

ET2595 Network and System Security

Crypto

Assignment 1

(Date: 22th November 2023)

Gattupalli Monica

(moga20@student.bth.se)

(19991130-5002)

Task-1: Enigma Encoding

In task to we the enigma tools to convert the given plain text to cipher text by using the key.

Link to enigma tool <https://cryptii.com/pipes/caesar-cipher>.

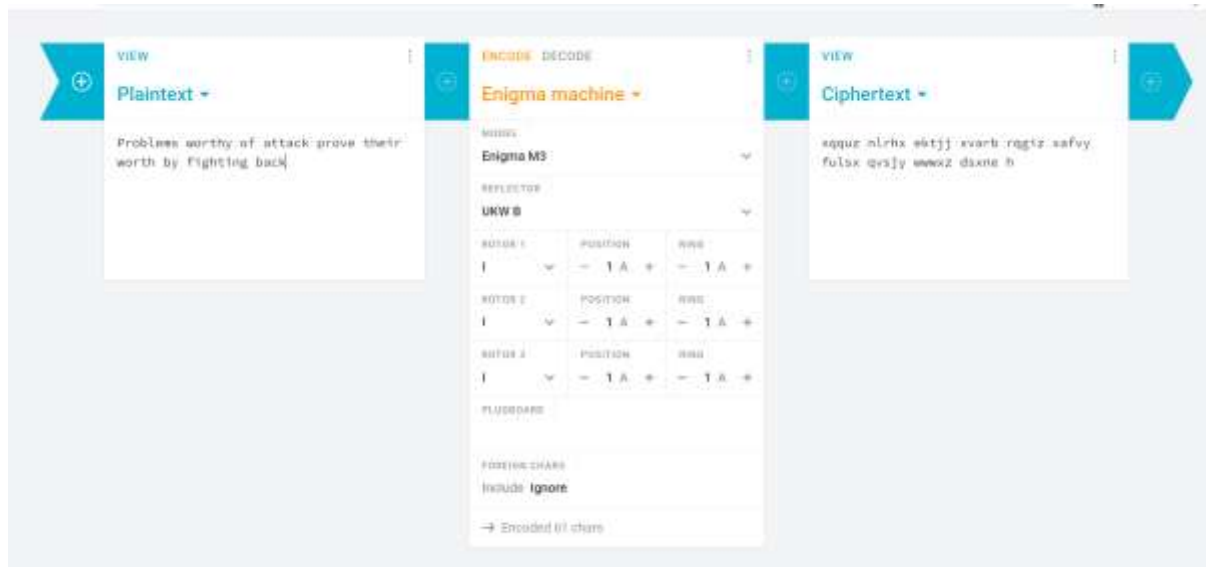


Figure-1: enigma encoding.

Task-2: Enigma Decoding

cipher text: “xqqz nlrhx ektjj xvarb rggiz xafvy fulsx qvsjy wwwxz dsxne h”

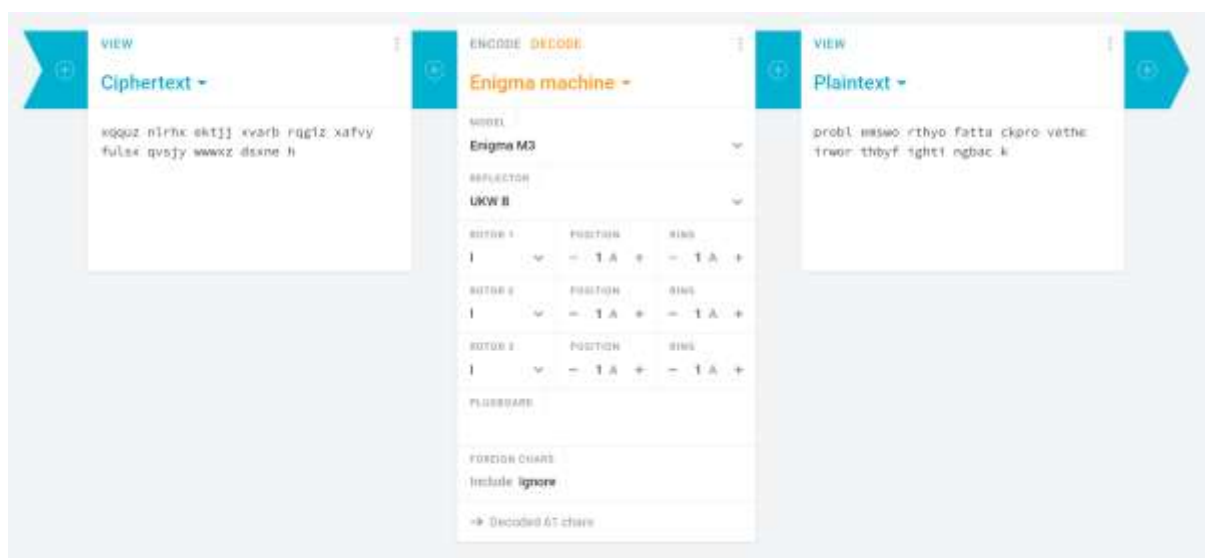


Figure-2: enigma decoding.

Plain text: “probl emswr rthyo fatta ckpro vethe irwor thbyf ighti ngbac k”

According to my personal number, the plain text, keys and the cipher are given for both the technique and the below are the tasks performed for the encryption and decryption

Task-3: Caesar cipher encryption

The task -3 is Caesar cipher encryption is performed, I need to encrypt the given plain text by using the key the below figure gives the plain text, key, and cipher text.

Assignment-7
Crypto Assignment

Name:- Monica Gattupalli
P-number:- 199911305002

Task-3 (Caesar Cipher)

Given text:- "Problems worthy of attack prove their worth by fighting back".

-Given key:- 119

Step-1 → Arranged according to the key.

P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10
A	B	C	D	E	F	G	H	I	J	K

A	B	C	D	E	F	G	H	I	J	K
11	12	13	14	15	16	17	18	19	20	21
L	M	N	O	P	Q	R	S	T	U	V

L	M	N	O
22	23	24	25
W	X	Y	Z

Du behöver inte vara raketforskare
för att fatta våra mobilabonnemang

Ingen bindningstid · Friä samtal inom Sverige · Går endast till Sverige

fello

Step II

by using formula;

$$C = [K + P] \bmod 26$$

C :- cipher, K = key, P = value of the alphabet

lets use the formula for "Problems"

"P"

$$\begin{aligned} C &= [119 + 15] \bmod 26 \\ &= 134 \bmod 26 \\ &= 4 \end{aligned}$$

So 4 is e in the alphabet so P is replaced with e P = E

"R"

$$C = [119 + 17] \bmod 26 = [136 \bmod 26] = 6$$

R is replaced with G

"O"

$$C = [119 + 14] \bmod 26 = [133 \bmod 26] = 3$$

O is replaced with D

Hälften sugar **inte alltid**

Hälsa
för

små
studenter

 storytel

"B"

$$C = [119 + 1] \bmod 26 = 120 \bmod 26 = 16$$

B is Replaced with q

"Z"

$$C = [119 + 11] \bmod 26 = 130 \bmod 26 = 0$$

Z is Replaced with A

"E"

$$C = [119 + 4] \bmod 26 = 123 \bmod 26 = 19$$

E is Replaced with t

"M"

$$C = [119 + 12] \bmod 26 = 131 \bmod 26 = 1$$

M is Replaced with B

"S"

$$C = [119 + 18] \bmod 26 = 137 \bmod 26 = 7 \text{ S Replaced h}$$

Hälften sugar

Hälften
för

inte alltid

priser
studenter

storytel

after following this formula for all we will get
the encrypted text is

"
egdqatbh ldgiwn du piiprz egdkt iwtg
ldgiw qn uavwizcv qprz".

Task-4: Caesar cipher decryption

The task -4 is Caesar cipher decryption is performed, I need to decrypt the given cipher text by using the key the below figures give the plain text, key, and cipher text.

Task-4 (Caesar cipher)

Cipher text :- "ndj sd edi wpkt id palph
qt gxvwi"

Key d = 119

Procedure to convert to plain text we use same process of task-3 but in reverse way.

find the alphabets in decoder side and match them

decrypt

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

Du behöver inte vara raketforskare för att fatta våra mobilabonnemang

Vägen är drömmen
För samtal om Sverige
Gå med till skolan

fello

Se alla erbjudanden
och fakta om fello

follow above process to all the letter in the cipher we will get plain text.

plain text :-

"you donot have to be always right"

Task-5: Caesar cipher Crack

In this we need to identify the key to decrypt the given plain text, so to that alphabets are moved towards right by one step until the correct plain text is identified.

Task-5

→ Caesar cipher Crack:-

In this, there is need in identifying the key so to find the key. The alphabets are moved the step of 1 toward Right. When ever we get the intellegable translation for the text that is considered as the key.

Given text:- "Jau cydt yi cixuhogjaydw mxoj Oek jayda Oek rusecu".

Identified Key:- 16 (So the A strat at the position of Q (16th)).

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

x	y	z	a	b	c	d	e	f	g	h	i	j
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

By following the process

plain text:- "The mind is everything what you think you become".

**Du behöver inte vara raketforskare
för att fatta våra mobilabonnemang**

Ingen bindningstid

Fria samtal inom Sverige

Öarnvänd surf sparar



Se alla erbjudanden
på fello.se/mobemat

fello

Task-6: Vigenère cipher encryption

The task-6 is Vigenère cipher encryption is performed, I need to encrypt the given plain text by using the key the below figure gives the plain text, key, and cipher text.

Task-6 (Vigenere cipher)

Given text:- "problems worthy of attack prove their worth by fighting back"

Given key:- n k f b s

Procedure:-

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

17	18	19	20	21	22	23	24	25
R	S	T	U	V	W	X	Y	Z

Key:- n k f b s
13 10 5 1 18

encoding-

PROBLEMS = c b t c d r w x
13 10 5 1 13 10 5

worthy = x g e d m z
3 10 5 1
1 18

of = g s
18 13

attack = k y u s p u
3
10 5 1 18 10

Hälften sugar inte alltid

after applying this technique to all the words.

The decrypted text

"cbtcdwax xgadmz gs kyuspu usgio
yiwvb bpjgr gz xvqmuaaq gbuu".

Task - 7 Vigenère cipher decryption

The task -7 is Vigenère cipher encryption is performed, I need to decrypt the given cipher text by using the key the below figures give the plain text, key, and cipher text.

Task-7 (Vigenere cipher)

Given text:- " V embdy x t u on cyf el
nfz k vx ysqux l vg c bt mg
a 0 y i w z "

key:- n k f b s
13 10 5 1 18

13 10 5 1 18 13 10 5 1 18 13 10 5 1 18 13 10
V c m b d y x t u on cyf t el

5 13 18 10 5 1 18 13 10 5 1 18 13 10 5 1 18 13
nfz k vx ysqux l vg c bt mg

a 0 y i w z
10 5 1 18 13 10

plain text:- "I shall not waste my days in
trying to prolong them."

Hälften sugar inte alltid
Häls för privat studenter
storytel