Cryptography and Network Security (CS60065)

AUTUMN, 2022-2023

TA: Tapadyoti Banerjee
Rijoy Mukherjee

Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India

TUTORIAL: 1
DATE: 12TH August 2022

QUESTION : 1 (The Shift Cipher)

Let P = C = K = $\mathbf{Z}_{26}$, where **Z** the set of integers. Consider the key for a Shift Cipher is K = 11, and the plaintext is “MEET”. Find the corresponding ciphertext.

QUESTION : 2 (The Substitution Cipher)

Let P = C = K = $\mathbf{Z}_{26}$, where **Z** the set of integers. Consider the random permutation for encryption function as follows:

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
X	*N*	*Y*	*A*	*H*	*P*	*O*	*G*	*Z*	*Q*	*W*	*B*	*T*

n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
S	*F*	*L*	*R*	*C*	*V*	*M*	*U*	*E*	*K*	*J*	*D*	*I*

And the ciphertext is “TVVM”. Find the corresponding plaintext.

The Affine Cipher

Let $P = C = K = \mathbf{Z}_{26}$, and let

$K = \{(a, b) \in \mathbf{Z}_{26} \text{ x } \mathbf{Z}_{26} : \gcd(a, 26) = 1\}$.

For K = (a, b) ∈ K, define

$$e_K(x) = (ax + b) \bmod 26$$

And

$$d_K(y) = a^{-1}(y - b) \bmod 26$$

where $(x, y) \in \mathbf{Z}_{26}$

QUESTION : 3 (The Affine Cipher)

Suppose that K = (7, 3), i.e., a = 7 and b = 3. Here all operations are performed in $\mathbf{Z}_{26}$, where **Z** the set of integers. verify that

$$d_K(e_K(x)) = x \text{ for all } x \in \mathbf{Z}_{26}.$$

QUESTION : 4 (The Affine Cipher)

Suppose that K = (7, 3), i.e., a = 7 and b = 3. Here all operations are performed in $\mathbf{Z}_{26}$, where **Z** the set of integers. Now, encrypt the plaintext “MEET” by using the concept of Affine Cipher.

QUESTION : 5 (The Vigenere Cipher)

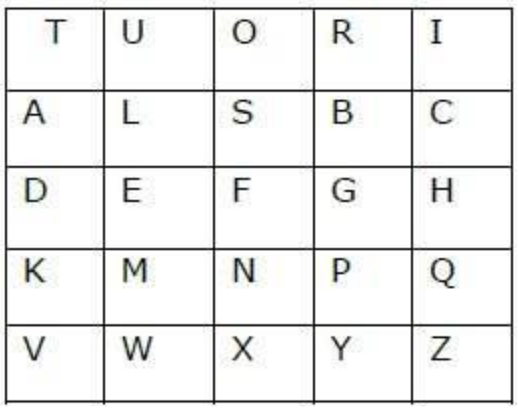
Suppose that K = “POINT”. Now, encrypt the plaintext “SOUTH EAST” by using the concept of Vigenere Cipher.

QUESTION : 6 (The One-time Pad)

Suppose we encrypt the name “point” with a one-time pad (consider the length of the keyword is 5). To break the ciphertext by brute force attack, find the number of computations you need.

The Playfair Cipher

Suppose Key = ‘tutorials’, then 5 x 5 grid is as follows:



T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

We want to encrypt the message “hide money”.
It will be written as − HI DE MO NE YZ
The encrypted Message is -- QC EF NU MF ZV

QUESTION : 7 (The Playfair Cipher)

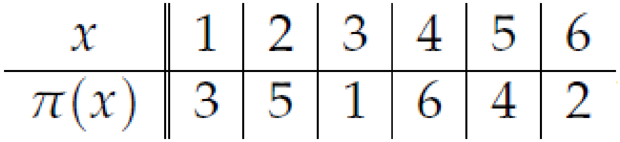
Find the security value of the Playfair Cipher.

QUESTION : 8 (The Simple Transposition Cipher)

Suppose the secret random key is “five”, and the plaintext is “golden statue is in eleventh cave”. Determine the ciphertext.

QUESTION : 9 (The Permutation Cipher)

Suppose key = 6 and the key is the permutation for encryption is



x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Determine the plaintext for the ciphertext:

EESLSHSALSESLSHBLEHSYEETHRAEOS