

Introduction to Computer Security

Assignment - 2.

1) cipher-text dually.

shift at 1
 $k=1$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 b c d e f g h i j k l m n o p q r s t u v w x y z a
 plaintext = cotzku.

shift at 2
 $k=2$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 c d e f g h i j k l m n o p q r s t u v w x y z a b
 plaintext = bnsyju.

shift at 3
 $k=3$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 d e f g h i j k l m n o p q r s t u v w x y z a b c
 plaintext = amrxiv.

shift at 4
 $k=4$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 e f g h i j k l m n o p q r s t u v w x y z a b c d
 plaintext = zlqwhu.

shift at 5
 $k=5$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 f g h i j k l m n o p q r s t u v w x y z a b c d e
 plaintext = ykpvgt.

shift at 6
 $k=6$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 g h i j k l m n o p q r s t u v w x y z a b c d e f
 plaintext = xjoufs.

shift at 7
 $k=7$
 a b c d e f g h i j k l m n o p q r s t u v w x y z
 h i j k l m n o p q r s t u v w x y z a b c d e f g
 plaintext = "winter"

At $k=7$, we get the english word "WINTER"

2.)

The rail fence cipher is a form of transposition cipher where it is encrypted / decrypted using a particular key / depth value.

Given cipher text :

"c d e f g h i j k l m n o p"

$$\text{depth} = 4$$

$$|\text{cipher}| = 14$$

$$\therefore \text{cipher} / \text{depth} = 14 / 4 = 3$$

$$\text{and } \text{cipher} \% \text{depth} = 14 \% 4 = 2$$

$$\therefore 1^{\text{st}} \text{ row} = 3 + 1 = 4 \text{ letters}$$

$$2^{\text{nd}} \text{ row} = 3 + 1 = 4 \text{ letters}$$

$$3^{\text{rd}} \text{ row} = 3 \text{ letters}$$

$$4^{\text{th}} \text{ row} = 3 \text{ letters}$$

c d e f

g h i j

k l m

n o p

So the plain text comes out as

c g k n d h l o e i m p f j jotted it down diagonally.

3.) Row transposition cipher is a form of transposition cipher where we write letters of message out in rows over a specified number of columns and reorder the columns according to some specified key and then reading of the rows.
To decrypt a cipher text using row transposition cipher.

Cipher text : c d e f g h i j k l m n o p q r s t
key : 3 1 5 2 6 4

key = 6

Cipher = 18

So no. of rows will be $\text{cipher} / \text{key} = 18 / 6 = 3$

3 1 5 2 6 4

e d

f l c r i o

g m d s j p

h n e t k q

So, in a group of

3, we write

down the cipher

text in against

the designated

column ~~row~~ for eg. here c d e will be written in the 3rd column before key 5.

So, the plain text turns out to be

f l c r i o g m d s j p h n e t k q.

4.)

The playfair cipher is a substitution cipher which uses a key to encrypt the plaintext. It consists of a key square which is a 5×5 grid of alphabets that acts as a key for encrypting the plaintext.

The 25 letters also filled in should be unique and without duplicates and also i/j contains in same block.

plaintext : heecggs

Keyword : helo!

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

To encrypt :

the plaintext is split in pairs. If there are odd number of letters or if there are any duplicates consecutively then we add 'x' as a filler.

Here in heecggs pairs will be he, ec, gx, gs.

Match the row-column of the letters respectively to arrive at the encrypted text.

If they are in same row/column, go with the next / below alphabets.

do for this problem.

he \rightarrow ei (same row, go with next alphabet)

ec \rightarrow ck (same column, go with below alphabet)

gx \rightarrow dz (replace by the letter in

gs \rightarrow du the same row and in the column of the other letter of the pair)

5.) S-Box

S-Boxes are substitution boxes of 8. It has 6 bit input & 4-bit output. The input of 48 bits are divided into 8 6-bit sub blocks.

(1.) output of given S-box is 6.

As given in the table, there are 4 occurrences of value 6 in given S-box.

Hence possible inputs are.

1.) Row 0, column 10.

So, this can be 010100

2.) Row 1, column 9 which is 010011

3.) Row 2, column 5 which comes out to be 101010

4.) Row 3, column 14 which can be written as 111101.

(2.) Output of S-box is 100101

take the first and the last of input digits
to calculate the row

So, 11 \rightarrow Row 3.

the middle four digits (exclude first and last)
to calculate column

So, 0010 \rightarrow Column 2.

The output against row 3 and column 2 is

8

6.)

(1.) output of P table

01000000 00100000 00000000 00000000

\uparrow

\uparrow

2nd bit

11th bit

So, against 2nd position and 11th position, we
can say that 7th and the 23rd bit will
be '1', and the rest will be the '0'.

(2.) Input of P table

01000000 00100000 00000000 00000000

2nd bit

11th bit

2nd is in 17th position and 11th is in 30th position.

So, 17th bit and 30th bit will be '1', rest will be '0'.

7.) Fermat's Little Theorem

If 'p' is a prime number and 'a' is a positive integer not divisible by 'p' then

$$a^{p-1} = 1 \pmod{p}$$

Given problem $3^{503} \pmod{11}$

$$\left[(3^{10})^{50} * 3^3 \pmod{11} \right]$$

$$\left[\underbrace{(3^{10} * 3^{10} * 3^{10} * \dots * 3^{10})}_{50 \text{ times}} * 3^3 \right] \pmod{11}$$

$$\left[(3^{10} \pmod{11}) * (3^{10} \pmod{11}) * \dots * (3^{10} \pmod{11}) * (3^3 \pmod{11}) \right] \pmod{11}$$

$$3^3 \pmod{11}$$

$$27 \pmod{11} = \underline{\underline{5}}$$

8.) To use S-box S3

prove that:

The 4 output bits from each S-box affects six different S-boxes on the next round.

considering for S-box S3.

as 9, 10, 11, 12

q^{th} $9 = 24^{th}$ place $10 = 16^{th}$ place $11 = 30^{th}$ place $12 = 6^{th}$ place

E-table :

 $24 \rightarrow 35 \rightarrow S6$ $24 \rightarrow 37 \rightarrow S7$ $16 \rightarrow 23 \rightarrow S4$ $16 \rightarrow 25 \rightarrow S5$ $30 \rightarrow 45 \rightarrow S8$ $6 \rightarrow 9 \rightarrow S2$

So four input output bits of S-box $S3$ affects six different S-boxes on next round are $S2, S4, S5, S6, S7, S8$

9.) The given website is likely to be scam one with the below reasons.

1.) Too Good to be True deals.

for one of the products, the price is \$ 133.24. but the discounted price displayed is \$ 39.97 which is way too low for such good and expensive product. This can be a warning sign.

2.) The products on the website do not have any customer reviews or comments for it.

So this website is likely a scam.

3.) In the contact us section, there is no address or any phone number provided. Also there is

something as a website name instead of contact email address or a contact number which seems to be a fake website.

- 48.) If this website is put in urlvoid reputation tracker it says that the domain registration is done 2 months ago and also the server location, latitude/longitude det and many such details are so shown to be as unknown.