IT301: Information Security

Midsem (Remote) Marks: 10 (Time: 40 Min)

Course Instructor: Dr. Dibyendu Roy Date: Sept 15, 2021

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be written clearly.

Problem 1 **2 marks**

Write down the decryption algorithm of DES in CBC mode of operation. You are NOT required to write the key-scheduling algorithm.

Problem 2 **2 marks**

Consider the plaintext set $\mathbb{P} = \{0, 1, \dots, 25\}$ and ciphertext set $\mathbb{C} = \{0, 1, \dots, 25\}$. The encryption algorithm takes the secret key randomly from the set $\mathbb{K} = \{0, 1, \dots, 25\}$. The encryption function is $c = \text{Enc}(p, k) = (p + k) \mod 26$, where $p \in \mathbb{P}, k \in \mathbb{K}, c \in \mathbb{C}$. Prove or disprove the following statement:

> "The above encryption algorithm will provide perfect secrecy if the key is used only once for each encryption."

Problem 3 **2 marks**

Suppose that $K = (5, 21)$ is a key in an Affine Cipher over $\mathbb{Z}_{31}$.

(a) Express the decryption function $d_K(y)$ in the form $d_K(y) = a'y + b'$, where $a', b' \in \mathbb{Z}_{31}$.

(b) Prove that $d_K(e_K(x)) = x$ for all $x \in \mathbb{Z}_{31}$.

Problem 4 **2 marks**

If an encryption function e_K is identical to the decryption function d_K, then the key K is said to be an involutory key.

(a) Suppose that $K = (a, b)$ is a key in an Affine Cipher over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \mod n = a$ and $b(a + 1) \equiv 0(\mod n)$

(b) Determine all the involutory keys in the Affine Cipher over $\mathbb{Z}_{15}$.

(c) Suppose that $n = pq$, where p and q are distinct odd primes. Prove that the number of involutory keys in the Affine Cipher over $\mathbb{Z}_n$ is $n + p + q + 1$.

Problem 5 **2 marks**

Consider a Feistel based block cipher E with 5 rounds. The block size of the cipher is 64 bits and key size is 32 bits. The keyscheduling algorithm generates the 5 round keys $K_1, \dots, K_5$ as follows $K_i = \text{left-circular-rotate}(K, i)$. Here left-circular-rotate function takes two inputs one is a 32-bit key K and another is a positive integer i. It performs circular rotation on K in the left direction by i times and produces a 32-bit output. The round function $f : \{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32}$ is defined as follows

- $f(X, Y) = S(X \oplus Y)$, where $S : \{0,1\}^{32} \to \{0,1\}^{32}$ and defined as

$$S(B) = (Subbytes(b_0), Subbytes(b_1), Subbytes(b_2), Subbytes(b_3)).$$

Here $B = (b_0 \parallel b_1 \parallel b_2 \parallel b_3)$ and $length(b_i) = 8$ bits and $Subbytes$ is the Subbytes table of AES.

Derive the relation between $E(M, K)$ and $E(\overline{M}, \overline{K})$. Here if $X = (x_1, \dots, x_n) \in \{0,1\}^n$ then $\overline{X} = (1 \oplus x_1, \dots, 1 \oplus x_n)$.