x_4) = (1,0,1,1,0)$. 3

(b) Compute $5^{21} \pmod{41}$ using repeated squaring algorithm. 4

(c) Let n = 2911 and $\phi(n) = 2800$. Factorise 2911 into two primes. 3

4. (a) What is Merkle-Damgard strengthening ? Illustrate this method with the string "SCRAMBLEDEGGS", assuming a block size 64 bits. 6

   (b) Check that $x^2 + 1 \in \mathbf{F}_3[x]$ is irreducible. Is it primitive ? Justify your answer. 4

5. (a) Alice uses the EIGamal digital signature scheme for signing her messages. She chooses the prime p = 43, primitive root $\overline{5}$ and the secret value $a = \overline{3}$. She makes the values (p, α, β) = (43, 5, 39) public.

   (i) Suppose Alice send the message M = 20 to Bob. She chooses the secret value k = 7. How will she generate the digital signature for this message ? What values will she send to Bob ? 4

   (ii) How will Bob verify the digital signature ? 4

   (b) Explain the difference between Las Vegas algorithm and Monte-Carlo algorithm. 2

6. Which of the following statements are true and which are false ? Justify your answer : 10

(a) We can speed up the encryption in OFB mode of a block cipher by precomputing the key stream.

(b) Non-repudiation is not required if the receiver can authenticate the origin of the message.

(c) The AKS test for primality is more reliable than the Miller-Rabin test.

(d) The pseudo-random sequence generated by a single LFSR is strongly secure.

(e) There is at least one finite field with fifteen elements.

× × × × × × ×