



JK Lakshmipat University, Jaipur
Institute of Engineering and Technology
Introduction to Cryptography (CS1229)
End Semester Examination, B.Tech., VI Semester

Duration: 2 hours

MM: 30

There are three questions in this paper with sub-parts. You have to attempt all the questions. The simple calculator and Casio FX-82MS version are allowed in the examination.

1. Explain the following: (2x3 - COs 1,2,3,4)

- (a) What are the fundamental differences between AES and DES in terms of their encryption algorithms?
- (b) Alice wants to encrypt the letter A, where the letter is given in ASCII code. The ASCII value for A is $65_{10} = 1000001_2$. Let's furthermore assume that the first key stream bits are $(s_0, \dots, s_6) = 0101100$.
- (c) Explain three classical Ciphers with mathematical equations. What are the advantages and disadvantages of classical ciphers over modern symmetric ciphers?

2. Short Answer Questions: (3 x 4 - COs 1, 2, 3,4)

- (a) If $m = 4$ (m here is number of Flip-Flops), $p_3 = 0$, $p_2 = 0$, $p_1 = 1$, $p_0 = 1$, What is the corresponding LFSR output? What is the maximum period? Design the corresponding LFSR if the initial values are 0000.
- (b) Encrypt and decrypt by means of the RSA algorithm with the following system parameters: $p = 5$, $q = 11$, $e = 3$, $x = 9$ x here is plaintext.
- (c) Explain different modes of block cipher. Illustrate the corresponding encryption-decryption figure with the suitable equations.
- (d) Explain the encryption scheme developed from the Diffie-Hellman key exchange protocol. List out its advantages over standard RSA.

3. Long Answer Questions:

(4x3 - CO 1, 2, 3, 4,5)

- (a) Using the Extended Euclidean algorithm, compute the greatest common divisor and the parameters/integer coefficients s , t of **67** and **12**. Note: $\gcd(r_0, r_1) = s \cdot r_0 + t \cdot r_1$ where s and t are integer coefficients.
- (b) Computing modular exponentiation efficiently is inevitable for the practicability of RSA. Compute the following exponentiations $x^e \bmod m$ applying the square-and-multiply algorithm: $x = 2$, $e = 79$, $m = 101$ After every iteration step, show the exponent of the intermediate result in binary notation.

- (c) As we know, the Diffie–Hellman protocol is as secure as the Diffie–Hellman problem, which is probably as hard as the DL problem in the group Z_p^* . However, this only holds for passive attacks, i.e., if Oscar is only capable of eavesdropping. If Oscar (the attacker) can manipulate messages between Alice and Bob, the key agreement protocol can easily be broken! Develop an active attack against the Diffie–Hellman key agreement protocol, with Oscar being the man in the middle.