00384

No. of Printed Pages : 3

MMTE-006

M.Sc. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE)

M.Sc. (MACS)

Term-End Examination

December, 2015

MMTE-006 : CRYPTOGRAPHY

Time : 2 hours *Maximum Marks : 50*

Note : *Question no. 1 is* ***compulsory****. Answer any* ***four*** *of the remaining questions.*

---

1. Which of the following statements are *true*, and which are *false* ? Justify your answers. *5×2=10*

(a) The encryption speed in OFB mode of a block cipher can be increased by precomputing the key stream.

(b) Non-repudiation is not required if authentication of the origin by the receiver is possible.

(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.

2. (a) Generate the first 10 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 the repeated squaring algorithm. 4

(c) Asha and Bano generate a common key by using the Diffie-Hellman protocol for secure communication. Suppose Asha chooses $p = 41$, $\alpha \equiv 6 \pmod{41}$, $x = 3$, and Bano chooses $y = 5$. Find the value of the common key, showing all the steps. 3

3. (a) If 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff is the message, and

round key =

00 05 0a 0f 04 09 0e 03

08 0d 02 07 0c 01 06 0f, then

(i) apply a shift row transformation of AES on the message;

(ii) apply round key addition on the result of (i) above;

(iii) apply a subbyte transformation on the output of (ii) above,

where $S[i] = i + 1 \pmod{256}$. 7

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

4. (a) In RSA, what is the advantage of choosing an encryption exponent with a low number of ones in its binary representation ? Is it advisable to have a small decryption exponent ? Justify your answer. *4*

(b) The cipher text EDYW was encrypted using the affine cipher. The plain text starts with HA. Find the complete message. *3*

(c) Find $b > 10$ such that 91 is a pseudoprime to base b. *3*

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

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

6. (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) Compute the multiplicative inverse of $x^5 + x^3 + 1$ in $\mathbf{F}_2 / \langle x^8 + x^4 + x^3 + x + 1 \rangle$. *4*

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