Cryptography

Some simple ciphers

Caesar's Cipher

- Simple Shift Cipher
- All letters in the plain text are shifted by the same amount
- Easily cracked

Example

plaintext: the sleepy brown fox ate doughnuts

shift: +5

CIPHERTEXT: ?

Encryption Process

1. Remove the spaces and punctuation from the plaintext
2. Set up the encryption alphabet based on the shift value
3. Generate the ciphertext by looking up the value in the encryption alphabet

Encryption

plaintext: thesleepybrownfoxatedoughnuts

shift: +5

encryption alphabet:

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

CIPHERTEXT: ?

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:
abcdefghijklmnopqrstuvwxyz
BCDEFGHIJKLMNOPQRSTUVWXYZA
CIPHERTEXT: ?

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:
abcdefghijklmnopqrstuvwxyz
CDEFGHIJKLMNOPQRSTUVWXYZAB
CIPHERTEXT: ?

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:
abcdefghijklmnopqrstuvwxyz
DEFGHIJKLMNOPQRSTUVWXYZABC
CIPHERTEXT: ?

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:
abcdefghijklmnopqrstuvwxyz
EFGHIJKLMNOPQRSTUVWXYZABCD
CIPHERTEXT: ?

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:

```
abcdefghijklmnopqrstuvwxyz
FGHIJKLMNOPQRSTUVWXYZABCDE
```

CIPHERTEXT: ?

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:

```
abcdefghijklmnopqrstuvwxyz
FGHIJKLMNOPQRSTUVWXYZABCDE
```

CIPHERTEXT:Y

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:

```
abcdefghijklmnopqrstuvwxyz
FGHIJKLMNOPQRSTUVWXYZABCDE
```

CIPHERTEXT:YM

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:

```
abcdefghijklmnopqrstuvwxyz
FGHIJKLMNOPQRSTUVWXYZABCDE
```

CIPHERTEXT:YMJ

Encryption

plaintext: thesleepybrownfoxatedoughnuts
shift: +5
encryption alphabet:
abcdefghijklmnopqrstuvwxyz
FGHIJKLMNOPQRSTUVWXYZABCDE
CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX

Decryption Process (with shift)

1. Set up the decryption alphabet based on the (negated)shift value
2. Generate the plaintext by looking up the value in the encryption alphabet
3. Insert spaces/punctuation

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX
shift: +5 (but shift backwards to decrypt)
decryption alphabet:
`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
`vwxyzabcdefghijklmnopqrstu`
plaintext: ?

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX
shift: +5
decryption alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
vwxyzabcdefghijklmnopqrstu
plaintext: t

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX
shift: +5
decryption alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
vwxyzabcdefghijklmnopqrstu
plaintext: th

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX
shift: +5
decryption alphabet:
`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
`vwxyzabcdefghijklmnopqrstu`
plaintext: thesleepybrownfoxatedoughnuts

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX
shift: +5
decryption alphabet:
`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
`vwxyzabcdefghijklmnopqrstu`
plaintext: the sleepy brown fox ate doughnuts

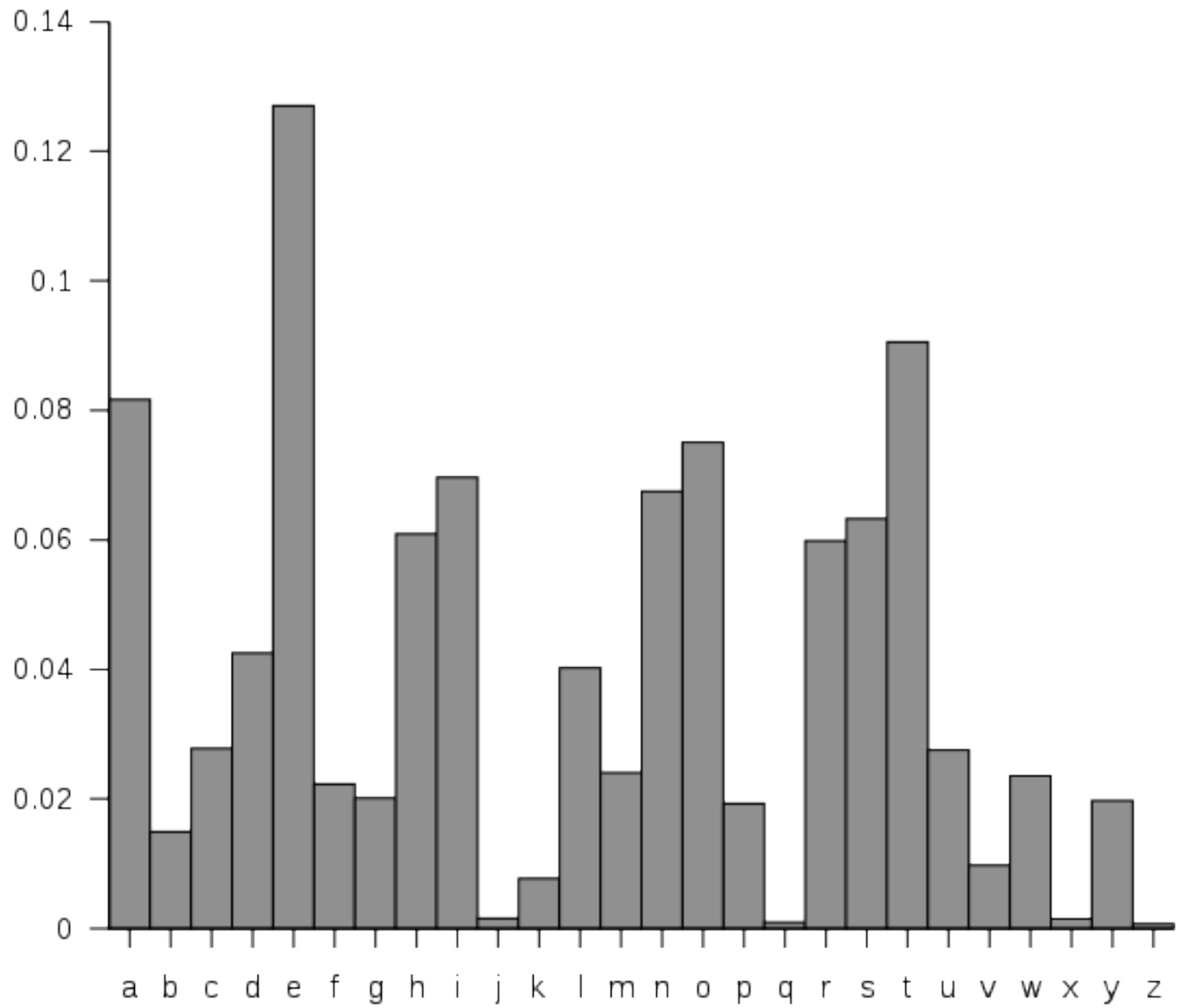
Decryption Process (without shift)

1. ?

Decryption Process (without shift)

1. Brute force
    1. how many different possible ciphers?
2. Frequency analysis
    1. Letter frequency
    2. Look for patterns that could be common words

Frequency Analysis



http://en.wikipedia.org/wiki/File:English_letter_frequency_%28alphabetic%29.svg

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX
shift: ?
decryption alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
plaintext: ?

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX

J=e?
shift = 5?

shift: ?

decryption alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
vwxyzabcdefghijklmnopqrstu

plaintext: ?

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX

J=e?
shift = 5?

shift: ?

decryption alphabet:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
vwxyzabcdefghijklmnopqrstu
```

plaintext: thesleepybrownfoxatedoughnuts

Decryption

CIPHERTEXT:
YMJXQJJDGWTBSKTCFYJITZLMSZYX

J=e?
shift = 5?

shift: ?

decryption alphabet:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
vwxyzabcdefghijklmnopqrstu
```

plaintext: the sleepy brown fox ate doughnuts

Caesar Cipher Practice

Encode the following using a shift of +11:

great minds think alike

Caesar Cipher Practice

Encode the following using a shift of +11:

great minds think alike

Answer: RCPLE XTYOD ESTYV LWTVP

Caesar Cipher Practice

The following was encoded with a shift of +6, decode it:

HXKGQGRRZNKIOVNKXY

Caesar Cipher Practice

The following was encoded with a shift of +6, decode it:

HXKGQGRRZNKIOVNKXY

Answer: break all the ciphers

Caesar Cipher Practice

The following was encoded with an unknown shift of, decode it:

DROPBOAEOXMIYPDROVODDOBOSCDRO UOI

Caesar Cipher Practice

The following was encoded with an unknown shift of, decode it:

DROPBOAEOXMIYPDROVODDOBOSCDRO UOI

Answer: the frequency of the letter e is key

Vigenere's Cipher

- A more complex shift cipher
- Uses a set of Caesar ciphers
- Usually a "key word" defines the shifts
- Use a Vigenere Square (or tabular recta) to encrypt/decrypt

Tabula recta

	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

http://en.wikipedia.org/wiki/File:Vigen%C3%A8re_square_shading.svg

Tabula recta

	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

Encryption:
Find plaintext column,
and keyletter row

Decryption:
Find keyletter row, and
locate CIPHERTEXT
letter in that row.
Column label is the
plaintext letter

Encryption

plaintext: the sleepy brown fox ate doughnuts

key: lemur

CIPHERTEXT: ?

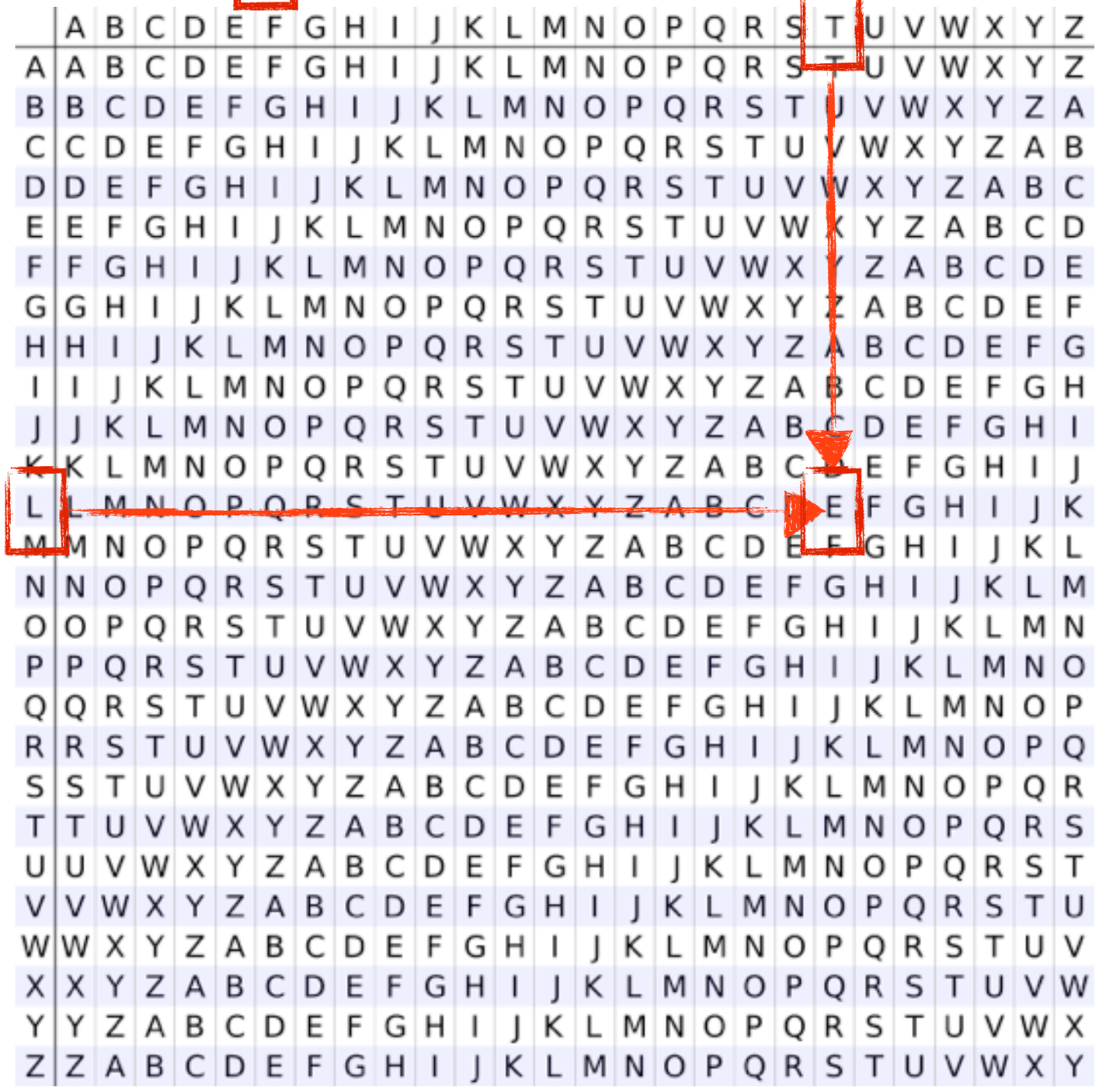
Encryption

plaintext: thesleepybrownfoxatedoughnuts
key: lemur

```
thesleepybrownfoxatedoughnuts
lemurlemurlemurlemurlemurlemu
```

CIPHERTEXT: ?

thesleepybrownfoxatedoughnuts
lemurlemurlemurlemurlemurlemu



Encryption:
Find plaintext column, and keyletter row

Decryption:
Find keyletter row, and locate CIPHERTEXT letter in that row. Column label is the plaintext letter

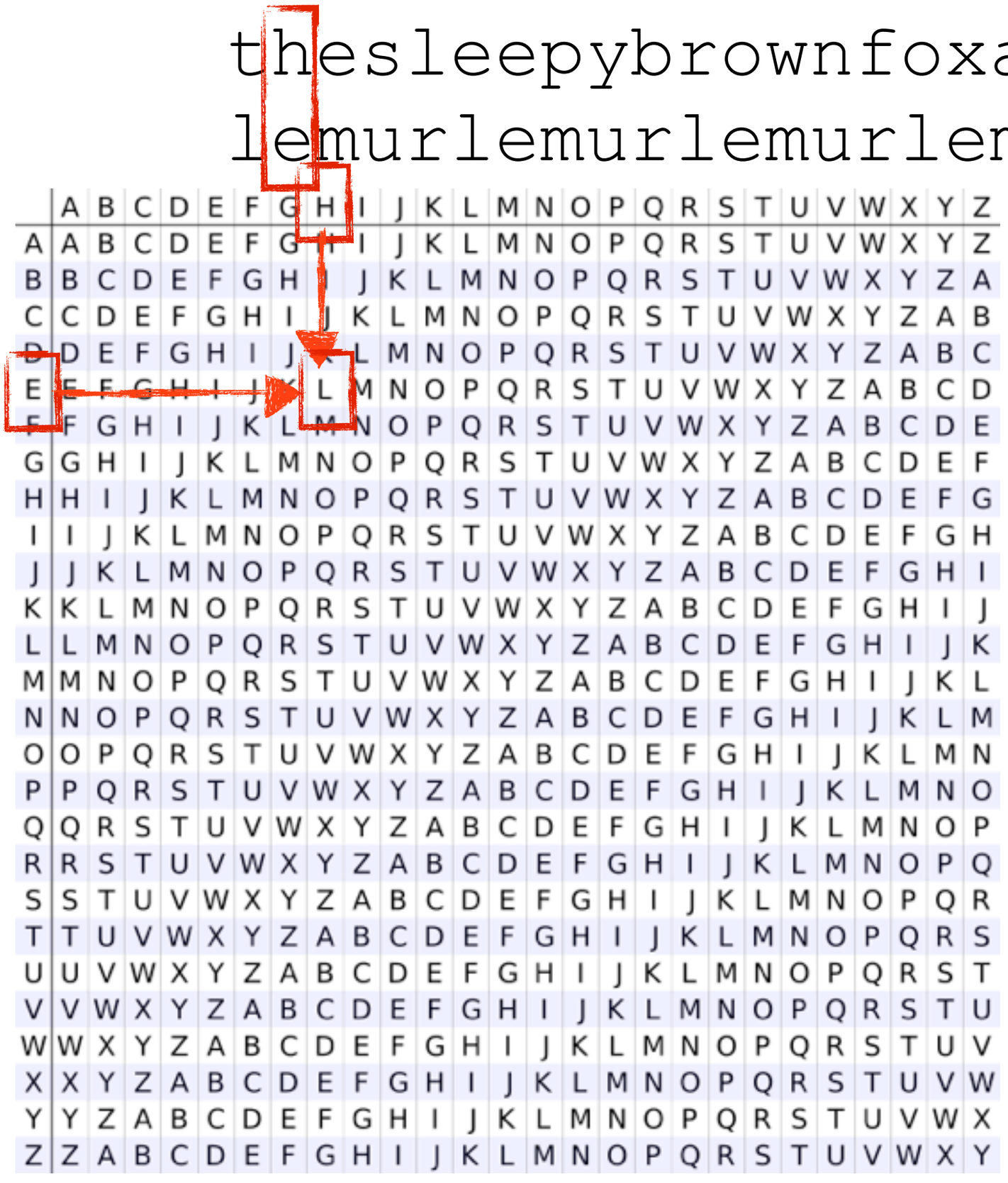
Encryption

plaintext: thesleepybrownfoxatedoughnuts
key: lemur

```
thesleepybrownfoxatedoughnuts
lemurlemurlemurlemurlemurlemu
E
```

CIPHERTEXT: ?

thesleepybrownfoxatedoughnuts
lemurlemurlemurlemurlemurlemu



	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

Encryption:
Find plaintext column, and keyletter row

Decryption:
Find keyletter row, and locate CIPHERTEXT letter in that row. Column label is the plaintext letter

Encryption

plaintext: thesleepybrownfoxatedoughnuts
key: lemur

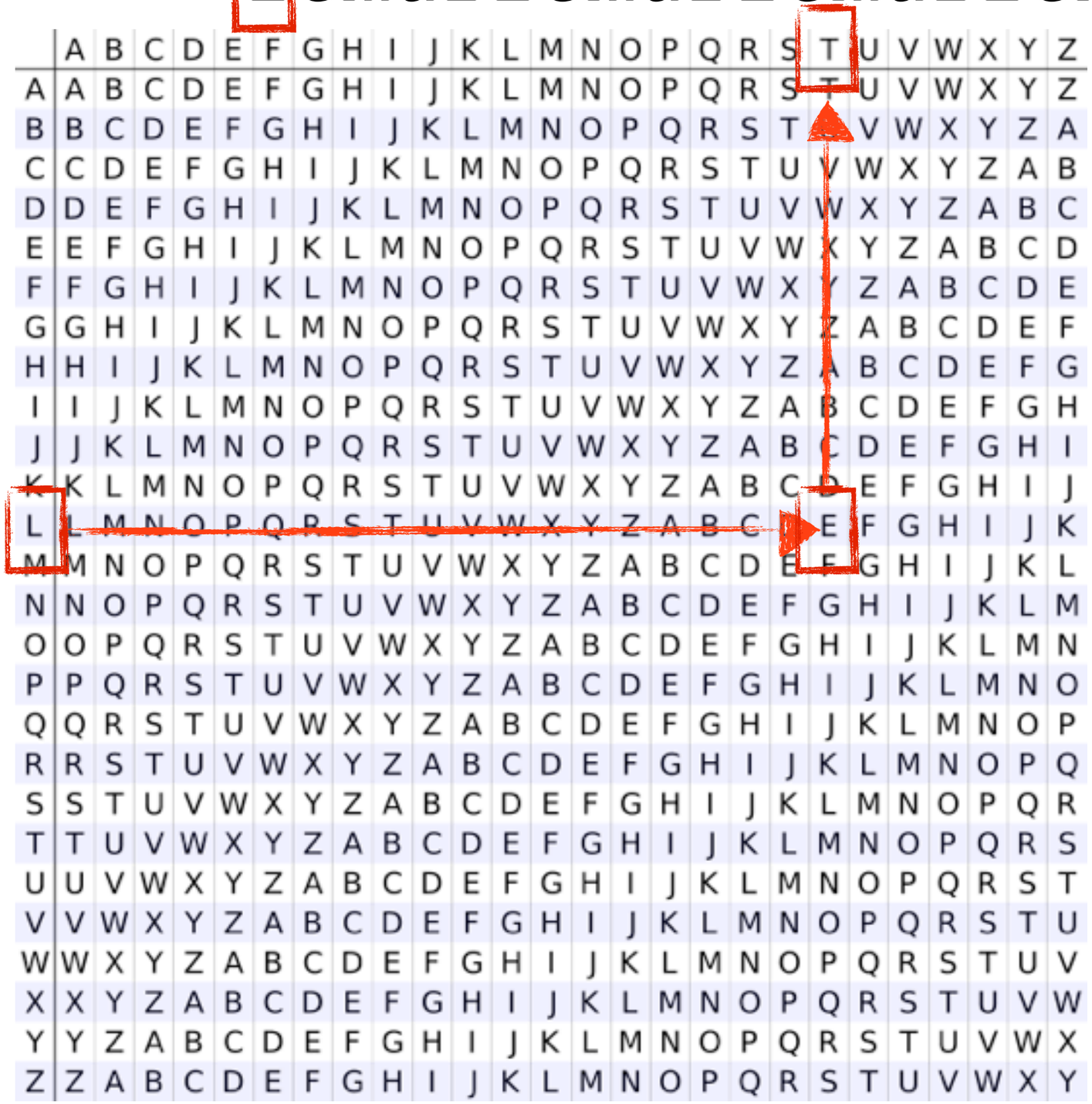
```
thesleepybrownfoxatedoughnuts
lemurlemurlemurlemurlemurlemu
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
```

Decryption (with key)

CIPHERTEXT:
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
key: lemur

plaintext: ?

ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
lemurlemurlemurlemurlemurlemu



Encryption:
Find plaintext column, and keyletter row

Decryption:
Find keyletter row, and locate CIPHERTEXT letter in that row. Column label is the plaintext letter

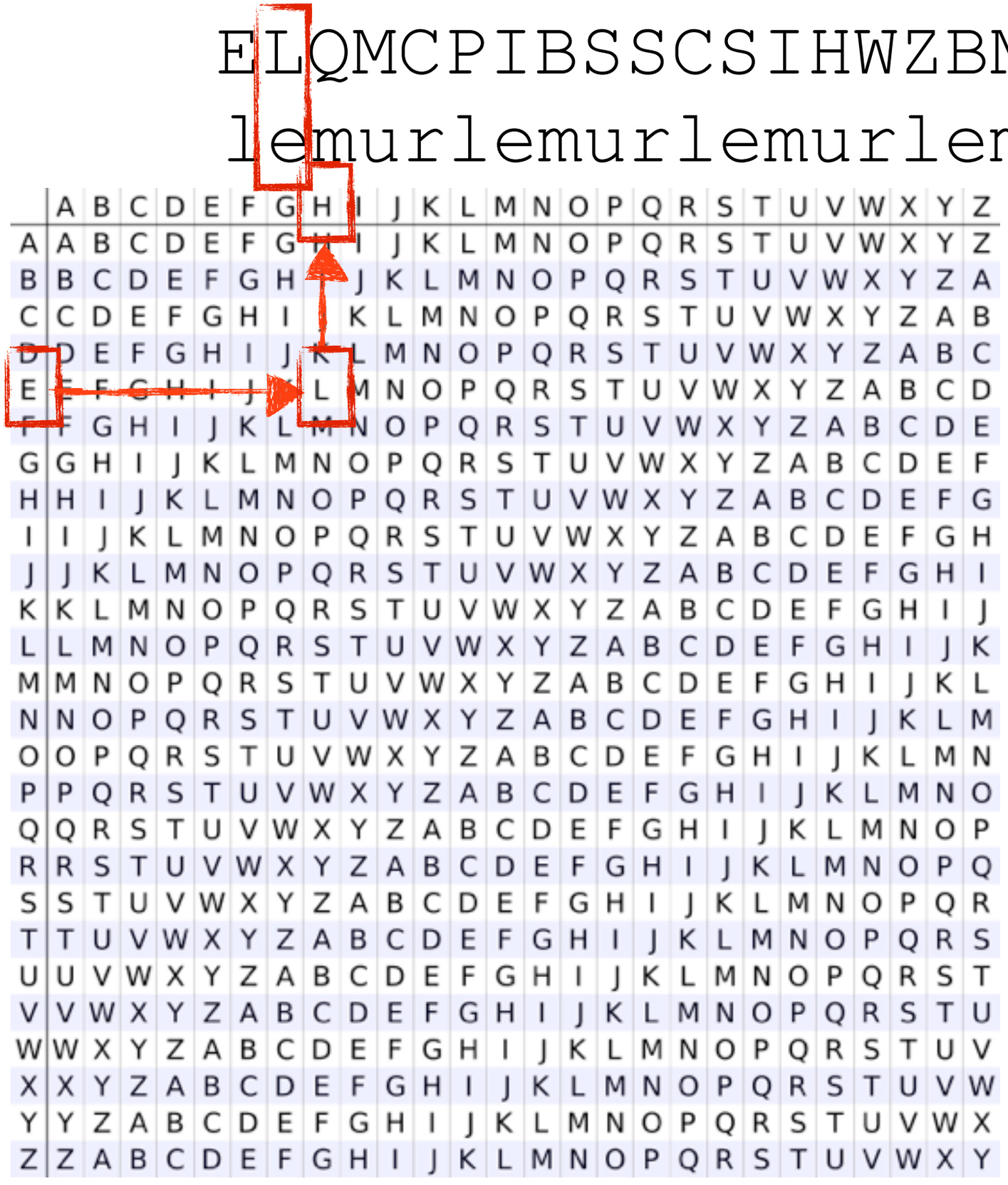
Decryption (with key)

CIPHERTEXT:
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
key: lemur

plaintext: t

ELQMCPIBSSCSIHWZBMNVOSGAYYYFM

lemurlemurlemurlemurlemurlemu



	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

Encryption:
Find plaintext column, and keyletter row

Decryption:
Find keyletter row, and locate CIPHERTEXT letter in that row. Column label is the plaintext letter

Decryption (with key)

CIPHERTEXT:
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
key: lemur

plaintext: th

Decryption (with key)

CIPHERTEXT:
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
key: lemur

plaintext: thesleepybrownfoxatedoughnuts

Decryption (with key)

CIPHERTEXT:
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
key: lemur

plaintext: the sleepy brown fox ate doughnuts

Decryption (without key)

CIPHERTEXT:
ELQMCPIBSSCSIHWZBMNVOSGAYYYFM
key: lemur

plaintext: ?

Decryption Process (without key)

- Brute force
  - how many different possible ciphers?
- Frequency analysis (If length of key is known)
- More advanced analysis
  - Kasiski Examination
    - When same word (or word-part) encrypted by same part of key
    - Look for repetition in CIPHERTEXT, then use the length of space between repeats to guess at key length

Vigenere Cipher Practice

Encode the following using the key `CAPER`:

I am slowly going crazy

I am slowly going crazy

	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

Encryption:
Find plaintext column, and keyletter row

Decryption:
Find keyletter row, and locate CIPHERTEXT letter in that row. Column label is the plaintext letter

Vigenere Cipher Practice

Encode the following using the key `CAPER`:

I am slowly going crazy

Answer: kabwcqwacxqickttaoc