

ЗАШТИТА ПОДАТАКА

Симетрични алгоритми заштите

увод у криптографију

Zadatak

- Poruku “racunarskatehnikaiinformatika” šifrovati šifrom “zastita”
- Istu poruku šifrovati sada uz upotrebu autokey poboljšanja Vigenère metode.
- Napomena: koristiti 26 slova engleske abecede.

Rešenje

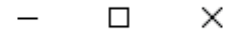
		Plaintext																									
		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Key	a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	e	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
	f	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
	g	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
	h	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
	i	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	H
	j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	z	Z	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

Rešenje

- Ključ: zastita
- Poruka: racunarskatehnikaiinformatika
- Šifrovana poruka:
qaunvtrrksmmanhksbqgfnretbbkz
- Auto key: zastitaracunarskatehnikaiinfo
- Šifrovana poruka:
qaunvtrjkcnrheavabmvswebmibvpo

Primer kriptanalize

Cryptanalysis Of Vigenere Algorithm



Visualization of Cryptanalysis of Vigenere cipher

Input here English text:

The city has long been named fashion capital of the world and the world's design capital thanks to several international events and fairs, including Milan Fashion Week and the Milan Furniture Fair, which are currently among the world's biggest in terms of revenue, visitors and growth. It hosted two Universal Expositions. The city hosts numerous cultural institutions, academies and universities, with eleven percents of the national total enrolled students. Milan is the destination of eight million overseas visitors every year, attracted by its museums and art galleries that boast some of the most important collections in the world, including major works by Leonardo da Vinci.

Type key here:

Ciphertext:

khfrwfilyjlbqunoileazhrrkwfzoafobsxycoswvqgspcdnqrfriufryggpowgxnppdudejkhngyedsqvruoxsrr
vradhuyryceihbfcelufnlfesracuqlbswmjmsdgtsslernoznxfvmvoozyppeigxfqpegiwulqtkvctueuszdpw
mbqufriufryggnskevsglbfovkjossushorsvwwfyvqmjqifagxfzturgfohrnohqwhovqrlradacmrzoavhtogg
kyurgfcrsdeeriemyjkuedzuxwrzthwwaxwyaqhaouwyedhqwhovqzvtvhgixfvlryszzipteawgapxfvnnwwa
xejkogdzqxvmclrggfehctfpwxkrjgtuhrqcxgeaglczyjczguwauvpgfnbysdcijjvwwfyvqvrumkoeprtguo
odibsyvwyewclmfdpbkvraxayosdsiqkhnwpakwrjzohcrdlcdofwwyzspkaawqavpcttvrbesryejrfxnmltlh
gwzqqyaoezcduwzplrrbmbhmuailbos

ENCRYPT
PLAINTEXT

START
CRYPTANALYSIS

GO BACK

Primer kriptanalize

Visualization of Cryptanalysis of Vigenere cipher

First, we have to find key length. We guess values from 2 to 20.

If key length is n , then every n 'th letter is encrypted by the same letter.

For every possible key length we calculate Index Of Coincidence which is measure of English-likeliness of sequence.

Message:

KHRFWFILYJLBQUNOILEAZHRRKWFZOAFBSXYC
OSWVQGSPCDNQRFRIUFRYGGPOWGXNPDDUDEJ
HNQYEDSQVVRUOXSRVRADHUYRYCEIHBFCELU
NLFESRACUQLBSWMJRNSDGTSSLNERNOZNXFVM
VOOZPYPEIGXFQPEGIWULQTKVCTUEUSZDPWRM
QUFRIUFRYGGNSKEVSLBFOVKJOSUSHORSVVV
WVYVQRNQJFAGXFZTURGFOHRNOHQWHOVQRLR
ADACMRZOAVHTOGGKYURGFCSRDEERIEMYJKUE

$$I.C. = \frac{\sum_{i=A}^{i=Z} f_i(f_i - 1)}{N(N - 1)}$$

f_i - frequency of i -th letter

N - ciphertext length

Calculation:

Index of coincidence of subsequence 1 is : 0.04049820815477533
Index of coincidence of subsequence 2 is : 0.0414931475732566
AVERAGE INDEX OF COINCIDENCE FOR KEY LENGHT 2 is : 0.040995677

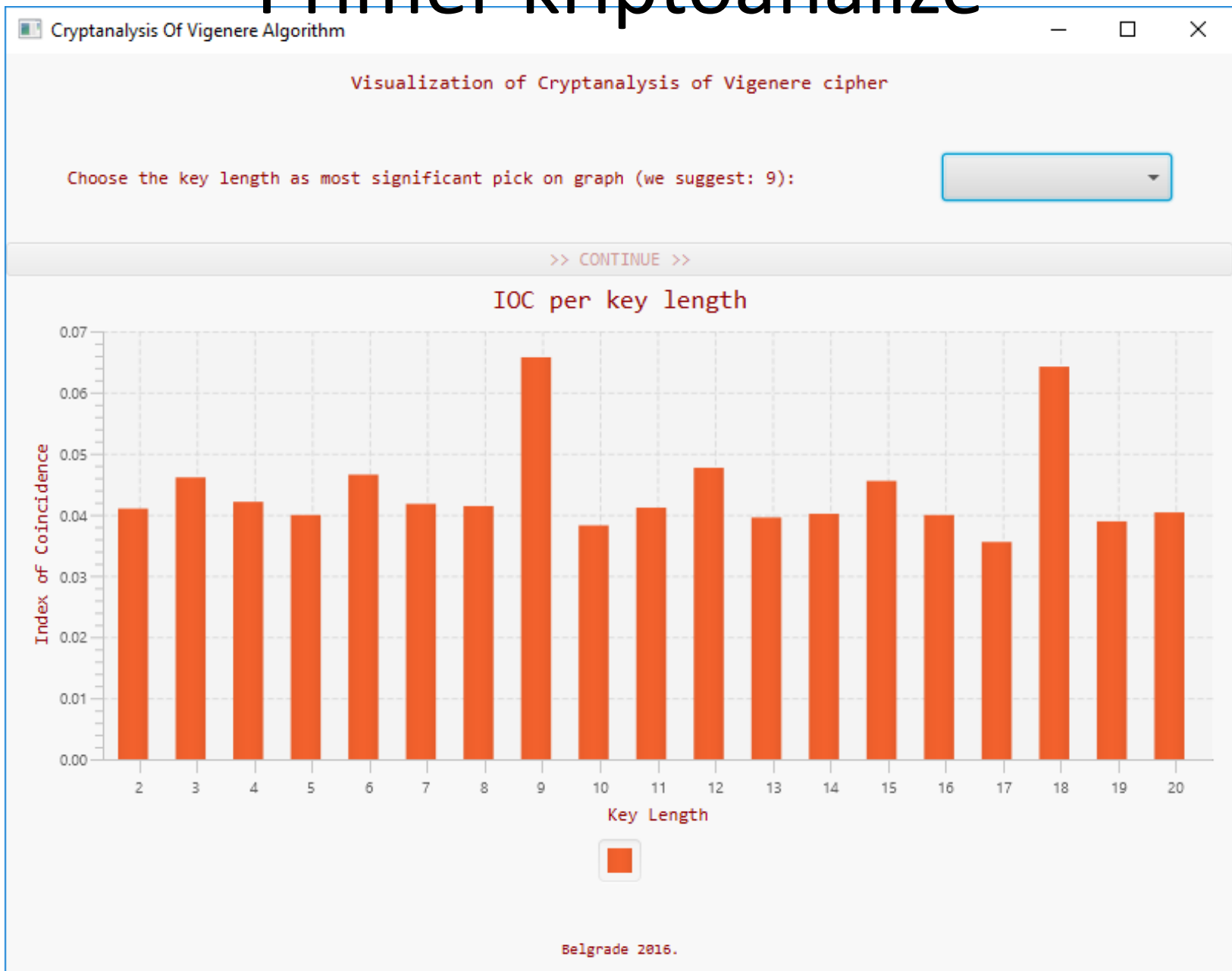
keyLength	indexOfCoin...
2	0.04099567786...
3	0.04609909011...
4	0.04210761020...
5	0.03994943109...
6	0.04655123280...
7	0.04177271002...
8	0.04141005453...
9	0.06574444808...

<< Previous step

Next step >>

Continue...

Primer kriptanalize



Primer kriptanalize

Visualization of Cryptanalysis of Vigenere cipher

We are identifying key word step by step, letter by letter.

The Chi-squared Statistic is a measure of how similar two categorical probability distributions are.

The letter with the minimum value of the Chi-squared Statistic is identified as part of key word.

Message:

KHRWFILYJLBQUNOILEAZHRRKWFZOAFOBXSXYCO
WVQGSPCDNQRFRUIFRYGGPOWGXPDDUDEJKHNC
YEDSQVVRUOXSRVRADHUYRYCEIHBFCELUFNLFES
RACUQLBSWMJRNSDGTSSLNERNOZNXFV MVOOZPY
PEIGXFQPEGIWULQTKVC TUEUSZDPWRMBQUFRUIF
YGGNSKEV SGLBFOVKJOSUSHORSVVVVWFYVQRNQ
FAGXFZTURGFOHRNOHQWQVQR LRADACMRZOAV
HTOGGKVIRGFCRSDEFERLEMVYIKUEDZIIIXWRZTHWW

$$\chi^2(C, E) = \sum_{i=A}^{i=Z} \frac{(C_i - E_i)^2}{E_i}$$

CA - count of letter A

EA - expected count of letter A

Chi-squared statistic in case that key letter is a: 1996.4607439991587
Chi-squared statistic in case that key letter is b: 1620.628643376284
Chi-squared statistic in case that key letter is c: 697.4764606168357
Chi-squared statistic in case that key letter is d: 1631.2934494840038
Chi-squared statistic in case that key letter is e: 518.8647996472498
Chi-squared statistic in case that key letter is f: 3020.8083639042097
Chi-squared statistic in case that key letter is g: 500.9066837628507
Chi-squared statistic in case that key letter is h: 711.5207957649818
Chi-squared statistic in case that key letter is i: 709.440983157764
Chi-squared statistic in case that key letter is j: 1246.5303015578597
Chi-squared statistic in case that key letter is k: 1380.7659492513117
Chi-squared statistic in case that key letter is l: 1981.8598971345068
Chi-squared statistic in case that key letter is m: 2214.6737461539215
Chi-squared statistic in case that key letter is n: 1022.404240989768

KEY
r
?
?
?
?
?
?
?
?
?

<< Previous step

Next step >>

Continue...

Primer kriptanalize

Visualization of Cryptanalysis of Vigenere cipher

We are identifying key word step by step, letter by letter.

The Chi-squared Statistic is a measure of how similar two categorical probability distributions are.

The letter with the minimum value of the Chi-squared Statistic is identified as part of key word.

Message:

```
KHRFWFILYJLBQUNOILEAZHRRKWFZOAFOBSXYCO
WVQGSPCDNQRFRIUFRYGGPOWGXNPPDUDEJKHN
YEDSQVVRUOXRRVRADHUYRYCEIHFCELUFNLFES
RACUQLBSWMJRNSDGTSSLNERNOZNXFVMVOOZPY
PEIGXFQPEGIWULQTKVCTUEUSZDPWRMBQUFRIUF
YGGNSKEVSLBFOVKJOSUSHORSVVVWFYVQRNQ
FAGXFZTURGFOHRNOHQWHOVRRLRADACMRZOA
TQGGKYIIRGECRSEFERIFEMVLIKUEDZILXWRZTHWVA
```

$$\chi^2(C, E) = \sum_{i=A}^{i=Z} \frac{(C_i - E_i)^2}{E_i}$$

CA - count of letter A

EA - expected count of letter A

```
Chi-squared statistic in case that key letter is a: 66.83636391054849
Chi-squared statistic in case that key letter is b: 1682.2260776946955
Chi-squared statistic in case that key letter is c: 782.382955530316
Chi-squared statistic in case that key letter is d: 2170.6614171352485
Chi-squared statistic in case that key letter is e: 1101.8305104591082
Chi-squared statistic in case that key letter is f: 2715.288415283214
Chi-squared statistic in case that key letter is g: 250.9501535846984
Chi-squared statistic in case that key letter is h: 549.1225077631927
Chi-squared statistic in case that key letter is i: 732.7967995463324
Chi-squared statistic in case that key letter is j: 388.74356155096854
Chi-squared statistic in case that key letter is k: 1987.4268929386526
Chi-squared statistic in case that key letter is l: 314.28234885456817
Chi-squared statistic in case that key letter is m: 1599.1228173487837
Chi-squared statistic in case that key letter is n: 631.0626988991694
```

KEY
r
a
?
?
?
?
?
?
?
?

<< Previous step

Next step >>

Continue...

Primer kriptanalize

Visualization of Cryptanalysis of Vigenere cipher

We are identifying key word step by step, letter by letter.

The Chi-squared Statistic is a measure of how similar two categorical probability distributions are.

The letter with the minimum value of the Chi-squared Statistic is identified as part of key word.

Message:

KHRFWFILYJLBQUNOILEAZHRRKW FZOAF OBSXYCO
WVQGS PCDNQRFR IUFRYGGPOWGXNPDDUDEJKN
YEDS QVVRUOXSR RVRADHU YRYCEIHBFC ELUFNLFES
RACUQLBSWM JRNSDGTSSLNERNOZNX FVMVOOZPY
PEIGXFQPEG IWULQTKVCTUEUSZDPWRMBQUFR IUF
YGGNSKEVSLBFOVKJOSUSHORSVVVWFYVQRNQ.
FAGXFZTURGFOHRNOHQWHOVQRLRADACMRZOAV
HTOGGKVIIRGECRSDEFRIEMVJKIIFEDZILXWRZTHWW

$$\chi^2(C, E) = \sum_{i=A}^{i=Z} \frac{(C_i - E_i)^2}{E_i}$$

CA - count of letter A

EA - expected count of letter A

Chi-squared statistic in case that key letter is a: 1448.7830742452895
Chi-squared statistic in case that key letter is b: 2381.18372748209
Chi-squared statistic in case that key letter is c: 535.9704552698938
Chi-squared statistic in case that key letter is d: 1523.198805209058
Chi-squared statistic in case that key letter is e: 305.96144610055353
Chi-squared statistic in case that key letter is f: 843.7199021886897
Chi-squared statistic in case that key letter is g: 1500.3940935651776
Chi-squared statistic in case that key letter is h: 2150.102863699195
Chi-squared statistic in case that key letter is i: 2673.838487381355
Chi-squared statistic in case that key letter is j: 820.344831211912
Chi-squared statistic in case that key letter is k: 775.1712276870727
Chi-squared statistic in case that key letter is l: 332.35846239659134
Chi-squared statistic in case that key letter is m: 1914.9123593377994
Chi-squared statistic in case that key letter is n: 278.61662074649166

KEY
r
a
n
d
o
m
k
e
y

<< Previous step

Next step >>

Continue...

Primer kriptanalize

Visualization of Cryptanalysis of Vigenere cipher

When we know the key word, we can simply decrypt our ciphertext using Vigenere table

cipher	key	plain
K	R	T
H	A	H
R	N	E
F	D	C
W	O	I
F	M	T
I	K	Y
L	E	H
Y	Y	A
J	R	S
L	A	L
B	N	O
Q	D	N
U	O	G
N	M	B
O	K	E
I	E	E

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