INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Department of Mathematics

End-Semester Examination 2018

MA61027 : Cryptography and Network Security

Duration: 3 Hours

Total Marks 50

Answer **ALL QUESTIONS**. All the notations are standard and no query or doubts will be entertained. If any data/statement is missing, identify it in your answer script. Marks are indicated at the end of each question.

1. Suppose Bob has an RSA Cryptosystem with modulus N and encryption exponent e_1 and Charlie has an RSA Cryptosystem with (the same) modulus N and encryption exponent e_2. Suppose also that $gcd(e_1, e_2) = 1$. Now consider the situation that aries if Alice encrypts the same plaintext m to send to both Bob and Charlie. Thus, she computes $c_1 = m^{e_1} \mod N$ and $c_2 = m^{e_2} \mod N$ and then she sends c_1 to Bob and c_2 to Charlie. Suppose Oscar intercepts c_1 and c_2, and performs the the computations indicated in the following algorithm:

   Algorithm: RSA Common Modulus Decryption (N, e_1, e_2, c_1, c_2)

   $b_1 = e_1^{-1} \mod e_2$

   $b_2 = \frac{(b_1 e_1 - 1)}{e_2} \mod e_1$

   $x = {c_1}^{b_1} ({c_2}^{b_2})^{-1} \mod N$

   return (x)

   Prove that the value x computed in the above algorithm is in fact Alice's plaintext m. Thus, Oscar can decrypt the message Alice sent, even though the cryptosystem may be "secure". [5]

2. a. [4 **mark**] Find all points (including the point at infinity) of the modular elliptic curve E defined by $y^2 = x^3 + 8 \pmod 7$.

   b. [4 **mark**] Describe an ElGammal cryptosystem using the Elliptic curve points.

   c. [2 mark] Discuss the advantages of using Elliptic Curve Cryptosystems (ECC) over other public key cryptosystems.

3. (a) Describe the **RSA algorithm** and illustrate how the public and private keys are generated.

   b. Given the superincreasing sequence $X = (2, 3, 6, 12, 24, 48, 96, 200)$. Encrypt the plaintext 10010110 using easy Knapsack cipher. Explain why it is not secure. To make it strong, choose $m = 453$ and $k = 61$, then generate the sequence $kX \mod 453$. What is the public key in this strong knapsack? Use this public key encrypt the plaintext 10010110. Use the private key (453, 61) to decrypt the message. [7]

4. (i) Draw a detailed diagram of a single DES round

(ii) Draw a detailed diagram of the CBC mode of operation on DES

(iii) Give three properties all random number **generators** should have.

(iv) Explain LFSR based Pseudorandom Number Generator. [8]

5. a) Find the quadratic residues and quadratic non-residues modulo 13.

b) Use the **Extended Euclidean Algorithm** to compute 17^{-1} mod 101. [7]

6. Describe Diffie-Hellman Key exchange technique. [4]

7. (a) Describe ElGamal Signature Scheme.

(b) What is the verification congruence if in the ElGamal signature scheme s is computed as $s = (ar + kh(m)) \mod p$?

(c) Modify the ElGamal signature system such that the verification only requires two exponentiation mod p. [9]

——-The End———