Nama : Puty Syalima

NIM ; 1811522014

Kelas : 02

Tanggal : Rabu/18 November 2020

Tugas Keamanan Sistem Informasi
Playfair Cipher

1. Lakukan enkripsi dan dekripsi Playfair Cipher pada plaintext:
   a. Jurusan Sistem Informasi
   b. Fakultas Teknologi Informasi

   Dengan kunci "NAMA PANGGILAN ANDA"

   Jawaban :

   Key : "PUTY"
   Plaintext 1 : "JURUSAN SISTEM INFORMASI"
   Plaintext 2 : "FAKULTAS TEKNOLOGI INFORMASI"

   Langkah-Langkah :

   1. Buat tabel 5x5 yang akan diisi oleh huruf alphabet.
   2. Tentukan key, key tidak ada huruf yang sama ("PUTY").
   3. Masukkan key pada tabel mulai dari baris paling atas, kolom paling kiri.
   4. Masukkan sisa huruf sesuai urutan alphabet.
   5. Perluas tabel dengan menambahkan baris ke-6 dan kolom ke-6.
   6. Pada plaintext ganti huruf J dengan huruf I, tulis pesan dalam pasangan huruf.
   7. Jika ada pasangan huruf yang sama sisipkan Z di tengahnya.
   8. Jika jumlah huruf ganjil, tambahkan Z di akhir.

   Tabel 5x5 :

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

Tabel 6x6 :

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

Plaintext 1 : IU RU SA NS IS TE MI NF OR MA SI (Jumlah huruf genap)
Plaintext 2 : FA KU LT AS TE KN OL OG IZ IN FO RM AS IZ (Jumlah huruf ganjil)

Algoritma Enkripsi & Dekripsi

Lakukan enkripsi Playfair Cipher dengan menyesuaikan plaintext yang telah disamarkan dan kita sesuaikan dengan tabel playfair 6 x 6 yang telah dibuat dengan ketentuan sebagai berikut :

1. Jika ada 2 huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (pada kunci yang telah diperluas).
2. Jika ada 2 huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang telah diperluas).
3. Jika ada 2 huruf tidak pada baris yang sama atau kolom yang sama, maka bentuk pola segiempat, dan gantikan huruf dengan huruf di baris yang sama pada sudut yang berlawanan.

Proses Enkripsi & Dekripsi

a. Plaintext Jurusan Sistem Informasi

Enkripsi

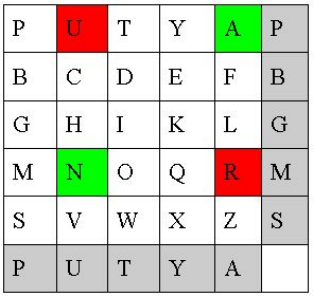
P	U	T	Y	A	P
B	C	D	E	F	B
G	H	I	K	L	G
M	N	O	Q	R	M
S	V	W	X	Z	S
P	U	T	Y	A	

I U => H T

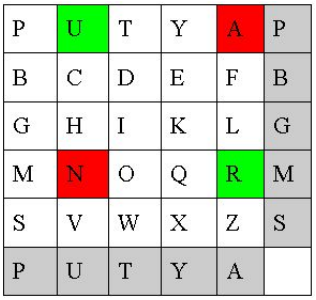
Dekripsi

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

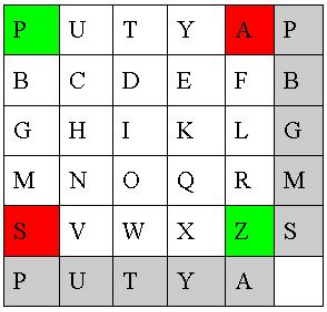
H T => U I



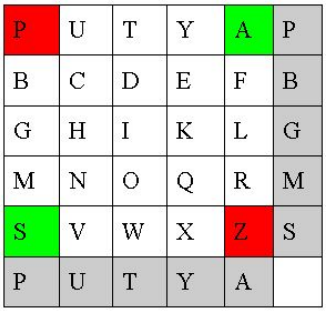
R U => N A



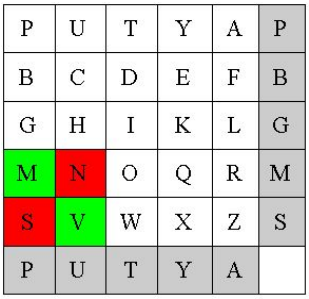
N A => R U



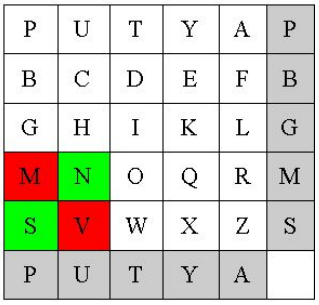
S A => Z P



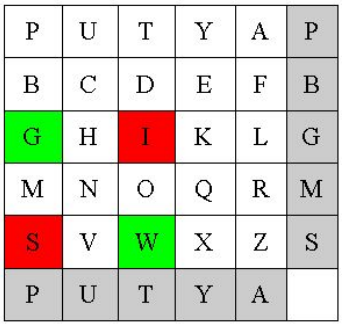
Z P => S A



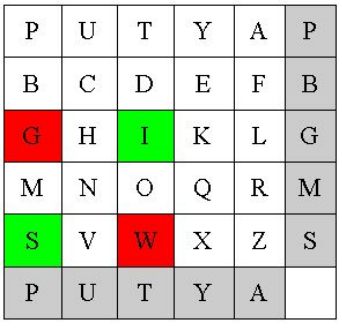
N S => M V



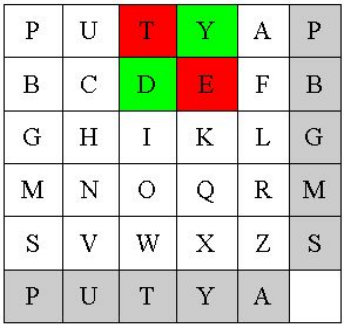
M V => N S



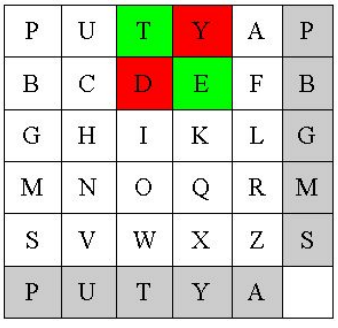
I S => G W



G W => I S



T E => Y D



Y D => T E

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

M I => O G

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

O G => M I

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

N F => R C

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

R C =>N F

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

O R => Q M

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

Q M => O R

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

M A => R P

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

R P => M A

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

S I => W G

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

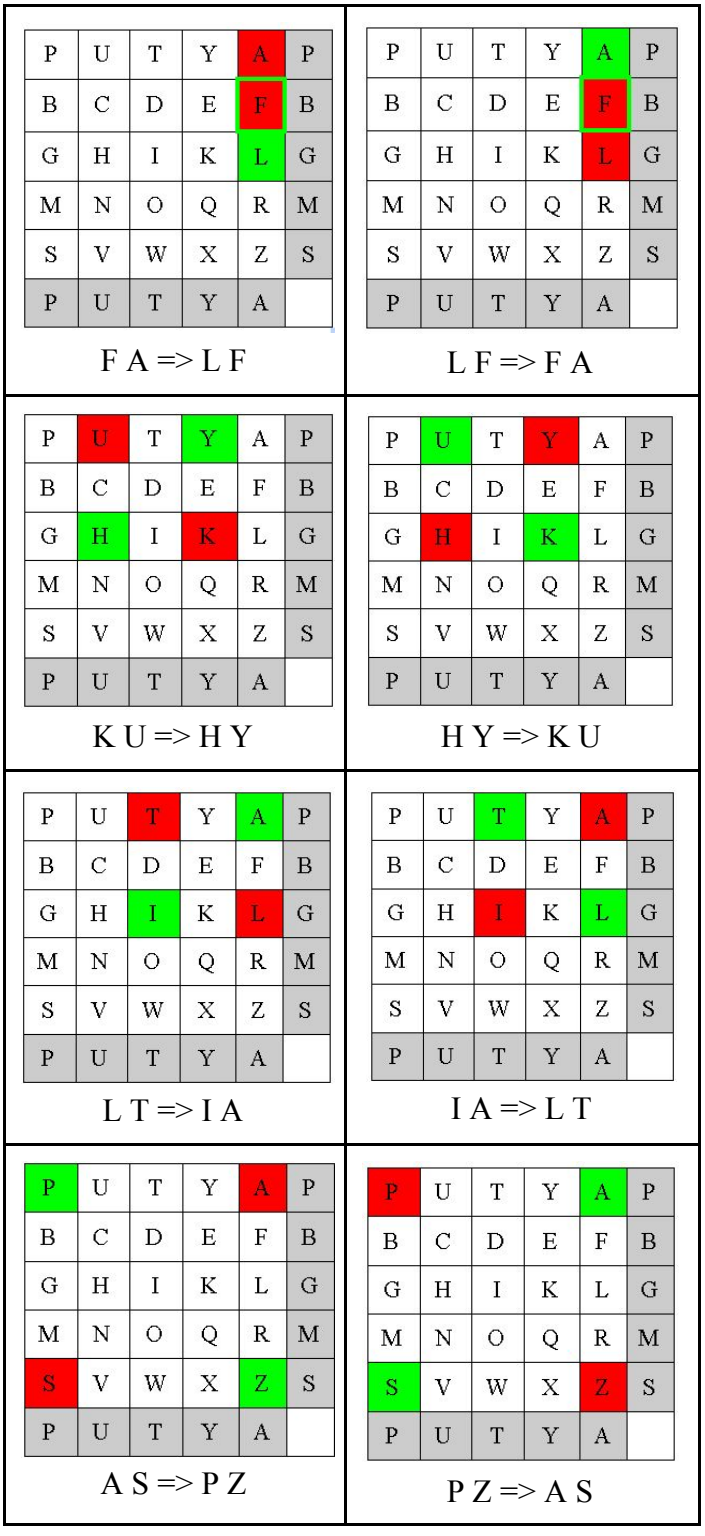
W G => S I

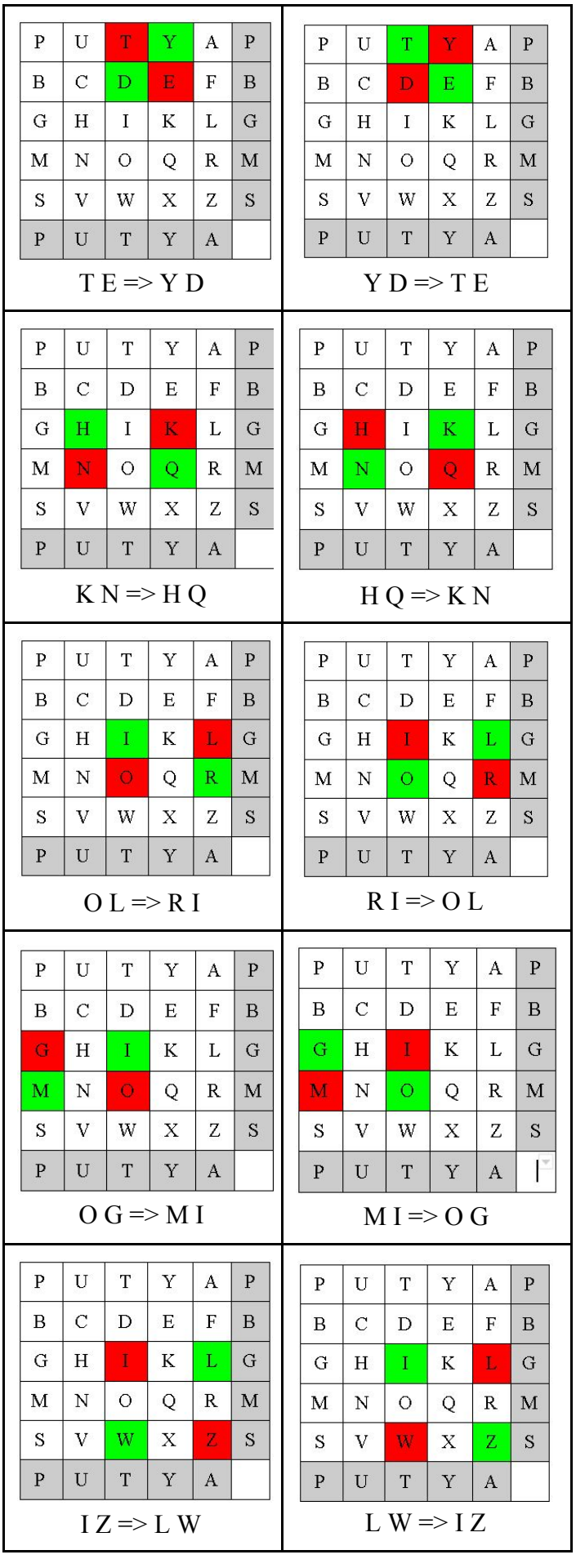
Hasil Enkripsi :
IURUSAN SISTEM INFORMASI => HTNAZPM VGWYDO GRCQMRPWG

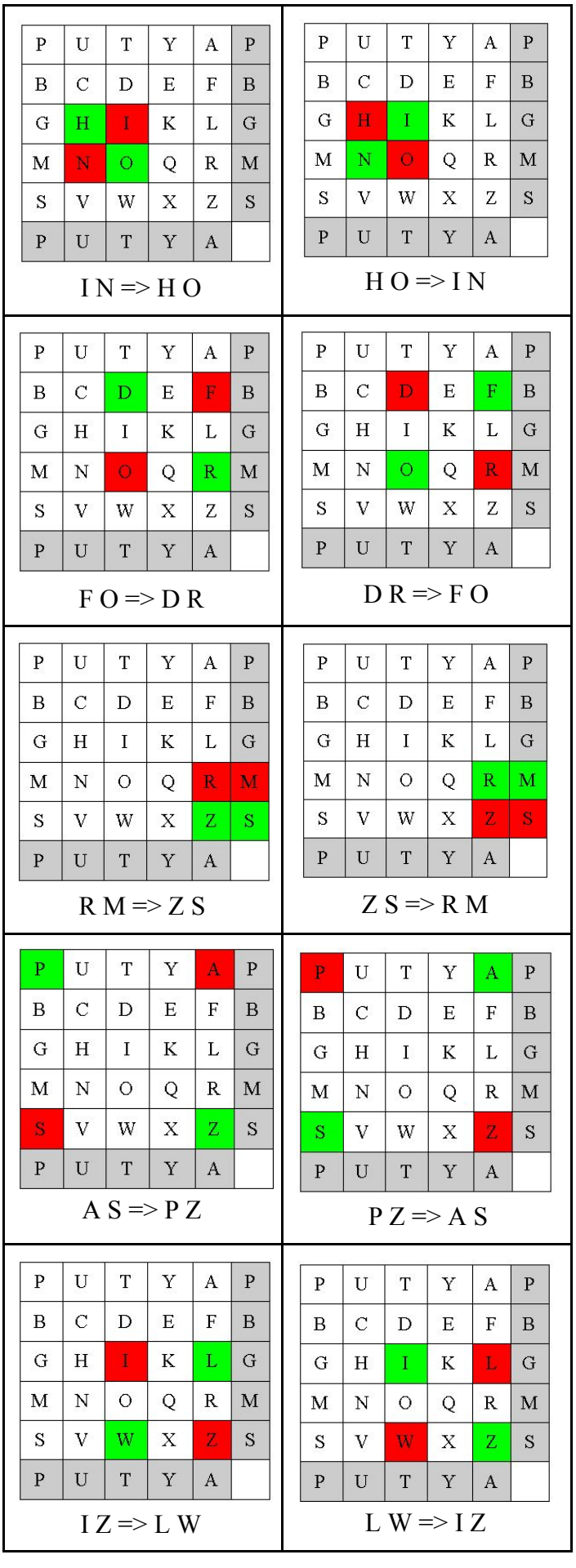
Hasil Dekripsi :
HTNAZPM VGWYDO GRCQMRPWG => IURUSAN SISTEM INFORMASI

(Terbukti)

b. Plaintext Fakultas Teknologi Informasi




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


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

Hasil Enkripsi :
FAKULTAS TEKNOLOGIZ INFORMASIZ => LFHYIAPZ YDHQRIMILW HODRZSPZLW

Hasil Dekripsi :
LFHYIAPZ YDHQRIMILW HODRZSPZLW => FAKULTAS TEKNOLOGIZ INFORMASIZ

(Terbukti)