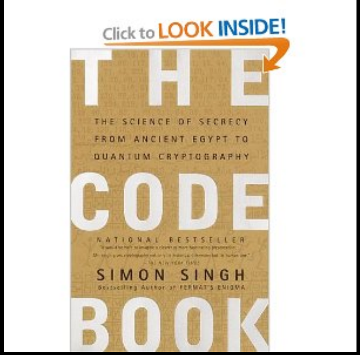
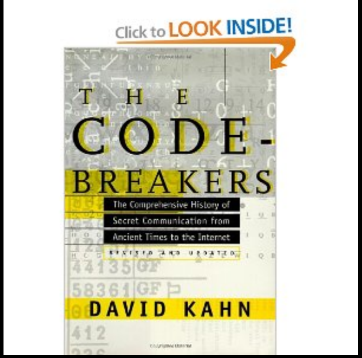
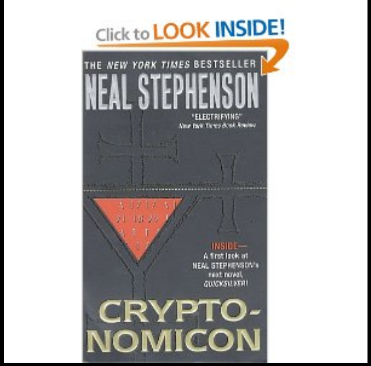
Cryptography

CSE 484

Books!

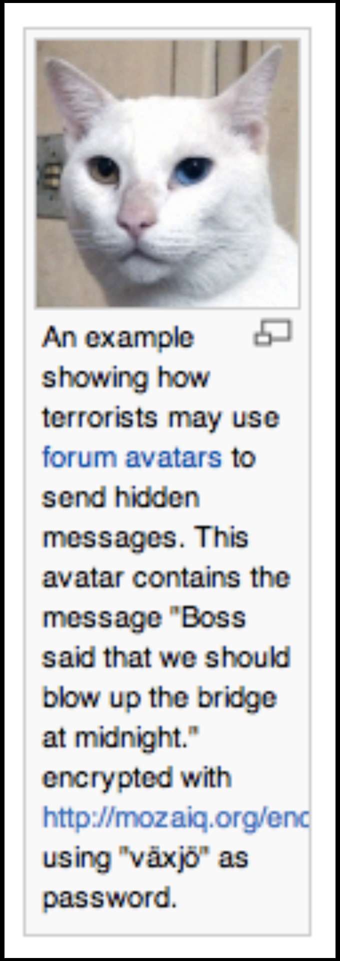

Click to LOOK INSIDE!
THE
THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY
CODE
NATIONAL BESTSELLER
SIMON SINGH
Bestselling Author of FERMAT'S ENIGMA
BOOK


Click to LOOK INSIDE!
THE
CODE-
BREAKERS
The Comprehensive History of Secret Communication from Ancient Times to the Internet
REVISED AND UPDATED
DAVID KAHN


Click to LOOK INSIDE!
THE NEW YORK TIMES BESTSELLER
NEAL STEPHENSON
"ELECTRIFYING"
INSIDE—
A first look at NEAL STEPHENSON's next novel, QUICKSILVER!
CRYPTO-
NOMICON

- The Code Book (Simon Singh)
- The Codebreakers (David Kahn)
- Cryptonomicon (Neal Stephenson)

Steganography

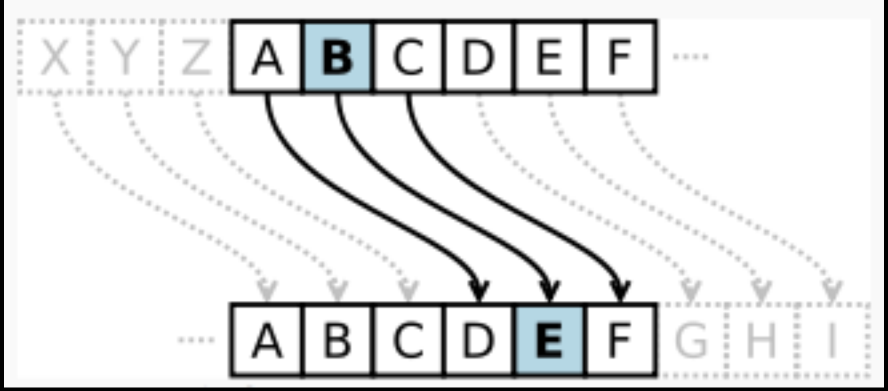


An example showing how terrorists may use forum avatars to send hidden messages. This avatar contains the message "Boss said that we should blow up the bridge at midnight." encrypted with http://mozaiq.org/enc using "växjö" as password.

Simple Steganography

Shift (Caesar) Cipher

- e.g. ROT13



```
the quick brown fox jumps over the lazy dog
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ
```

Monoalphabetic Substitution Cipher

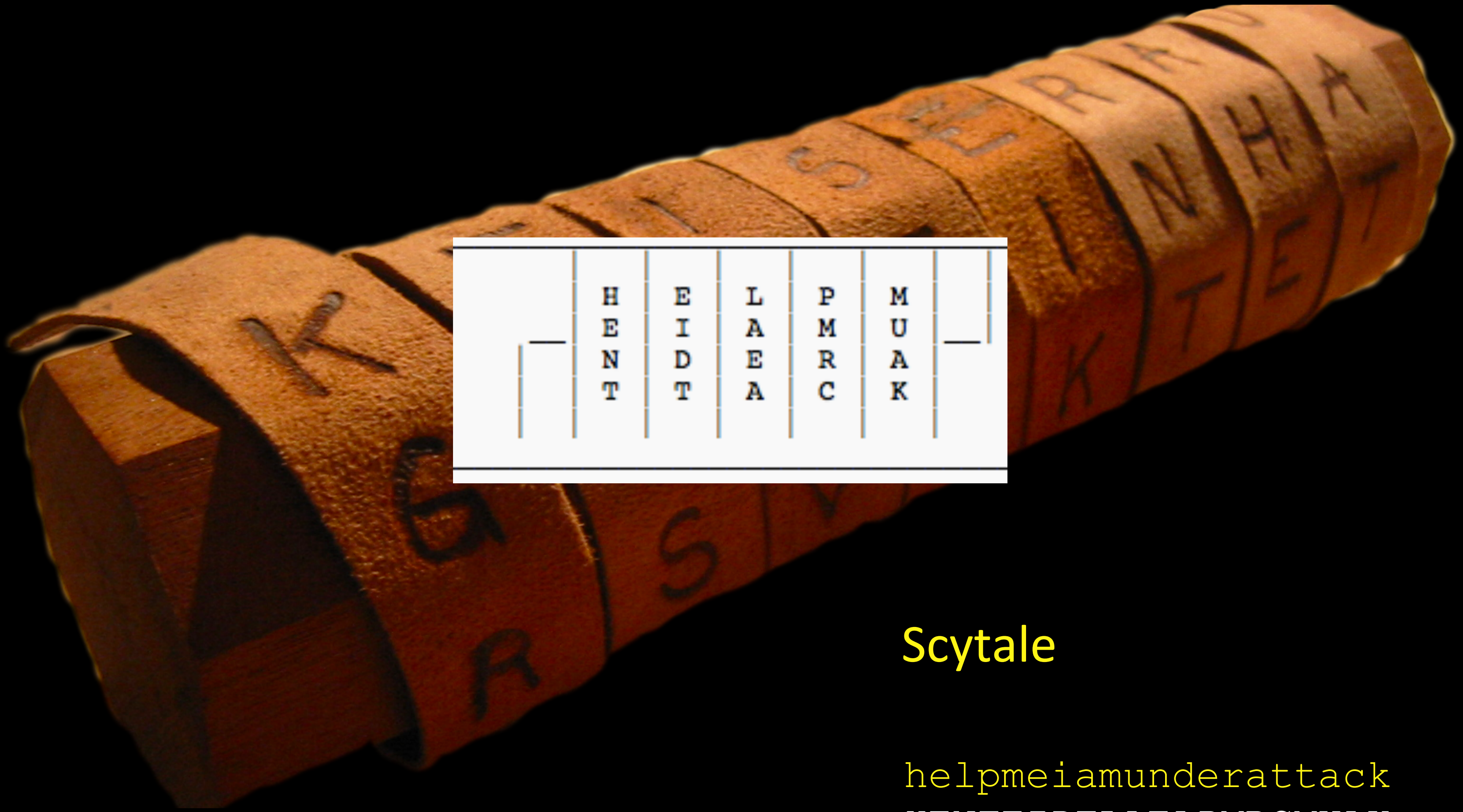
zebras

Plaintext alphabet:	abcdef…
Ciphertext alphabet:	ZEBRASCDFGHIJKLMNOPQTUVWXY

flee at once. we are discovered!

SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!

Transposition Cipher

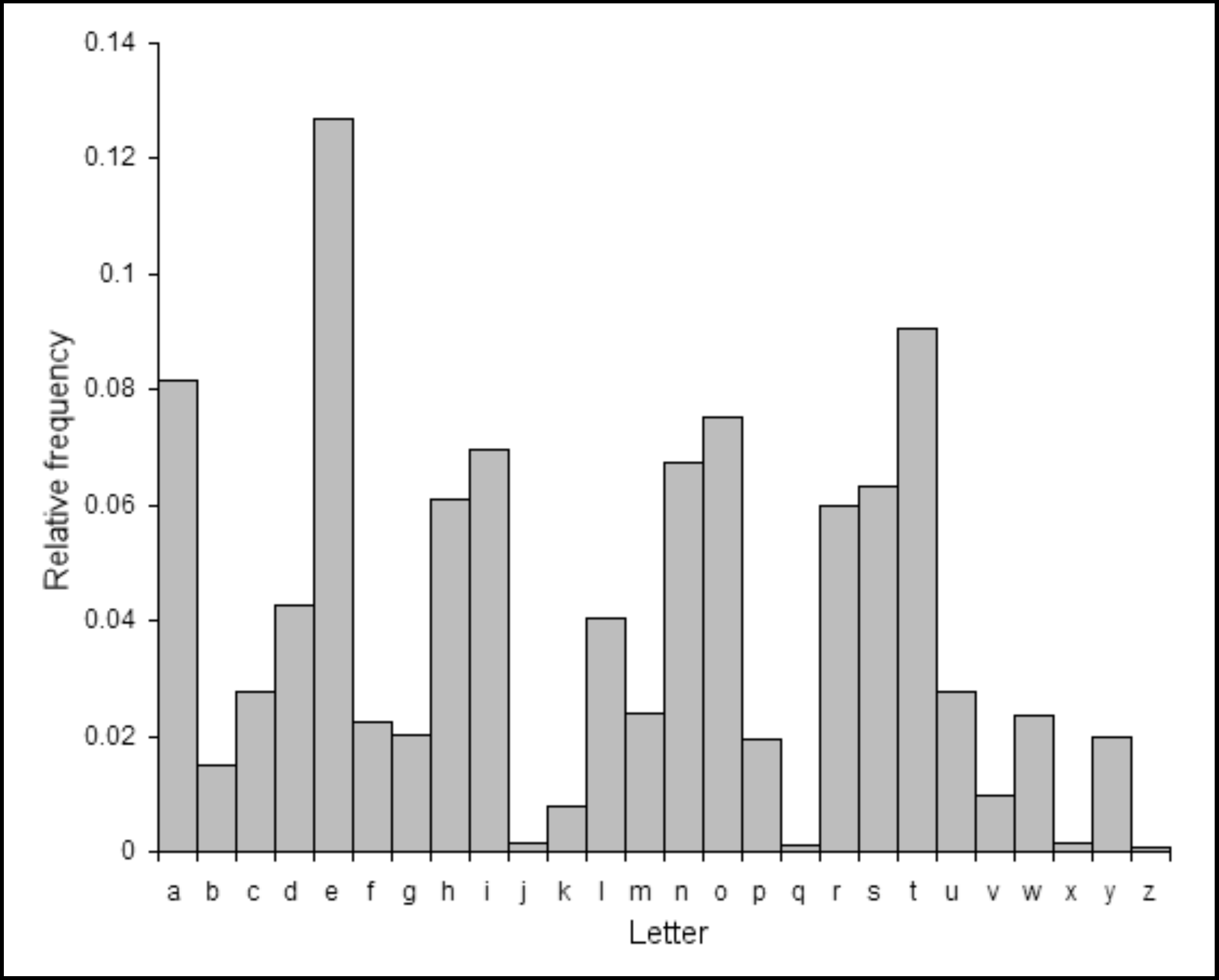


H	E	L	P	M
E	I	A	M	U
N	D	E	R	A
T	T	A	C	K

Scytale

helpmeiamunderattack
HENTEIDTLAEAPMRCMUAK

Frequency Analysis



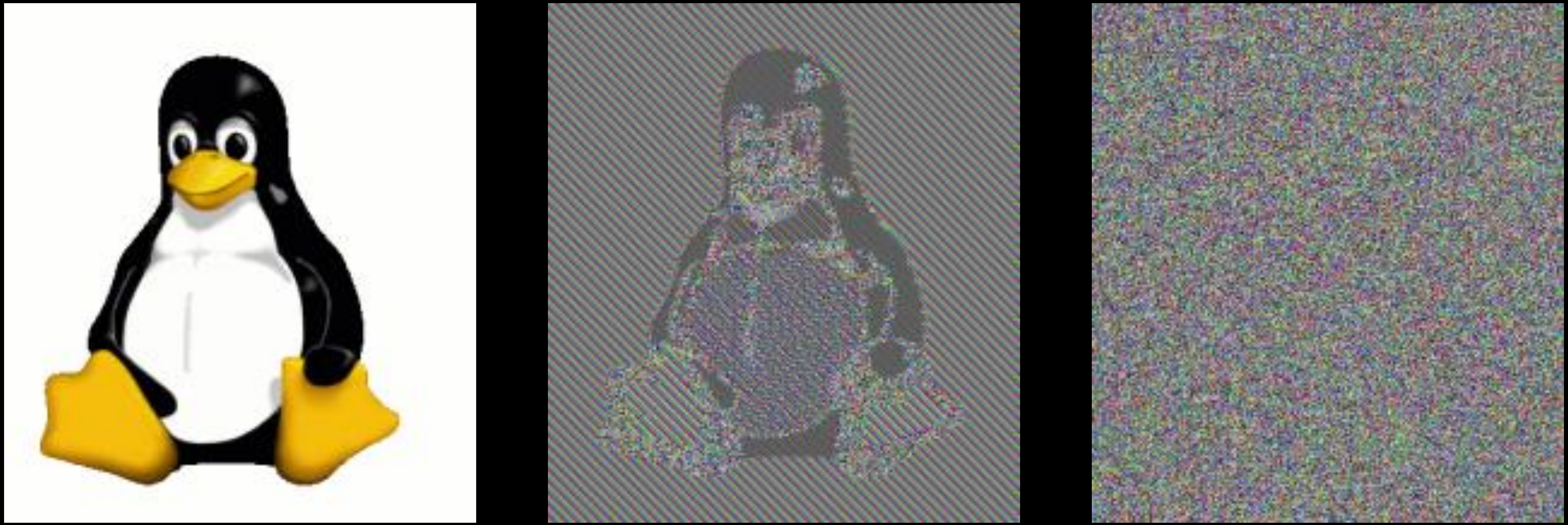
Bigrams

th	1.52%
he	1.28%
in	0.94%
er	0.94%
an	0.82%
re	0.68%
nd	0.63%
at	0.59%
on	0.57%
nt	0.56%
ha	0.56%
es	0.56%
st	0.55%
en	0.55%
ed	0.53%
to	0.52%
it	0.50%
ou	0.50%
ea	0.47%
hi	0.46%
is	0.46%
or	0.43%
ti	0.34%
as	0.33%
te	0.27%
et	0.19%
ng	0.18%
of	0.16%
al	0.09%
de	0.09%
se	0.08%
le	0.08%
sa	0.06%
si	0.05%
ar	0.04%
ve	0.04%
ra	0.04%
ld	0.02%
ur	0.02%

Trigrams

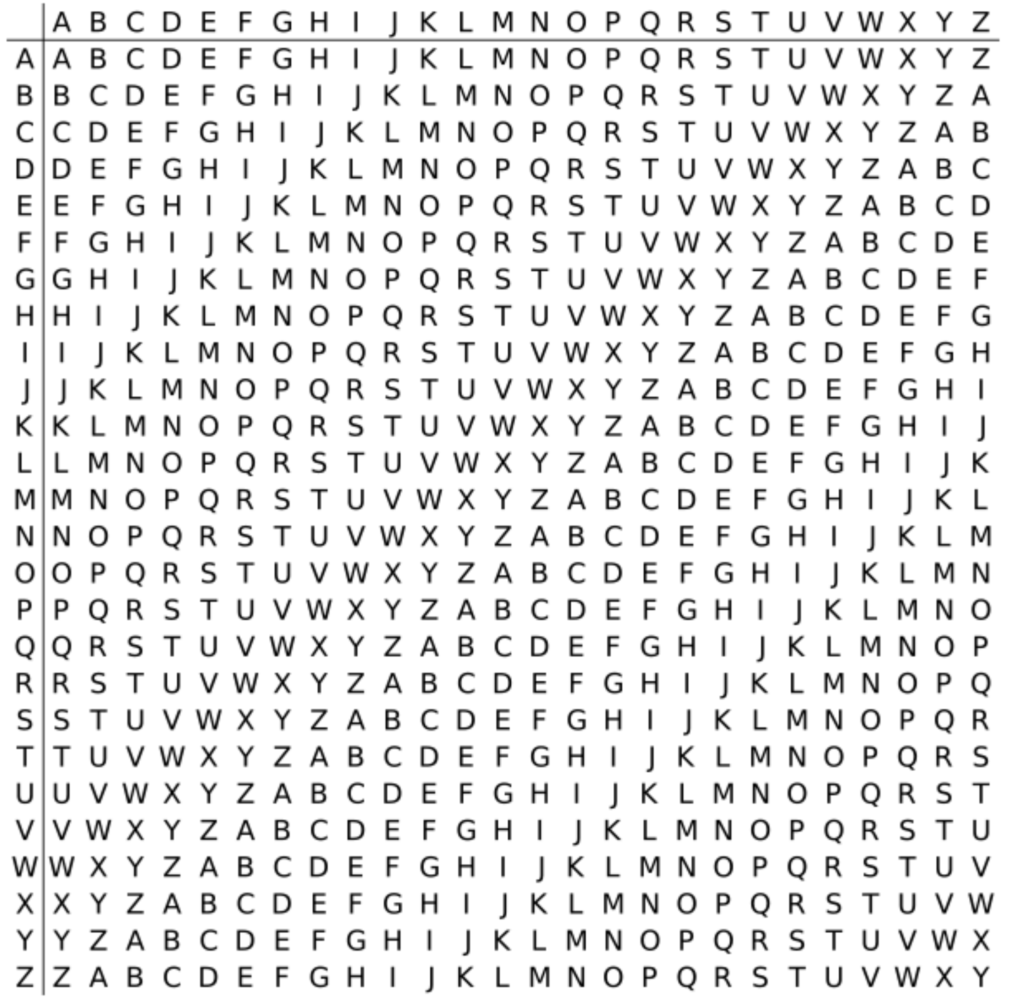
RANK	TRIGRAM
1	the
2	and
3	tha
4	ent
5	ing
6	ion
7	tio
8	for
9	nde
10	has
11	nce
12	edt
13	tis
14	oft
15	sth
16	men

Encryption Modes



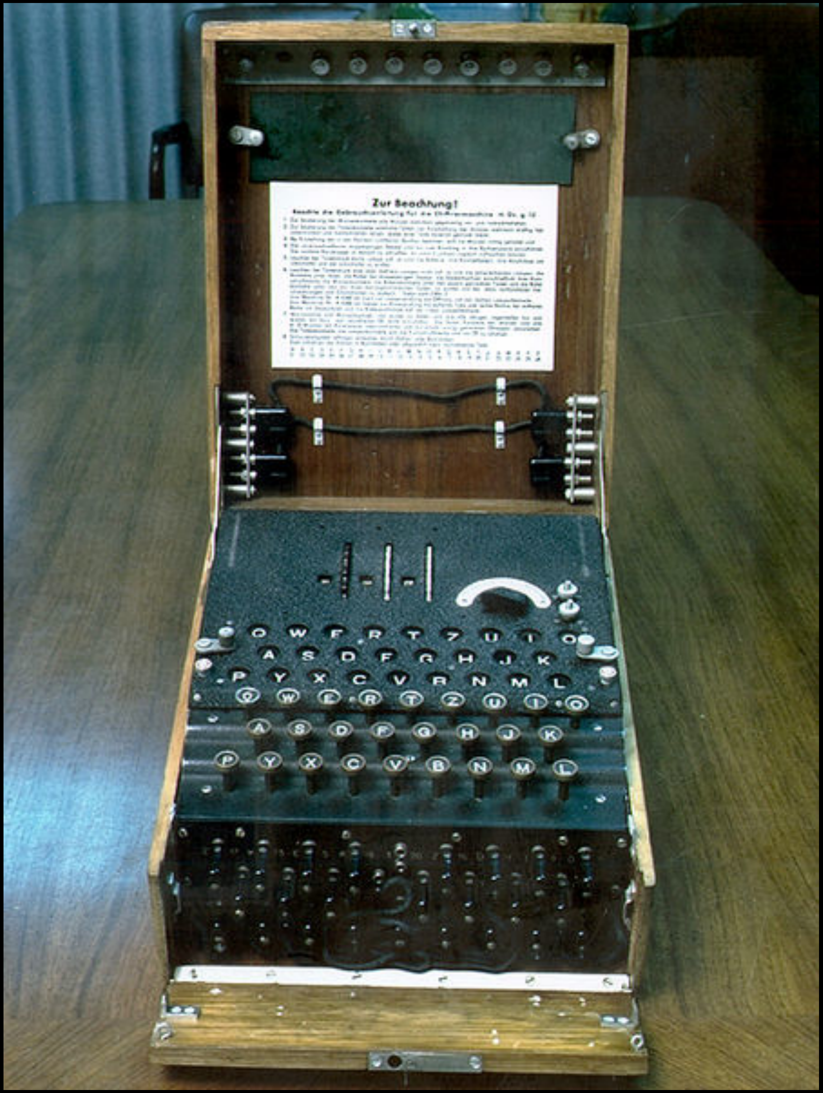
Polyalphabetic Substitution Cipher: Vigenère Cipher

Vigenère Cipher



	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

Enigma


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