Laporan Tugas Seleksi IRK Mesin Enigma

Bernardus Willson K03 / 13521021

1. Pengertian Enigma

Enigma merupakan sebuah mesin enkripsi yang digunakan secara luas oleh Jerman pada masa Perang Dunia II. Mesin ini dirancang untuk merahasiakan komunikasi militer Jerman dengan cara mengubah huruf-huruf dalam sebuah pesan menjadi teks terenkripsi yang sulit dipecahkan. Sehingga jika pesan ingin dibaca oleh musuh, musuh tidak dapat mengetahui isi sebenarnya dari surat itu. Meskipun musuh memiliki Enigma ini, diperlukan konfigurasi yang tepat dan hanya diketahui oleh pihak Jerman untuk mendekripsi pesan tersebut.

2. Cara Kerja Enigma

Pertama-tama, kita perlu tahu komponen-komponen penting pada Enigma. Berikut adalah komponen-komponen pada mesin Enigma:

- a. Keyboard: Komponen ini digunakan untuk memasukkan huruf-huruf yang ingin dienkripsi atau didekripsi.
- b. Rotors: Enigma menggunakan sejumlah rotors yang dapat berputar. Setiap rotor memiliki huruf-huruf di sekitarnya dan kabel internal yang menghubungkan satu huruf dengan huruf lainnya. Rotors bertanggung jawab untuk mengganti huruf-huruf dalam pesan.
- c. Reflector: Reflector adalah komponen yang mengarahkan sinyal kembali ke rotors setelah melewati langkah-langkah enkripsi awal. Sinyal dipantulkan melalui reflector sebelum melalui rotors lagi untuk tahap selanjutnya.
- d. Plugboard: Plugboard adalah papan yang digunakan untuk menghubungkan pasangan huruf-huruf dengan kabel. Pengaturan pada plugboard memberikan substitusi awal sebelum sinyal melewati rotors.

Setelah memahami komponen-komponen Enigma, berikut adalah langkah-langkah enkripsi pada mesin Enigma:

- Posisikan rotors: Setiap rotor pada Enigma dapat diatur dalam berbagai posisi.
 Sebelum enkripsi dimulai, rotors harus dikonfigurasi ke dalam posisi awal yang ditentukan oleh kunci enkripsi.
- 2. Masukkan huruf: Ketika huruf pada plaintext dimasukkan melalui keyboard, sinyal elektrik melewati plugboard.

- 3. Posisi rotor bergerak: Setelah setiap huruf dimasukkan, rotor-rotor pada mesin Enigma akan berputar satu langkah. Ketika posisi rotor berada pada turnover, rotor sebelahnya akan ikut berputar satu langkah.
- 4. Substitusi plugboard: Sinyal yang keluar dari plugboard mengalami substitusi awal berdasarkan pengaturan pasangan huruf pada plugboard.
- 5. Enkripsi rotor: Sinyal yang keluar dari plugboard masuk ke rotor kanan, rotor tengah, lalu rotor kanan. Setiap rotor akan mengubah sinyal menjadi huruf yang berbeda berdasarkan konfigurasi kabel internal di dalam rotor tersebut.
- 6. Reflector: Setelah melewati rotors, sinyal mencapai reflector. Reflector mengarahkan sinyal kembali ke rotor kiri.
- 7. Enkripsi rotor terbalik: Sinyal kembali melewati rotor-rotor dalam urutan yang terbalik dari sebelumnya.
- 8. Substitusi plugboard: Sinyal yang keluar dari rotor akan kembali disubstitusi berdasarkan konfigurasi plugboard.
- 9. Hasil: Mesin akan mengeluarkan huruf-huruf yang sudah terenkripsi.
- 10. Ulangi langkah-langkah di atas: Setelah satu huruf dienkripsi, proses akan diulang untuk huruf-huruf berikutnya dalam pesan hingga seluruh pesan telah dienkripsi.

3. Contoh Enkripsi Enigma

Misalkan kita ingin mengenkripsi pesan "AKU" dengan konfigurasi rotor I, rotor II, rotor III, secara berurutan dari kiri, tengah, dan kanan. Posisi awal rotor adalah AAA dan plugboard tidak digunakan.

1. Posisi awal rotor adalah seperti berikut, paling kiri adalah reflektor UKW-B, kedua dari kiri adalah rotor I, ketiga dari kiri adalah rotor II, keempat dari kiri adalah rotor III, dan yang paling kanan adalah input/output:

Α	Υ	Α	E	Α	Α	Α	В	Α
В	R	В	K	В	J	В	D	В
C	U	C	М	C	D	C	F	C
D	Н	D	F	D	K	D	H	D
Ε	Q	Ε	L	Ε	S	Ε	J	Ε
F	S	F	G	F	1	F	L	F
G	L	G	D	G	R	G	С	G
Н	D	Н	Q	Н	U	Н	P	Н
1	P	I	V	I	X	1	R	1
J	X	J	Z	J	В	J	T	J
K	N	K	N	K	L	K	X	K
L	G	L	T	L	Н	L	V	L
M	О	M	О	М	W	M	Z	M
Ν	K	N	W	N	Т	N	N	N
N 0	K M	N O	W Y	N O	M	N O	Y	N O
								_
0	М	0	Υ	O	М	O	Υ	0
O P	M I	O P	Y H	O P	M C	O P	Y E	O P
O P Q	M I E	O P Q	Y H X	O P Q	M C Q	O P Q	Y E I	O P Q
O P Q R	M I E B	O P Q R	Y H X U	O P Q R	M C Q G	O P Q R	Y E I W	O P Q R
O P Q R	M I E B	O P Q R S	Y H X U	O P Q R S	M C Q G	O P Q R S	Y E I W G	O P Q R
O P Q R S	M I E B F Z	O P Q R S	Y H X U S	O P Q R S	M C Q G Z	O P Q R S	Y E I W G A	O P Q R S
O P Q R S T	M I E B F Z C	O P Q R S T	Y H X U S P	O P Q R S T	M C Q G Z N	O P Q R S T	Y E I W G A K	O P Q R S T
O P Q R S T U	M I E B F Z C	O P Q R S T U	Y H X U S P A	O P Q R S T U	M C Q G Z N P	O P Q R S T U	Y E I W G A K	O P Q R S T U
O P Q R S T U V	M I E B F Z C W V	O P Q R S T U V W	Y H X U S P A I B	O P Q R S T U V	M C Q G Z N P Y	O P Q R S T U V	Y E I W G A K M U	O P Q R S T U V

2. Ketika huruf "A" diketik, rotor kanan akan bergerak naik sekali sehingga posisi rotor berubah menjadi seperti ini:

nei	ubanı	nenjaui se	peri	1 11111.					
Α	Υ	Α	E	Α	Α		В	D	Α
В	R	В	K	В	J		С	F	В
C	U	C	M	С	D		D	Н	C
D	Н	D	F	D	K		E	J	D
Е	Q	E	L	E	S		F	L	E
F	S	F	G	F	1		G	С	F
G	L	G	D	G	R		Н	Р	G
Н	D	Н	Q	Н	U		I	R	Н
1	P	1	V	1	X		J	Т	I
J	X	J	Z	J	В		K	X	J
K	N	K	N	K	L		L	V	K
L	G	L	Т	L	Н		M	Z	L
M	O	N	1 0	M	W		N	N	М
N	K	N	W	N	Т		O	Υ	N
O	M	0	Y	О	М		P	E	O
P	1	P	Н	P	C		Q	1	Р
Q	E	Q	X	Q	Q		R	W	Q
R	В	R	U	R	G		S	G	R
S	F	S	S	S	Z		Т	Α	S
Т	Z	Т	P	Т	N		U	K	Т
U	С	U	ΙΑ	U	Р	,	V	M	U
٧	W	V	1	V	Υ	,	W	U	V
W	V	V	V B	W	F		X	S	W
X	J	X	R	X	V	,	Υ	Q	X
Υ	Α	Υ	С	Υ	О		Z	О	Υ
Z	Т	Z	J	Z	Ε		Α	В	Z

3. Input huruf "A" kemudian dikirim menuju ke rotor paling kanan. Huruf masuk lalu dikonversi menjadi huruf "D".

Α	Υ	Α	E	Α	Α	В	D 4	Α
В	R	В	K	В	J	С,	F	В
C	U	C	M	C	D	D	Н	C
D	Н	D	F	D	K	Ε	J	D
Ε	Q	Ε	L	Ε	S	F	L	E
F	S	F	G	F	1	G	С	F
G	L	G	D	G	R	Н	P	G
Н	D	Н	Q	Н	U	1	R	Н
1	P	1	V	1	X	J	T	1
J	X	J	Z	J	В	K	X	J
K	N	K	N	K	L	L	V	K
L	G	L	T	L	Н	М	Z	L
М	O	М	О	M	W	Ν	N	M
Ν	K	Ν	W	N	Т	O	Υ	N
O	М	O	Υ	O	М	Р	E	O
Р	1	Р	Н	P	C	Q	I	P
Q	Ε	Q	X	Q	Q	R	W	Q
R	В	R	U	R	G	S	G	R
S	F	S	S	S	Z	Т	A	S
Т	Z	Т	P	T	N	U	K	Т
U	C	U	Α	U	P	V	M	U
V	W	V	1	V	Υ	W	U	V
W	V	W	В	W	F	X	S	W
X	J	X	R	X	V	Υ	Q	X
Υ	Α	Υ	С	Υ	O	Z	0	Υ
Z	T	Z	J	Z	Ε	Α	В	Z

4. Huruf "D" dari rotor kanan dikirim menuju ke rotor tengah. Huruf masuk lalu dikonversi menjadi huruf "D".

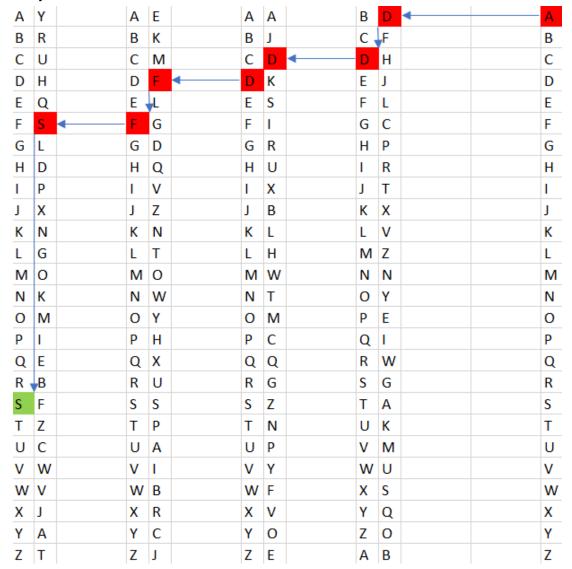
uik	OHIV	ersi menjad	יוו וג	urui	υ.							
Α	Υ		Α	Ε		Α	Α		В	D	◀	Α
В	R		В	K		В	J		С,	F		В
C	U		C	М		C	D	◀	D	Н		C
D	Н		D	F		D	K		Ε	J		D
Ε	Q		Ε	L		Ε	S		F	L		Ε
F	S		F	G		F	1		G	C		F
G	L		G	D		G	R		Н	Р		G
Н	D		Н	Q		Н	U		1	R		Н
1	Р		1	V		1	X		J	Т		1
J	X		J	Z		J	В		K	X		J
K	N		K	N		K	L		L	V		K
L	G		L	Т		L	Н		М	Z		L
M	О		М	O		М	W		Ν	N		M
N	K		N	W		Ν	Т		O	Υ		N
O	М		O	Υ		O	М		Р	Ε		О
P	1		Р	Н		Р	С		Q	1		Р
Q	Е		Q	X		Q	Q		R	W		Q
R	В		R	U		R	G		S	G		R
S	F		S	S		S	Z		Т	Α		S
Т	Z		Т	Р		Т	N		U	K		Т
U	С		U	Α		U	Р		V	М		U
٧	W		V	1		V	Υ		W	U		V
W	V		W	В		W	F		X	S		W
X	J		Χ	R		Χ	V		Υ	Q		X
Υ	Α		Υ	С		Υ	O		Z	0		Υ
Z	Т		Z	J		Z	Ε		Α	В		Z

5. Huruf "D" dari rotor tengah dikirim menuju ke rotor kiri. Huruf masuk lalu dikonversi menjadi huruf "F".

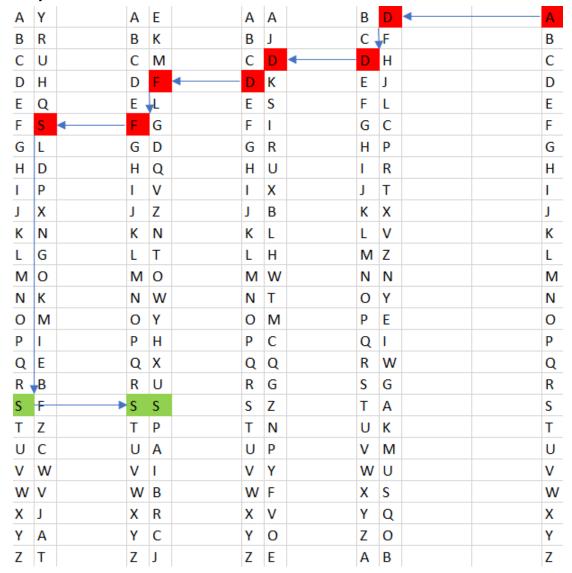
A A A B B D A

Α	Υ	Α	Е		Α	Α		В	D	◀	Α
В	R	В	K		В	J		С,	F		В
C	U	C	М		C	D	◀	D	Н		C
D	Н	D	F	◆	D	K		Е	J		D
E	Q	Εų	L		Е	S		F	L		E
F	S	F	G		F	1		G	С		F
G	L	G	D		G	R		Н	Р		G
Н	D	Н	Q		Н	U		1	R		Н
1	P	1	V		1	X		J	Т		1
J	X	J	Z		J	В		K	X		J
K	N	K	N		K	L		L	V		K
L	G	L	Т		L	Н		М	Z		L
M	O	М	O		М	W		Ν	N		M
Ν	K	N	W		Ν	Т		O	Υ		N
0	М	O	Υ		O	М		Р	Е		O
P	1	Р	Н		Р	C		Q	1		P
Q	Е	Q	X		Q	Q		R	W		Q
R	В	R	U		R	G		S	G		R
S	F	S	S		S	Z		Т	Α		S
Т	Z	Т	Р		Т	N		U	K		Т
U	C	U	Α		U	P		V	М		U
V	W	V	1		V	Υ		W	U		V
W	V	W	В		W	F		X	S		W
X	J	X	R		X	V		Υ	Q		X
Υ	Α	Υ	C		Υ	O		Z	O		Y
Z	Т	Z	J		Z	Ε		Α	В		Z

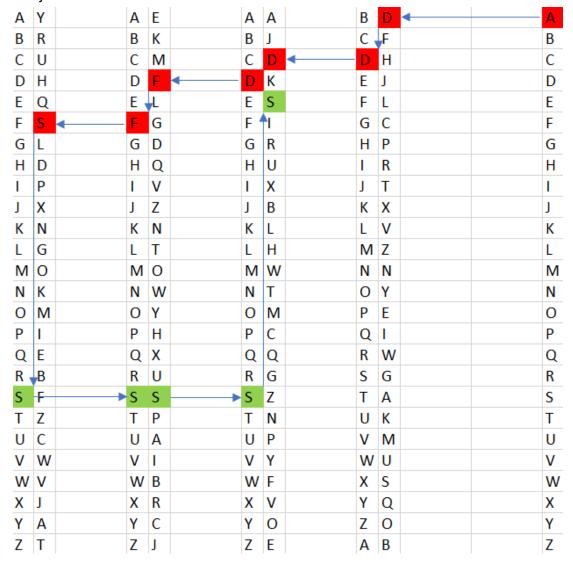
6. Huruf "F" dari rotor kiri dikirim menuju ke reflektor. Huruf masuk lalu dikonversi menjadi huruf "S".



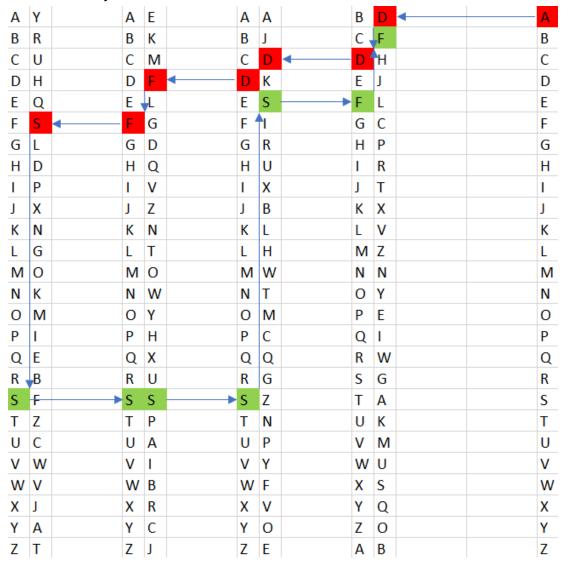
7. Huruf "S" dari reflektor dikirim menuju ke rotor kiri. Huruf masuk lalu dikonversi menjadi huruf "S".



8. Huruf "S" dari rotor kiri dikirim menuju ke rotor tengah. Huruf masuk lalu dikonversi menjadi huruf "S".



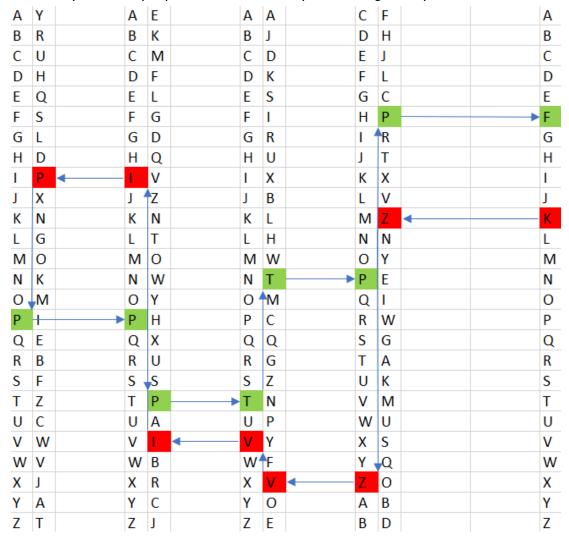
9. Huruf "S" dari rotor tengah dikirim menuju ke rotor kanan. Huruf masuk lalu dikonversi menjadi huruf "F".



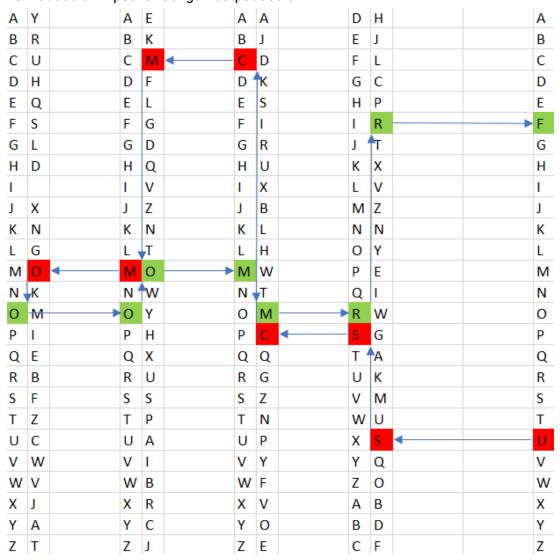
10. Huruf "F" dari rotor kanan dikirim menuju ke output menjadi huruf "B".

Α	Υ		Α	E		Α	Α		В	D	◀	Α
В	R		В	K		В	J		С,	F	-	В
С	U		С	М		С	D	◀	D 4	Н		С
D	Н		D	F	•	D	K		Ε	J		D
Ε	Q		Ε,	L		Ε	S	-	F	L		Е
F	S	◀	F	G		F ⁴	ı		G	С		F
G	L		G	D		G	R		Н	P		G
Н	D		Н	Q		Н	U		L	R		Н
1	Р		1	V		I	Х		J	T		I
J	X		J	Z		J	В		K	Χ		J
K	N		K	Ν		K	L		L	٧		K
L	G		L	Т		L	Н		М	Z		L
M	O		М	O		М	W		Ν	N		М
N	K		Ν	W		Ν	Т		O	Υ		Ν
0	М		O	Υ		0	М		Р	E		O
P	I		Р	Н		P	C		Q	I		P
Q	Ε		Q	X		Q	Q		R	W		Q
R	В		R	U		R	G		S	G		R
S	Г	-	S	S	-	S	Z		Т	Α		S
Т	Z		Т	Р		Т	N		U	K		T
U	C		U	Α		U	Р		٧	М		U
V	W		V	1		٧	Υ		W	U		V
W	V		W	В		W	F		X	S		W
X	J		X	R		Χ	V		Υ	Q		X
Υ	Α		Υ	C		Υ	0		Z	0		Υ
Z	Т		Z	J		Z	Ε		Α	В		Z

11. Untuk input-input lain kurang lebih caranya sama, namun jangan lupa bahwa rotor selalu berputar setiap input. Berikut adalah input "K" dengan output adalah "F".



12. Berikut adalah input "U" dengan output adalah "F".

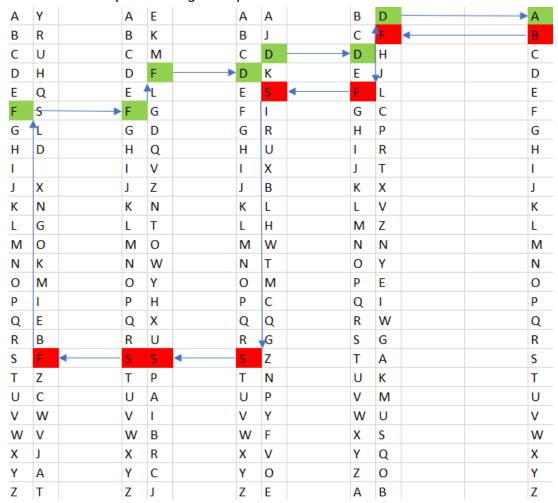


13. Kesimpulannya, kata "AKU" jika dienkripsi akan menghasilkan kata "BFF".

4. Contoh Dekripsi Enigma

Cara kerja dekripsi pada mesin ini sama dengan cara kerja enkripsinya dikarenakan enkripsi enigma bersifat simetris, yang berarti bahwa pengaturan yang sama dapat digunakan untuk mengenkripsi atau mendekripsi pesan. Misalkan kita ingin mendekripsi pesan "BFF" dengan konfigurasi rotor I, rotor II, rotor III, secara berurutan dari kiri, tengah, dan kanan. Posisi awal rotor adalah AAA dan plugboard tidak digunakan.

1. Berikut adalah input "B" dengan output adalah "A".



2. Berikut adalah input "F" dengan output adalah "K".

		•			-	•						
Α	Υ		Α	Ε		Α	Α		C	F		Α
В	R		В	K		В	J		D	Н		В
С	U		С	M		С	D		Е	J		С
D	Н		D	F		D	K		F	L		D
Ε	Q		Ε	L		Ε	S		G	C		
F	S		F	G		F	I		Н	Р	←	E F
G	L		G	D		G	R		L	R		G
Н	D		Н	Q		Н	U		J	Т		Н
l		-	1	٧		L	X		K	Χ		1
J	X		J	Z		J	В		L	٧		J
K	N		K	N		K	L		М	Z	-	K
L	G		L	Т		L	Н		N '	N		L
M	0		М	0		М	W		ο,	Υ		M
N	K		N	W		N	Т	←	Р	Ε		N
0	М		0	Υ		0	М		Q	l.		O
Р	1	◀	Р	Н		Р	С		R	W		Р
Q	Ε		Q ⁴	Χ		Q	Q		S	G		Q
R	В		R	U		R	G		Т	Α		R
S	F		S	S		s,	Z		U	K		
Т	Z		Т	Р	←	Т	N		٧	М		S T
U	С		U,	Α		U	Р		W	U		U
٧	W		٧	I	-	٧	Υ		Χ	S		V
W	٧		W	В		w,	F		Υ	Q		W
X	J		Χ	R		Χ	٧	-	Z	0		X
Υ	Α		Υ	С		Υ	0		Α	В		Υ
Z	Т		Z	J		Z	Ε		В	D		Z

3. Berikut adalah input "F" dengan output adalah "U".

Α	Υ		Α	Ε		Α	Α		D	Н		Α
В	R		В	K		В	J		Ε	J		В
С	U		С	M		С	D		F	L		С
D	Н		D ⁴	F		D	K		G	C		D
Ε	Q		Ε	L		Ε	S		Н	Р		
F	S		F	G		F	L		1	R	←	E F
G	L		G	D		G	R		J	Т		G
Н	D		Н	Q		Н	U		K	Х		Н
1			L	٧		L	Χ		L	٧		L
J	Χ		J	Z		J	В		М	Z		l J
K	N		K	N		K	L		N	N		K
L	G		L	Т		L	Н		O	Υ		L
М	0	-	М	О	•	М	W		Р	Ε		М
	A						<u> </u>		_	١.		
N '	K		N,	W		N '	T		Q١	И		N
N '	K M	◀	N v	W Y		N '	T M	◀		W		0
		◀										
0	М	◀	0	Υ		ο,	М	←	R	W		0
O P	M I	4	O P	Y H		O , P	M C	←	R S	W G		O P Q R
O P Q	M I E	◄	O P Q	Y H X		O , P Q	M C Q	*	R S T	W G A		O P Q R
O P Q R	I E B	4	O P Q R	Y H X U		O , P Q R	M C Q G	←	R S T U	W G A K M		O P Q R
O P Q R	M I E B	4	P Q R S	Y H X U S		O , P Q R S	M C Q G	*	R S T U	W G A K M		O P Q R
O P Q R S T	I E B F Z	4	P Q R S	Y H X U S		O , P Q R S	M C Q G Z	←	R S T U V	W G A K M	-	O P Q R S
O P Q R S T U	I E B F Z	◄	P Q R S T	Y H X U S P		O , P Q R S T U	M C Q G Z N	*	R S T U V W	W G A K M U S	-	O P Q R S T
O P Q R S T U V	I E B F Z C	4	P Q R S T U	Y H X U S P A		O , P Q R S T U	M C Q G Z N P	←	R S T U V X Y	W G A K M U S	-	O P Q R S T U V
O P Q R S T U V	I E B F Z C W		P Q R S T U V	Y H X U S P A I B		O , P Q R S T U V W	M C Q G Z N P Y	•	R S T U V W X Y	W G A K M U S Q O	-	O P Q R S T U V

5. Hasil program dengan enigma di internet

Enigma Ma	achine Simulator		
-Initialization Rotors:	[I-II-III	-Encoding	Rotor ▼ Rotor ▼ Rotor ▼ Rotor Positions K E T Plugboard Configuration
Rotor Start:	KET		1
Rings:	AAA	Type Message Here:	3 -
Plugboard:		ENIGMA	4
	Set from passkey	© ₂	5
To learn more about th Engima. You can also Simulator.	e <u>Enigma Machine</u> , try using the <u>Paper</u> read the <u>source code</u> used by this Enigma	Read Output Here:	7
0 -	Proper Entire Machine § All Internal Communications and Section 1997 Address 1997 A	JVEFTI	10
		☑ Preserve spacing	Text Input ENIGMA
		Send to Twitter: 🤣	Ciphertext JVEFTI
	A Supposed American Sept. (Contract Contract Con		
	I should make a place to produce the state of the state o		Encrypt
Enigma M	lachine Simulator		
by Mike Koss		-Encoding-	Rotor Configurations Rotor III ▼ Rotor II ▼ Rotor I ▼
Enigma M by Mike Koss Initialization Rotors:		-Encoding	Rotor Configurations Rotor
by Mike Koss Initialization	III-II-I	Encoding R Q	Rotor Configurations Rotor III Rotor II Rotor I Rotor II Rotor III Roto
oby Mike Koss Initialization Rotors:	III-II-I	I R Q Type Message Here:	Rotor Configurations Rotor III Rotor II Rotor Positions Ro
Plnitialization Rotors: Rotor Start	III-II-I : IRK AAA	I R Q	Rotor Configurations Rotor III Rotor II Rotor I Rotor II Rotor Positions I
-Initialization Rotors: Rotor Start Rings:	III-II-I : IRK AAA	I R Q Type Message Here:	Rotor Configurations Rotor III Rotor II Rotor I Rotor II Rotor Positions I
Plugboard:	III-II-I : IRK AAA Set from passkey	I R Q Type Message Here:	Rotor Configurations Rotor III Rotor II Rotor I Rotor II Rotor Positions Rotor Positions Rotor II Rotor II Rotor Positions Rotor P
Plugboard:	III-II-I : IRK AAA	I R Q Type Message Here:	Rotor Configurations Rotor III Rotor II Rotor I Rotor Positions Rotor Positions Rotor II Rotor I Rotor Positions
Initialization Rotors: Rotor Start Rings: Plugboard: To learn more about Engima. You can als	III-II-I : IRK AAA Set from passkey the Enigma Machine, try using the Paper	Type Message Here: ENIGMA	Rotor Configurations Rotor III
Initialization Rotors: Rotor Start Rings: Plugboard: To learn more about Engima. You can als	III-II-I : IRK AAA Set from passkey the Enigma Machine, try using the Paper	Type Message Here: ENIGMA Read Output Here:	Roter Configurations
Initialization Rotors: Rotor Start Rings: Plugboard: To learn more about Engima. You can als	III-II-I : IRK AAA Set from passkey the Enigma Machine, try using the Paper or read the source code used by this Enigma	Type Message Here: ENIGMA Read Output Here: SEREVD	Rotor Configurations
Initialization Rotors: Rotor Start Rings: Plugboard: To learn more about Engima. You can als	III-II-I : IRK AAA Set from passkey the Enigma Machine, try using the Paper	Type Message Here: ENIGMA Read Output Here: SBREVD Preserve spacing	Rotor Configurations

