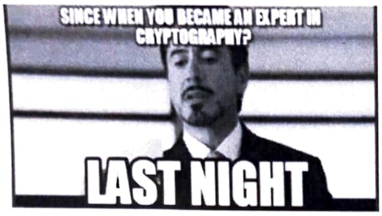
IIT Jodhpur
Cryptography

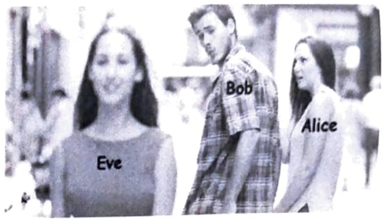
CSL-7480
Major exam
Time: 2 hours (12-2 pm, 9 May 2024)

Sem. 2, 2023-24
Instructor: Somitra Sanadhya
Max. Marks: 40

Notes:

1. There are 10 questions of 4 marks each.
2. Do not write unnecessarily verbose answers.
3. No queries will be entertained during the test.
4. Notation: || denotes concatenation of two strings, and LSB(x) denotes the least significant bit of x.





Some jokes before we begin the exam. Best wishes. :-)

1. State whether the following statements are true or false. Proper justification is required in support of your answer.
   (a) There exists a pseudorandom generator G_n where for every n, $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ such that for every $x \in \{0,1\}^n$, the first $n/3$ bits of $G_n(x)$ are zero.
   (b) There exists a pseudorandom generator G_n where for every n, $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ such that for every $x \in \{0,1\}^n$, there exist $n/3$ bits of $G_n(x)$ that are zero.

(2+2 =4 marks)

2. You are given a PRF $f_K(x) : \{0,1\}^n \to \{0,1\}^n$. Using this, you wish to create a PRP $g_K : \{0,1\}^{3n} \to \{0,1\}^{3n}$. In both of these constructions, K is the secret key which allows us to index the specific function/permutation from the keyed family.

   For notational convenience, we use the inputs and outputs of g as 3 strings of n bits each. That is, $g_K(x_1||x_2||x_3) = (y_1||y_2||y_3)$.
   Further, let $y_2 = f_K(x_1) \oplus x_2 \oplus f_K(x_3)$, $y_1 = x_1 \oplus f_K(y_2)$, and $y_3 = x_3 \oplus f_K(y_2)$.

   (a) Prove that $g_K(\cdot)$ is a permutation.
   (b) Show that $g_K(\cdot)$ is not a PRP. You are allowed to query $g_K(\cdot)$ without knowing how $f_K(\cdot)$ is constructed.

(2+2 = 4 marks)

3. Let $h(user)$ be defined as $h(user) = \text{SHA256}(user@\text{iitj.ac.in})$ where $user$ is the username of a student in the institute email service. You pick x as your own email-id and let y be some other email-id. Your goal is to find any y such that the first 100 bits of $h(x)$ and $h(y)$ match.

   How many calls to SHA256 will be required to find such a username y? Justify your answer.

(4 marks)

$O(2^{N/2})$

4. Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a private-key encryption scheme that is CPA secure and operates on fixed-length messages $M \in \{0,1\}^n$ with keys $K \in \{0,1\}^\ell$. We use it to construct a new encryption scheme $\Pi^* = (\text{Gen}, \text{Enc}^*, \text{Dec}^*)$. In which of the following cases is Π^* also CPA secure? Prove your answer.

   (a) $\text{Enc}^*_K(M) = \text{Enc}_K(M \oplus 1^n)$.

   (b) $\text{Enc}^*_K(M) = \text{Enc}_K(M) \| \text{ LSB}(M)$.

(2+2= 4 Marks)

5. Suppose Alice wants to send a message to Bob containing her name N, her computer's IP address IP, and a request R for Bob. Explain what message m should Alice send to Bob to meet the security requirements below. Assume that Alice and Bob share a symmetric key K and have securely distributed their public keys K_A and K_B. (Their secret keys are not needed in this question). Assume that all the messages include Alice's name, IP address, and the request.

   (a) Using the symmetric key, design a message that enables Bob to verify that the message's integrity has not been violated and that it is from Alice.

   (b) Using public key cryptography, design a message that enables Bob to verify that the message's integrity has not been violated and that it is from Alice.

(2+2 = 4 marks)

6. Your friend uses $n = 51$ in the RSA encryption scheme. Compute a valid key pair (e, d) for this parameter. How many values of e are possible for this n ? (2+2 = 4 marks)

7. Diffie-Hellman Key Exchange allows two parties to share a secret key in one step of communication by these parties. Explain how can you share a secret key among 3 parties in a single step. Formally state the assumption which ensures that the scheme you presented is secure. (2+2 = 4 marks)

8. Formally define a Commitment scheme. What are the security properties of the same? (2+2 = 4 marks)

9. Explain what is meant by completeness and soundness with respect to a Zero-knowledge proof (ZKP). Show a ZKP for two large graphs being isomorphic. (2+2 = 4 marks)

10. In Shamir's Secret Sharing scheme, a secret has been shared among n parties using a polynomial of degree k. Party i has an input (x_i, y_i) with them. Is is observed that there are two users i and j with inputs (x_i, y_i) and (x_j, y_j) such that $x_i = x_j$ but $y_i \neq y_j$. It is clear that one of them is trying to cheat the system (by sharing an incorrect secret). How can you know who is the cheater? What restriction do you need on n in terms of k? (4 Marks)

*****