CS304: Introduction to Cryptography & Network Security

Assignment #1

Course Instructor: Dr. Dibyendu Roy Due: March 16, 2024, 11:59 pm

Instructions: Clearly write your name and roll number on the top of each page. Solutions must be written clearly. I expect all students to behave according to the highest ethical standards. Any cheating or dishonesty of any nature will result in deduction of marks.

Problem 1

Consider the plaintext (i.e., message) CRYPTOGRAPHY and the permutation π on 12 numbers as defined below.

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 5 & 6 & 9 & 11 & 1 & 8 & 2 & 10 & 4 & 12 & 7 \end{pmatrix}$$

(a) Using the encryption technique of Transposition cipher encrypt the above plaintext.

(b) Check whether decryption is possible or not (provide justification). If decryption is possible write down the decryption technique.

Problem 2

Consider the plaintext (i.e., message) WEAREINDIAN and generate the ciphertext using the Shift cipher encryption algorithm with the secret key 4. Perform decryption on the ciphertext to check the correctness of your encryption.

Problem 3

Encrypt the plaintext WEAREINDIAN using Playfair cipher, where the secret key is CRICKET. Perform decryption on your generated ciphertext to validate your encryption.

Problem 4

In case of Affine cipher the key is $K = (a, b)$, where $0 \leq a, b \leq 25$ and the encryption algorithm is $y = Enc_K(x) = (a \cdot x + b) \mod 26$. Find out the case when the decryption is not possible. Write down the decryption algorithm when we can have successful decryption. Find out the exact number of different keys for which we will have the same plaintext-ciphertext pair (x, y).

Problem 5

If Enc is the encryption function of DES then find out the relation between the ciphertexts $C_1 = \mathsf{Enc}(\mathsf{M}, \mathsf{K})$ and $C_2 = \mathsf{ENC}(\overline{\mathsf{M}}, \overline{\mathsf{K}})$. Here $\overline{X}$ denotes the bitwise complement of X i.e., if $X = (x_1, \ldots, x_n)$ then $\overline{X} = (1 \oplus \overline{x_1}, \ldots, 1 \oplus \overline{x_n})$.

Problem 6

One unknown plaintext is encrypted using shift cipher encryption algorithm. The ciphertext is AFITIFWF. Find the plaintext and the secret key.

Problem 7

We use the following correspondence $A \to 0$, $B \to 1$, $\ldots$, $Z \to 25$ to map english letters (A to Z) to numbers from 0 to 25. Let the message HILL is encrypted to XIYJ by using Hill cipher. Find atleast one possible key.

Problem 8

Using Euclidean algorithm solve the following problems.

(a) Find the $gcd(222, 18)$.

(b) Find x_0, y_0 such that $1 = 33x_0 + 13y_0$.

(c) If b is the multiplicative inverse of a under modulo n i.e., $a \cdot b \equiv 1 \mod n$. Find the multiplicative inverse of 5 under modulo 26.

Problem 9

Prove that if we apply AES Subbytes function on $D3$ you will get 66 as output.

Problem 10

Find the AES-Mixcolumn$(33, 42, 66, 24)$. Here inputs and outputs are given in integer.

Problem 11

Let p be a prime number For $a, b \in \mathbb{Z}_p$, define $f(a, b) : \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule $f_{(a,b)}(x) = ax + b \mod p$. Let $x \neq x' \in \mathbb{Z}_p$ such that $f_{(a,b)}(x) = y$ and $f_{(a,b)}(x') = y'$. Given x, x', y, y' is it possible to find $a, b \in \mathbb{Z}_p$, if possible derive a, b, if not give proper justifications.

Problem 12

Define a toy hash function $h : (\mathbb{Z}_2)^7 \to (\mathbb{Z}_2)^4$ by the rule $h(x) = xA$ where all operations are modulo 2 and the matrix A is given below

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Find all preimages of $(0, 1, 0, 1)$.

Problem 13

Suppose $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ is a collision resistant hash function. Define $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ as follows:

(a) Write $x \in \{0,1\}^{4m}$ as $x = x_1 \parallel x_2$, where $x_1, x_2 \in \{0,1\}^{2m}$.

(b) Define $h_2(x) = h_1(h_1(x_1) \parallel h_1(x_2))$.

Show that h_2 is collision resistant.