Playfair

Playfair encryption algorithm principle

First: A polybius square consisting (5*5 character array consisting of keywords) of five rows and five columns is drawn and contains the key phrase in addition to the remaining letters of the alphabet (provided that they are not included in the key phrase).Since the letters of the English language number 26 and the number of cells in the square is 25 cells, the letters (i,j) are combined or the (q) is excluded due to its scarcity.

Second: We divide the explicit text into pairs and put two letters together according to the conditions:

If the pairs consist of the same two letters (or one letter remains at the end), then the letter (x) is added between the similar letters or at the end

For example,

1- the balloon first turns it into four pairs of letters,

ba lx lo on.

2- the ali , first turns it in to two pairs of letters, al ix

- If the two letters fall in the same row of the square, then each letter is replaced by the letter to its right (with the possibility of rotating to the left if necessary).
- If the two letters fall into the same column of the square, each letter is replaced by the letter directly below it (with the possibility of rotating upwards if necessary).
- Otherwise, each letter is replaced by the letter in the same row and column as the second letter.

Example:

Key : MONARCHY

Plaintext: instruments

The Algorithm consists of 2 steps:

1-Generate the key Square(5×5):

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

2- split PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz‘

Rules for Encryption:

If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

Example:

Diagraph: "me"

Encrypted Text: cl

Encryption:

m -> c

e -> l

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

If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

Example:

Diagraph: "st"
Encrypted Text: tl
Encryption:
s -> t
t -> l

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

If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Example:

Diagraph: "nt"
Encrypted Text: rq
Encryption:
n -> r
t -> q

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

Playfair

Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:
- i -> g
- n -> a
- s -> t
- t -> l
- r -> m
- u -> z
- m -> c
- e -> l
- n -> r
- t -> q
- s -> t
- z -> x

in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

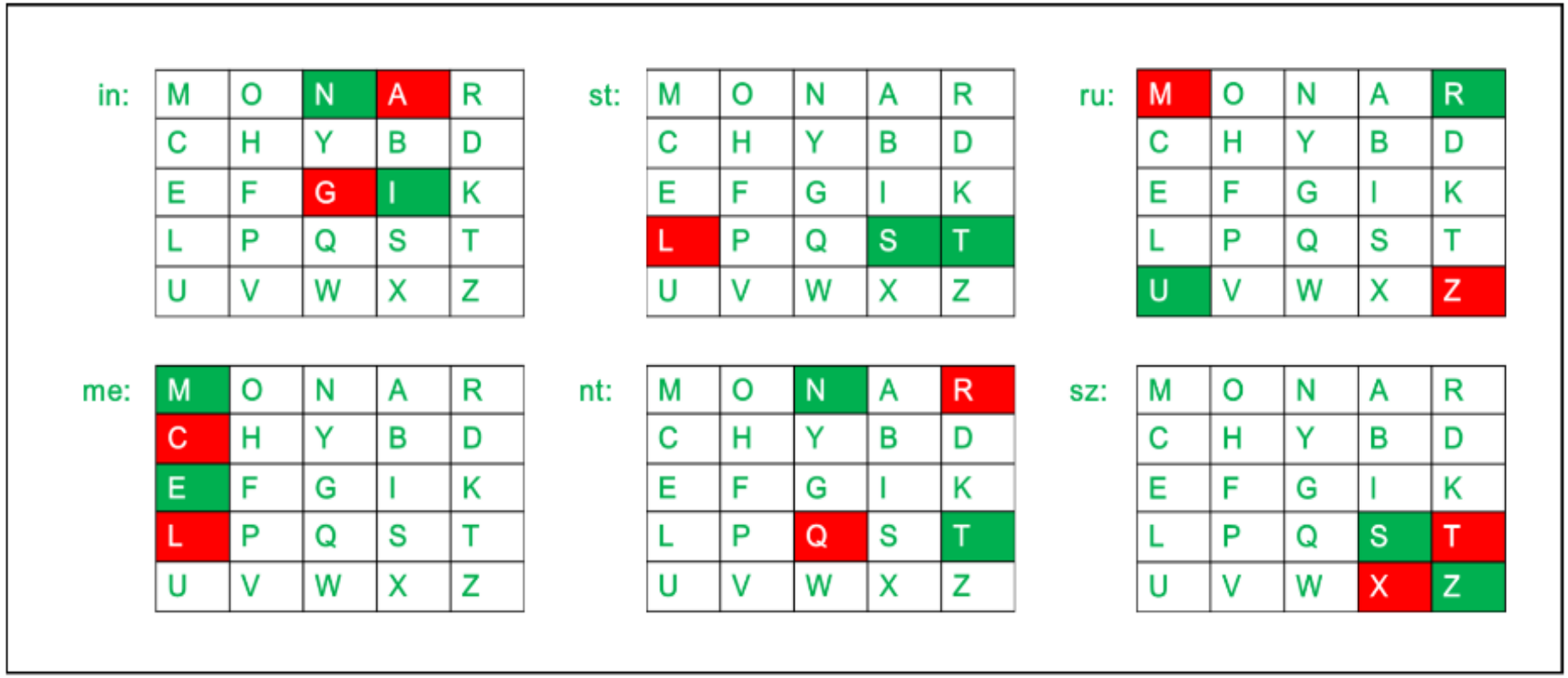
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Playfair

CipherText: "gatlmzclrqtx"

After Split: 'ga' 'tl' 'mz' 'cl' 'rq' 'tx‘

Plain Text: "gatlmzclrqtx"
Decrypted Text: instrumentsz
Decryption:
(red)-> (green)
ga -> in
tl -> st
mz -> ru
cl -> me
rq -> nt
tx -> sz



Playfair Cipher: Encryption

1: If both letters are in the same row, replace them with the letter on the right of the letter. If the letter is on the end, go back to the start of the same row and use the letter to replace with the end letter.

2. If both of the letters are in the same column, replace them with the letter below them. If the letter is on the bottom, go back to the top of the column and use the letter to replace with the bottom letter.

3. If neither of the letters are in the same column nor same row, imagine creating a rectangle with two letters on opposite corners, write down the other two letters on the other corners of the rectangle.

Playfair Cipher: Encryption

PUZZLE

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

THE MEETING IS AT TREFFOREST

THEMEXETINGISATXTREFXFOREST

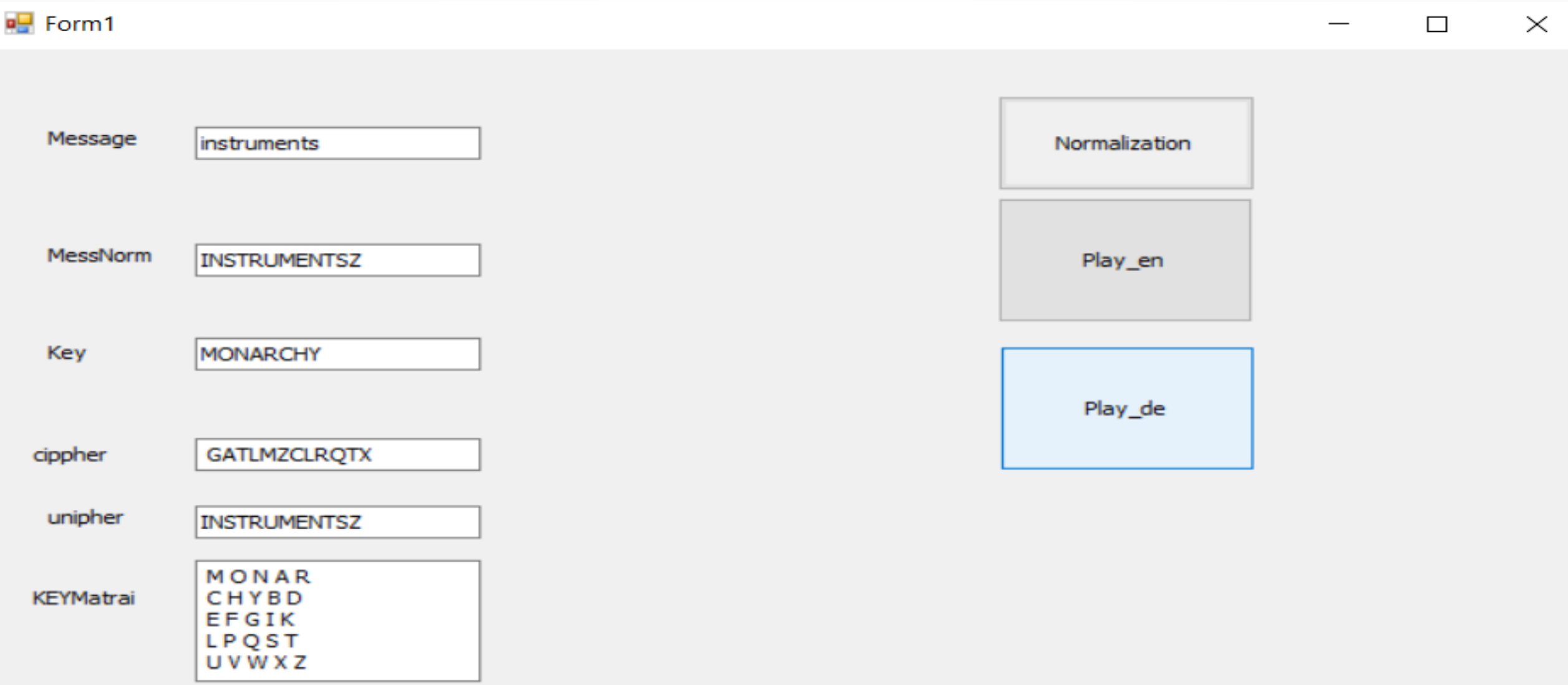
Playfair Cipher: Encryption

THEMEXETINGISATXTREFXFORESTX

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

Plaintext	TH	EM	EX	ET	IN	GI	SA	TX	TR	EF	XF	OR	ES	TX
Method	3	2	3	3	3	1	3	1	3	2	3	1	2	1
Encryption	VG	FS	LY	PY	GQ	HK	NF	VY	XN	FM	YD	QS	FY	VY

Playfair


Form1
Message
instruments
MessNorm
INSTRUMENTSZ
Key
MONARCHY
cippher
GATLMZCLRQTX
unipher
INSTRUMENTSZ
KEYMatrai
M O N A R
C H Y B D
E F G I K
L P Q S T
U V W X Z
Normalization
Play_en
Play_de