DHANAMANJURI UNIVERSITY

SAMPLE QUESTIONS

Paper Code	**:**	**EMA-008C**
Paper Title	**:**	**Cryptography & Network Security**
Semester	**:**	**VIII**
Full Marks	**:**	**80**
Pass Mark	**:**	**40**

The figures in the right margin indicates full marks for the questions
Answer all the questions:

1. **Choose and rewrite the correct answer:** **(1×3=3)**
   (a) The decryption formula for RSA-cryptosystem is:
   (i) $M = C^e \pmod{n}$, (ii) $C = M^d \pmod{n}$
   (iii) $C = M^e \pmod{n}$, (iv) $M = C^d \pmod{n}$.
   (b) 11×10^6 is equivalent to:
   (i) 128 bits, (ii) 192 bits,
   (iii) 256 bits, (iv) None of the above.
   (c) The value of $14^4 \bmod 55$ is:
   (i) 11, (ii) 14, (iii) 31, (iv) 26
2. **Write very short answer for each of the following:** **(1×6=6)**
   (a) What do you mean by Koblitz Curve?
   (b) Give an example of the replay attacks.
   (c) Change $(1101111)_2$ into a digital form.
   (d) For which n in $\phi(n) \equiv 2 \bmod(4)$.
   (e) Write briefly about PGP.
   (f) What do you mean by mobile security?
3. **Write short answers for each of the following:** **(3×5=15)**
   (a) Write the working of side channel attack.
   (b) Explain briefly Diffie-Hellman key exchange.
   (c) Write the roles of the public and private keys.

(d) Encrypt the message COME SOON using Caesar cipher.

(e) Write three important threats of email.

4. **Answer any *five* of the following:** **(4×5=20)**

(a) Write down the four basic conditions of a field.

(b) Find the value of x if $x \equiv 3^{201} \bmod 11$ by using Fermat's Theorem.

(c) How will you factorize a big number into two prime numbers? Factorize 10403 into two primes.

(d) What do you mean by hash function? Can you write the best hash to use?

(e) What are the differences between DES and AES?

(f) How do Schnorr Signatures Work?

5. **Answer any *two* of the following:** **(6×2=12)**

(a) Encrypt the message "MEET ME AT NINE OCLOCK" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result.

(b) How many one-to-one affine Caesar ciphers are there? Write the digital decryption of the word 'WR WDON LQ FRGHWR LV LQWHOOIJLEH' using Caesar cipher.

(c) Construct a Playfair matrix with the key *occurrence*. Make a reasonable assumption about how to treat redundant letters in the key.

6. **Answer any *two* of the following:** **(6×2=12)**

(a) Solve the simultaneous congruences: $x \equiv 2 (\bmod 3)$, $x \equiv 1 (\bmod 4)$ and $x \equiv 3 (\bmod 5)$. Find the value of x by using the Chinese Remainder Theorem.

(b) State and prove Euler's theorem.

(c) Use the key 1010 0111 0011 1011 to encrypt the plaintext 'ok' as expressed in ASCII, that is 0110 1111 0110 1011. The designers of S-AES got the ciphertext 0000 0111 0011 1000. Do you?

7. **Answer any *two* of the following:** **(6 × 2=12)**

(a) If the plaintext message is $M = 6$ in a public-key cryptosystem using the RSA- algorithm. Perform encryption and decryption, where $p = 5$, $q = 11$, $e = 3$.

(b) What is email architecture? Describe in detail how does email system work in computer network.

(c) If E be the elliptic curve $Y^2 = X^3 - 15X + 18$ and the points $P = (7,16)$ and $Q = (1,2)$ lie on the curve E. Then obtain $P \oplus Q$ and $P \oplus P$ with diagrams.

*****