DEPARTMENT OF MATHEMATICS, IIT - Kharagpur
Mid Semester Examination (Autumn 2018)
MA 61027 Cryptography and Network Security
Instructor: Dr. Sourav Mukhopadhyay
No. of students: 150. Total Points: 30. DURATION: 2 Hours

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. An S-box $S : \{0,1\}^m \to \{0,1\}^n$ is said to be balanced if $|S^{-1}(y)| = 2^{m-n}$ for all $y \in \{0,1\}^n$. Consider the following DES S-box $S_5 : \{0,1\}^6 \to \{0,1\}^4$:

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Table 1: DES S-box S_5

   (a) Determine the set ${S_5}^{-1}(1001)$.

   (b) Prove that S_5 is balanced. [4]

2. What is perfect secrecy? State Shannon's theorem. [2]

3. Describe the AES-Rijndael encryption function. [5]

4. In the RSA cryptosystem encryption is performed using $C \equiv M^e (mod\ N)$, where $N = pq$ for suitably chosen large primes p, q, and $gcd(e, \phi(N)) = 1$. In a chaining attack on RSA, given a ciphertext $C \equiv M^e (mod\ N)$ the attacker computes,

$$C^e (mod\ N),\ C^{e^2} (mod\ N),\ \ldots,\ C^{e^k} (mod\ N)$$

unless $C \equiv C^{e^k} (mod\ N)$ is obtained. That is, k is the least positive integer that specifies the cycle.

   (a) Explain why attacker can always find $k \in [1, N-1]$ so that $C \equiv C^{e^k} (mod\ N)$.
   Hint: Recall that RSA is an encryption algorithm and therefore bijective, i.e. $M_1 \neq M_2$ cannot be mapped to the same ciphertext.

   (b) Can attacker recover the message M from the observed sequence above in case $C \equiv C^{e^k} (mod\ N)$ is valid?

   (c) Explain how attacker can factor N by finding an integer u such that $gcd(C^{e^u}, N) > 1$. [6]

——-P.T.O.—

4. What is Knapsack problem? Describe Merkle-Hellman Knapsack cryptosystem. [5]

5. Describe Diffie-Hellman Key exchange protocol and the Man in the middle (MITM) attack on Diffie-Hellman Key exchange protocol. [4]

6. In ElGamal cryptosystem let us choose prime $p = 107$, randomness $k = 46$, generator $g = 2$. If you have the secret key as $\alpha = 67$, then find the ciphertext encrypting the message $m = 44$. [2]

7. Let $P = (3, 8)$ and $Q = (10, 13)$ be two points on an Elliptic curve $y^2 = x^3 - 5x + 1$ over $\mathbb{Z}_{17}$. Find $P + Q$ and $2P$. [2]

[End]