॥ त्वं ज्ञानमयो विज्ञानमयोऽसि ॥

Indian Institute of Technology Jodhpur

**Cryptography ( CSL-7480)**

Minor-1, Date: Feb 08, 2024

Instructor: Somitra Sanadhya

Timing: 2:30 to 3:30 PM

Autumn 2023-24

Max mark: 15

Note:

(1) The notation $x \parallel y$ denotes concatenation of strings $x$ and $y$.

(2) No clarification will be provided on the test. Whatever was to be explained has already been mentioned in the questions.

(3) Be brief and to-the-point in your answers.

1. A common technique to ensure error-free communication is to add some extra (redundant) bits in the transmission. For example, rather than sending a message 10, one might send 101010 and the recipient can understand what was the intended message even if some bit gets flipped due to disturbance during the communication. This is commonly called "error correction".

   You are a communication expert who is approached by an organization for consulting. They are considering two approaches of using error correction with encryption:

   (a) encrypt a message and then add error correction to the cipher text, or

   (b) add error correction to the plaintext and then encrypt the modified plaintext.

   Which of the two should you recommend? Why? **(2)**

2. Your friend wishes to use the OTP encryption for $n$-bit messages. But she realizes that the encryption of a message $m$ with the zero key (i.e. $k = 0^n$) results in the same ciphertext as the plaintext. So she suggests not using the zero key. Her modified encryption scheme is as follows:

   (a) Pick a key $k$ uniformly at random. If the key happens to be $0^n$ then retry until you get a different key.

   (b) Use this key to encrypt the message $m$ as $m \oplus k$.

   Is this an improvement over OTP or a bad idea? Justify your answer. **(1)**

3. Consider the following mode of encryption of a block cipher $E_k(\cdot)$ with block length $n$. We assume that the message length (after padding) is a multiple of $n$. Let $m = m_1 \parallel m_2 \parallel \ldots \parallel m_t$, where each $m_i$ is $n$ bits long.

$r_0$ = Randomly pick a string from $\{0,1\}^n$
$c_0 = r_0$
for(i=1; i $\leq$t; i++){
    $r_i = E_k(m_i)$
    $c_i = r_i \oplus r_{i-1}$
}
return $c_0 \parallel c_1 \parallel \ldots \parallel c_t$.

(a) How can you decrypt the ciphertext? (1)

(b) Show that the above mode is not CPA secure. That is, show an attacker who can break the CPA security definition for this construction. (2)

4. Let $G$ be a secure PRG from $\{0,1\}^n$ to $\{0,1\}^{3n}$. Which of the following constructions are PRG? Justify your answers. (Note that $s \in \{0,1\}^n$)

   (a) $G_1(s)$: $G(s) = x \parallel y \parallel z$, Return $G(x) \parallel G(y)$. (1)

   (b) $G_2(s)$: $G(s) = x \parallel y \parallel z$, Return $x \parallel y$. (1)

   (c) $G_3(s)$: $G(s) = x$, $G(0^n) = y$, Return $x \oplus y$. (1)

5. Prove that $n$ rounds of Feistel structure can be inverted by the same structure with the round key schedule reversed. (3)

6. (a) Suppose $G = \langle g \rangle$ be a group, and let $x = g^i$ be an element of $G$. Suppose you have an algorithm $\mathcal{A}$ available to you, which on input $g^j$ produces $j$. However, you are not allowed to call $\mathcal{A}$ with input $x$. How can you compute $i$ using $\mathcal{A}$ ? (2)

   (b) Define CDH and DDH problems and show that a solver for CDH can solve DDH. (1)

****