NOVEMBER 4 – 5

TexSAW 2016

6th ANNUAL

TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE

Celebrating 30 Years

THE UNIVERSITY OF TEXAS AT DALLAS

Presenting Sponsor

StateFarm®

Supporting Sponsor

Raytheon

The University of Texas at Dallas

Introduction to Cryptography

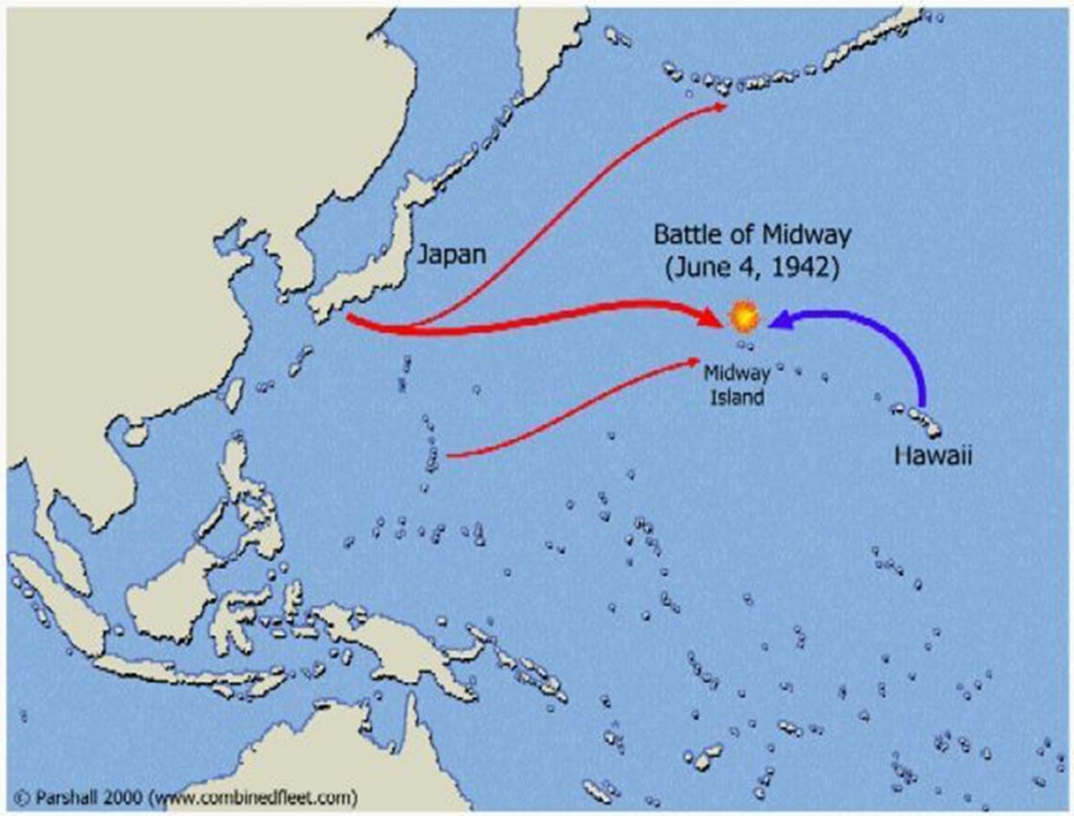
Jeremiah Shipman
Kyle Tillotson
Raman

Outline

- Classical Ciphers
- Hash Functions
- Modern Cryptography
  - Symmetric
  - Asymmetric
- Hands-On

Cryptography

- Cryptography is the process of writing or reading secret messages or codes. – Merriam Webster
- Midway story



Basic Terminology

- Plaintext/Message - the original message to encrypt.
- Ciphertext - an encrypted message.
- Cipher - an algorithm to convert plaintext to cipher text and vice/versa.
- Key - a word/phrase or string of bits that modifies the enciphering/deciphering process

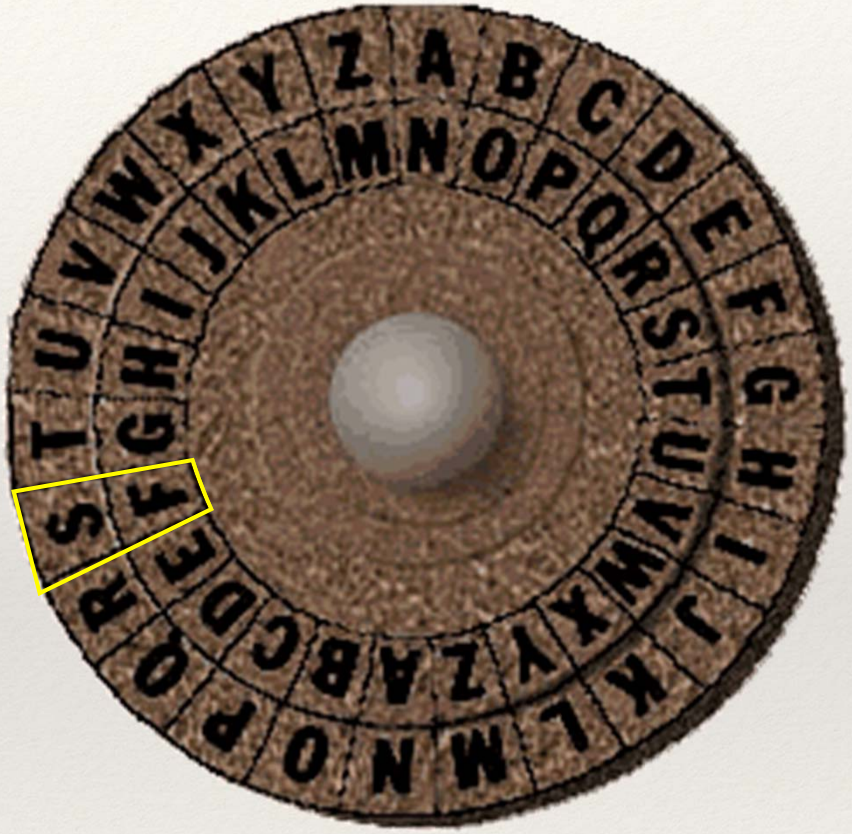
Caesar Cipher

- Shift/Caesar Cipher - rotate each letter of the plaintext by a fixed amount
- Example:
  - Plaintext - SEND HELP
  - Key - rotate up by 13
  - Ciphertext - FRAQ URYC

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
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

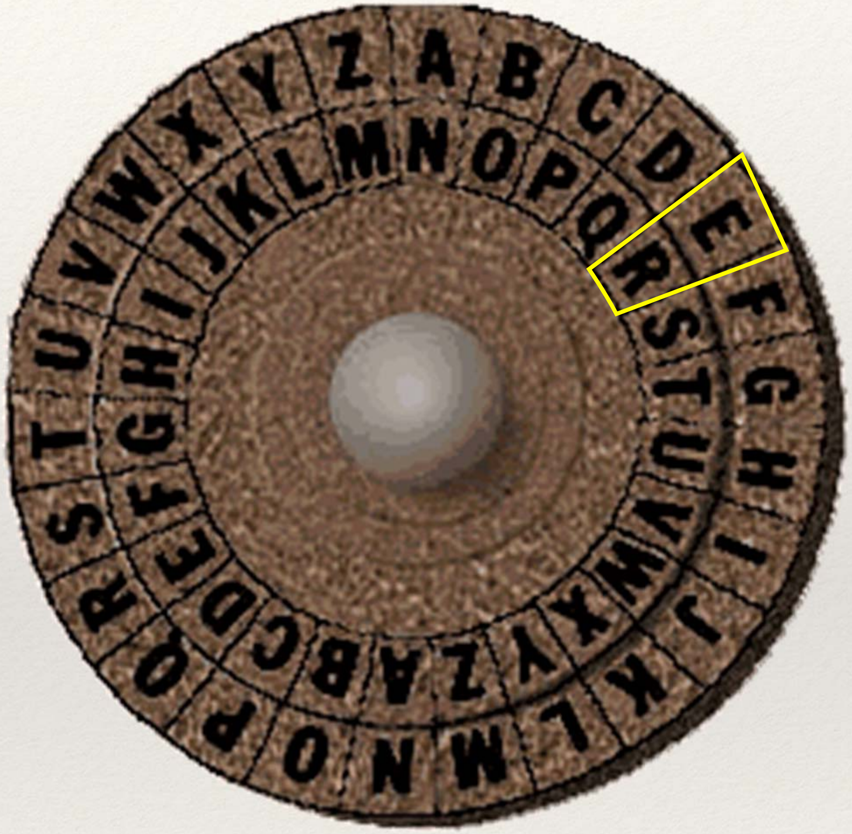
Caesar Cipher

- Shift/Caesar Cipher - rotate each letter of the plaintext by a fixed amount
- Example:
  - Plaintext - SEND HELP
  - Key - rotate up by 13
  - Ciphertext - FRAQ URYC


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
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

Caesar Cipher

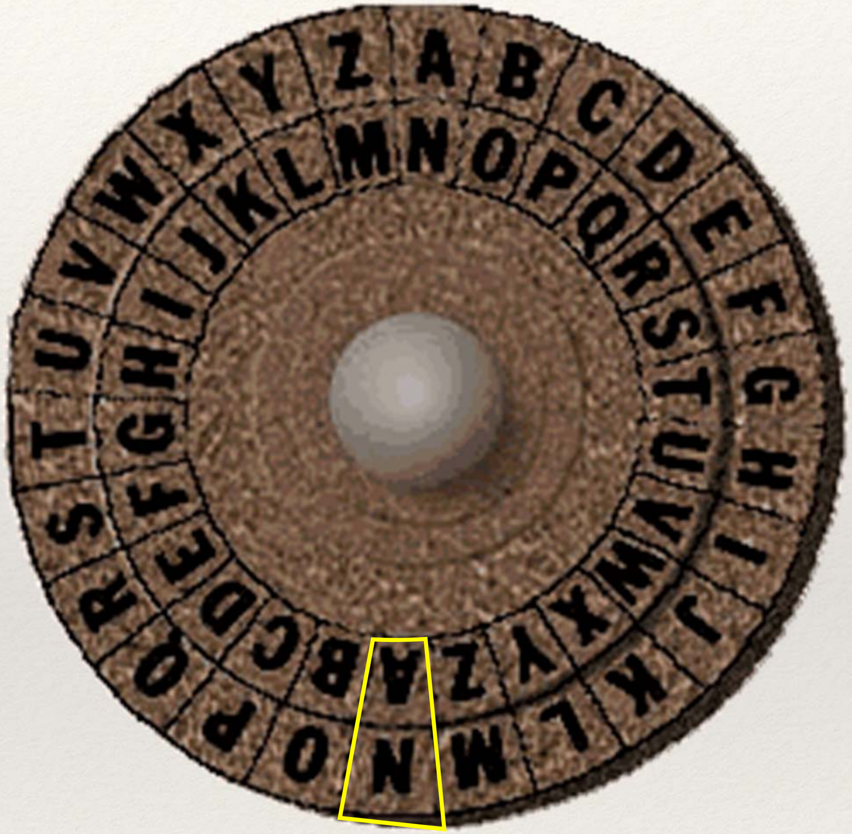
- Shift/Caesar Cipher - rotate each letter of the plaintext by a fixed amount
- Example:
  - Plaintext - SEND HELP
  - Key - rotate up by 13
  - Ciphertext - FRAQ URYC



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
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

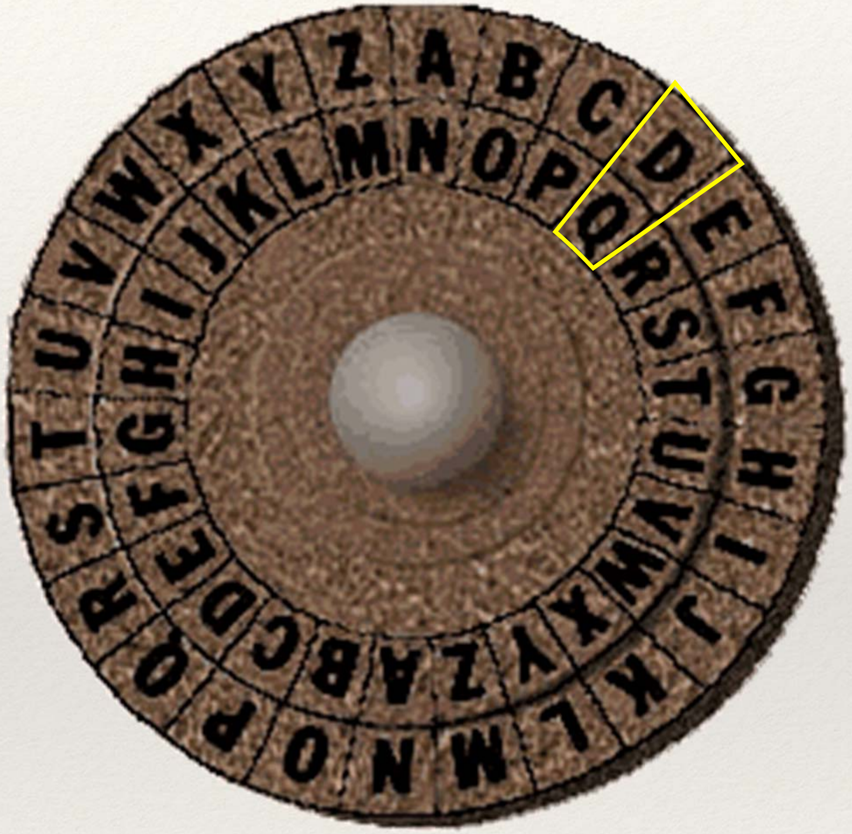
Caesar Cipher

- Shift/Caesar Cipher - rotate each letter of the plaintext by a fixed amount
- Example:
  - Plaintext - SEND HELP
  - Key - rotate up by 13
  - Ciphertext - FRAQ URYC


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
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

Caesar Cipher

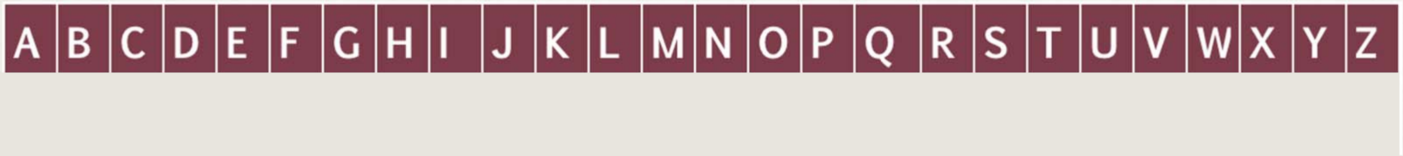
- Shift/Caesar Cipher - rotate each letter of the plaintext by a fixed amount
- Example:
  - Plaintext - SEND HELP
  - Key - rotate up by 13
  - Ciphertext - FRAQ URYC



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
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

Substitution Cipher

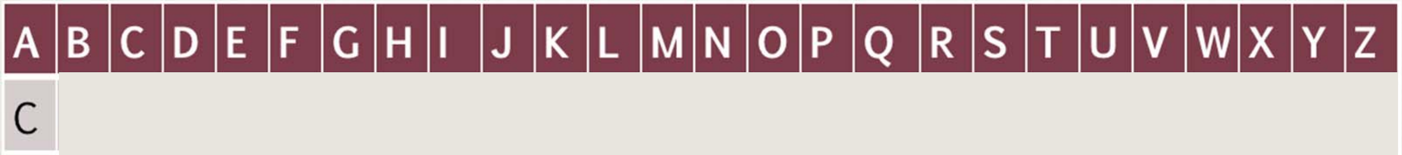
- Create a mapping of the alphabet:



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

Substitution Cipher

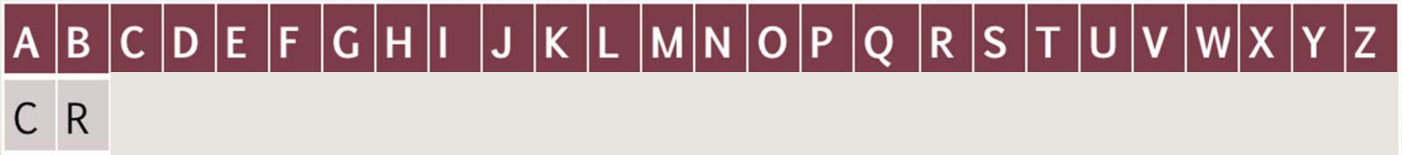
- Create a mapping of the alphabet:



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
C																									

Substitution Cipher

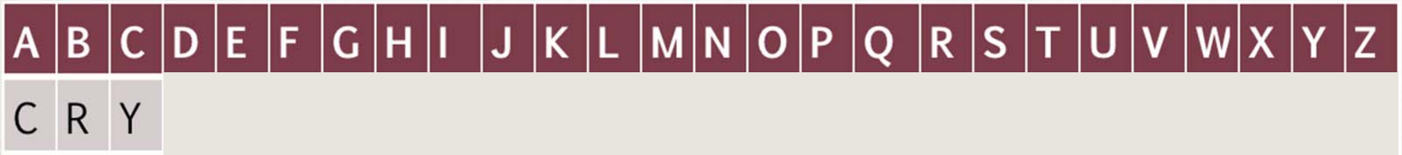
- Create a mapping of the alphabet:



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
C	R																								

Substitution Cipher

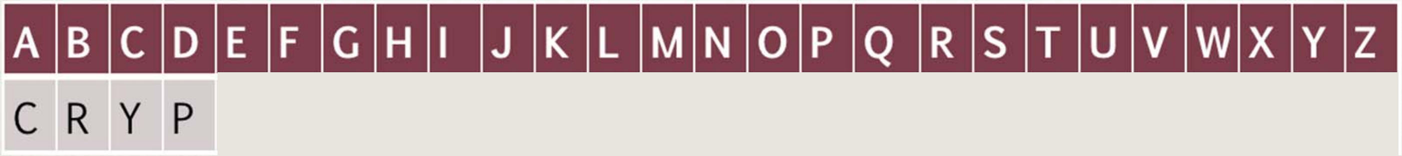
- Create a mapping of the alphabet:



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
C	R	Y																							

Substitution Cipher

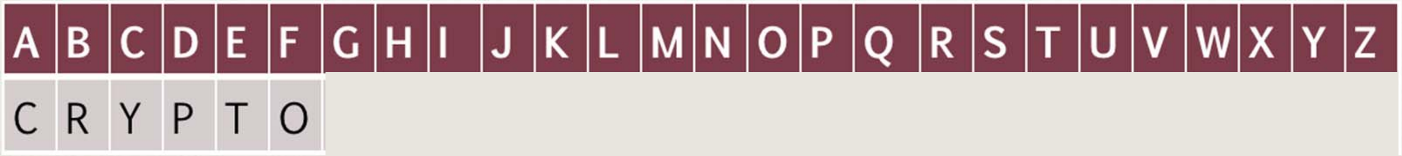
- Create a mapping of the alphabet:



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
C	R	Y	P																						

Substitution Cipher

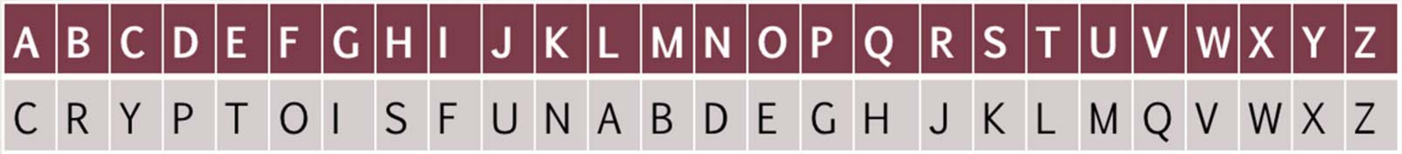
- Create a mapping of the alphabet:



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
C	R	Y	P	T	O																				

Substitution Cipher

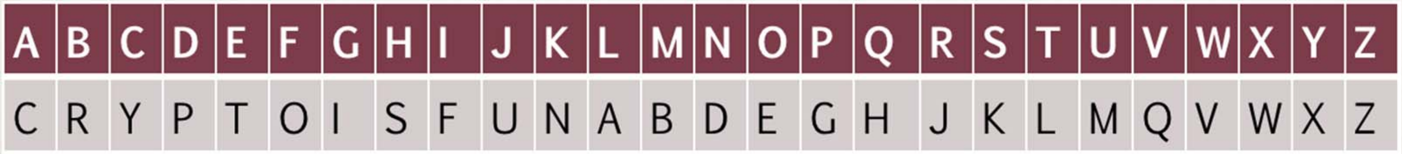
- Create a mapping of the alphabet:



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

Substitution Cipher

- Substitute each letter of the plaintext.

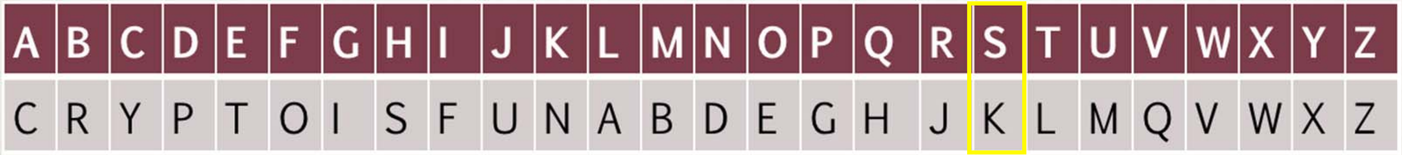


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	I	S	F	U	N	A	B	D	E	G	H	J	K	L	M	Q	V	W	X	Z

- Example:
  - Plaintext - send reinforcements
  - Key - knowledge of the mapping of the alphabet
  - Ciphertext - ktdp jtfdoejytbtdlk

Substitution Cipher

- Substitute each letter of the plaintext.

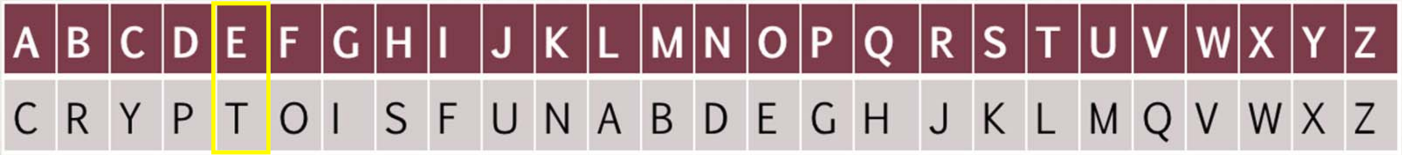


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	I	S	F	U	N	A	B	D	E	G	H	J	K	L	M	Q	V	W	X	Z

- Example:
  - Plaintext - send reinforcements
  - Key - knowledge of the mapping of the alphabet
  - Ciphertext - ktdp jtfdoejytbtdlk

Substitution Cipher

- Substitute each letter of the plaintext.

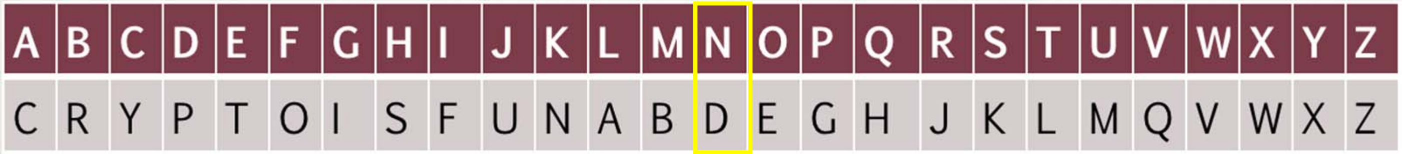


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	I	S	F	U	N	A	B	D	E	G	H	J	K	L	M	Q	V	W	X	Z

- Example:
  - Plaintext - send reinforcements
  - Key - knowledge of the mapping of the alphabet
  - Ciphertext - ktdp jtfdoejytbtdlk

Substitution Cipher

- Substitute each letter of the plaintext.

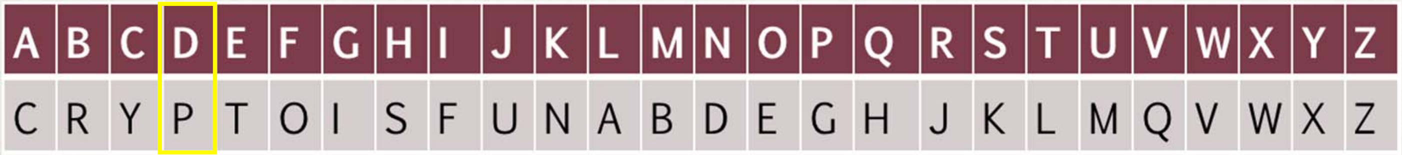


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	I	S	F	U	N	A	B	D	E	G	H	J	K	L	M	Q	V	W	X	Z

- Example:
  - Plaintext - send reinforcements
  - Key - knowledge of the mapping of the alphabet
  - Ciphertext - ktdp jtfdoejytbtdlk

Substitution Cipher

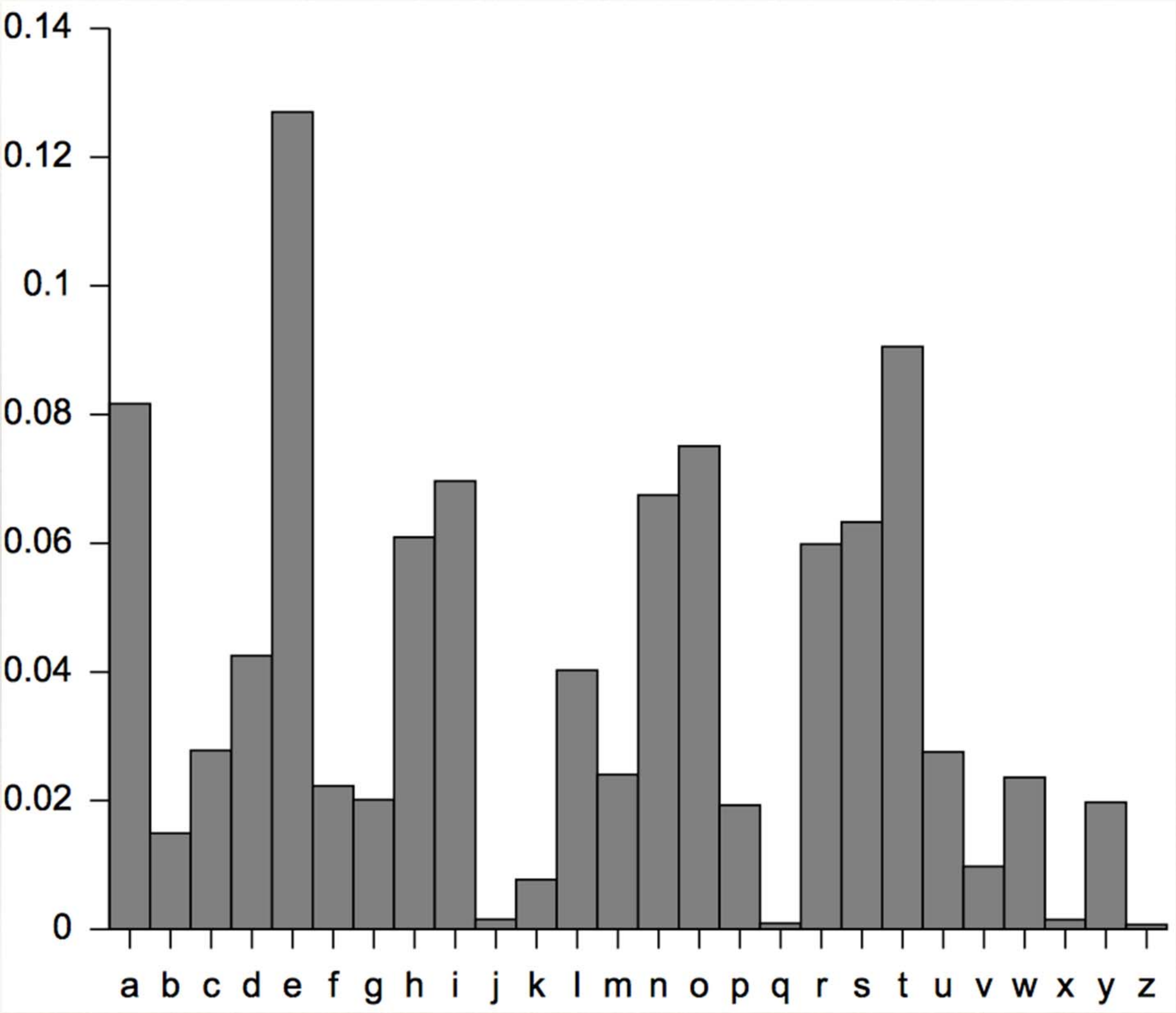
- Substitute each letter of the plaintext.



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

- Example:
  - Plaintext - send reinforcements
  - Key - knowledge of the mapping of the alphabet
  - Ciphertext - ktdp jtfdoejytbtdlk

Frequency Analysis



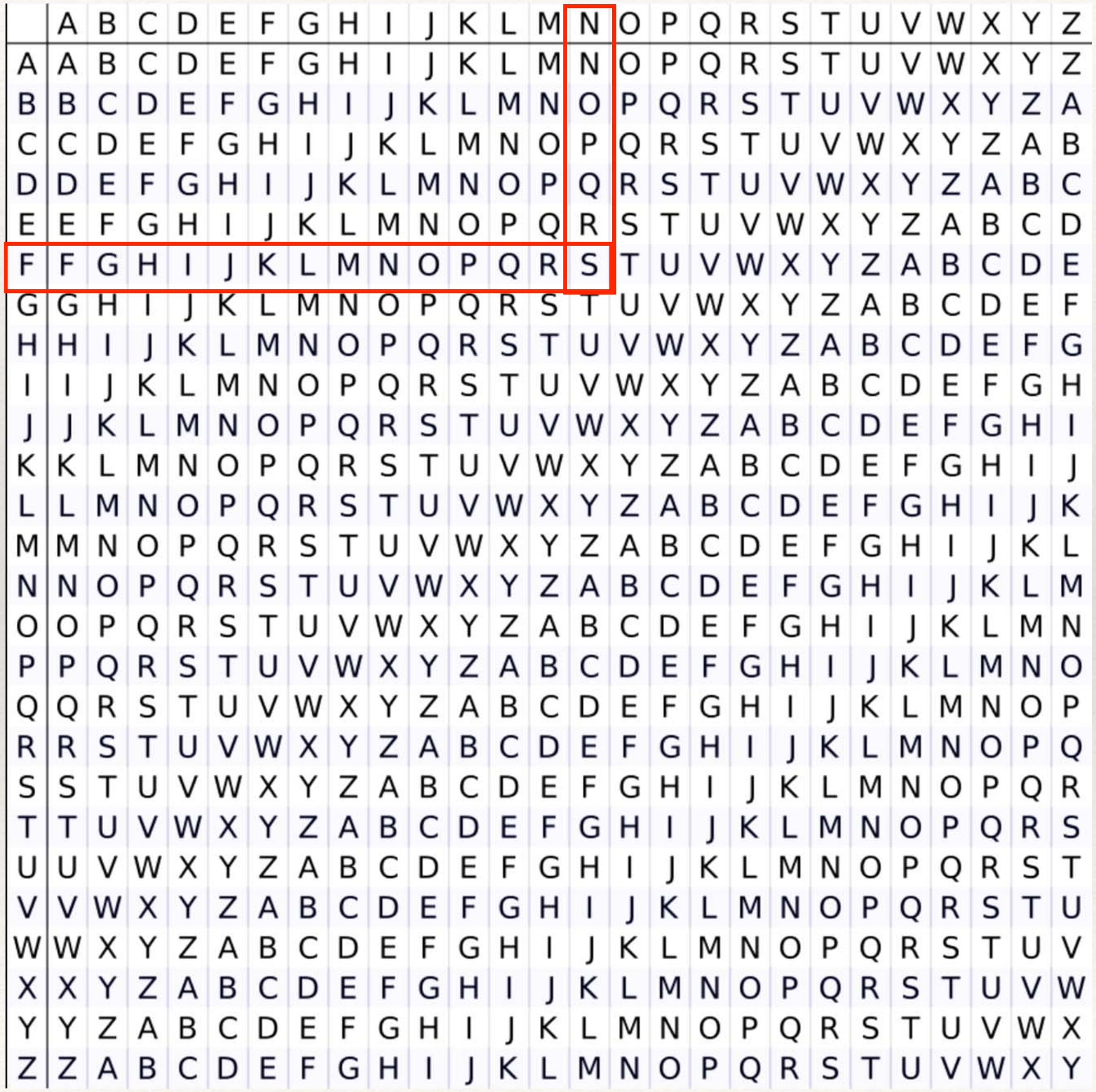
Vigenere Cipher

- Extend the key to be the length of the plaintext.
- Plaintext $P=P_1P_2P_3..$ Ciphertext $C=C_1C_2C_3..$
- Encryption: $C_i = (P_i + k_i) \bmod 26$
- Decryption: $P_i = (C_i - k_i) \bmod 26$

Vigenere Cipher

- To encrypt:
  - Extend the key to be the length of the plaintext.
  - Use the Vigenere Table to get the ciphertext.
- Example:
  - Plaintext: NINE ONE ONE AND ONE ONE TWO
  - Key: FOUR FOU RFO URF OUR FOU RFO
  - Ciphertext: SWHV TBY FSS UEI CHV TBY KBC

Vigenere Cipher

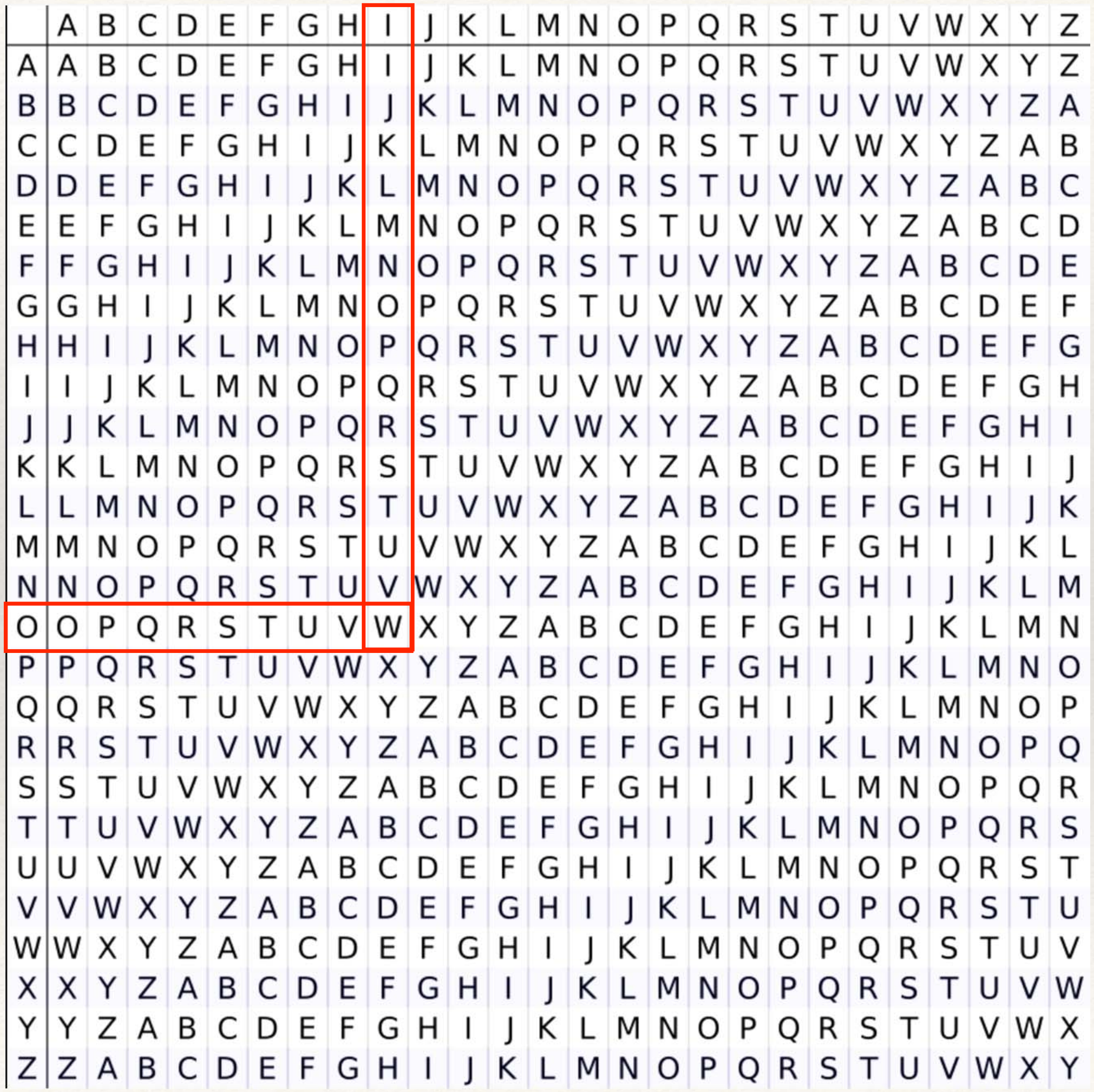


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Vigenere Cipher

- To encrypt:
  - Extend the key to be the length of the plaintext.
  - Use the Vigenere Table to get the ciphertext.
- Example:
  - Plaintext: NINE ONE ONE AND ONE ONE TWO
  - Key: FOUR FOU RFO URF OUR FOU RFO
  - Ciphertext: SWHV TBY FSS UEI CHV TBY KBC

Vigenere Cipher

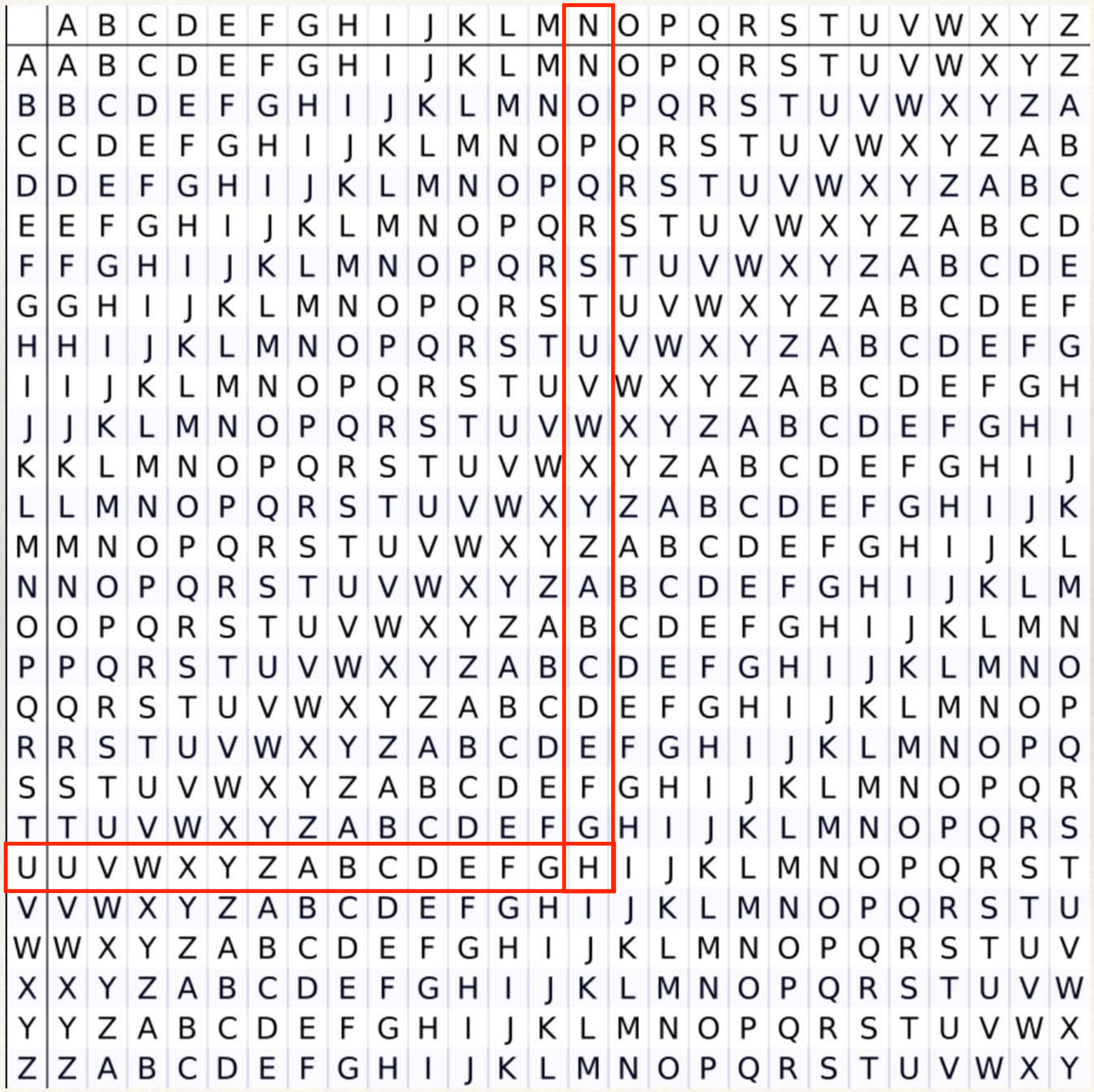


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Vigenere Cipher

- To encrypt:
  - Extend the key to be the length of the plaintext.
  - Use the Vigenere Table to get the ciphertext.
- Example:
  - Plaintext: NINE ONE ONE AND ONE ONE TWO
  - Key: FOUR FOU RFO URF OUR FOU RFO
  - Ciphertext: SWHV TBY FSS UEI CHV TBY KBC

Vigenere Cipher

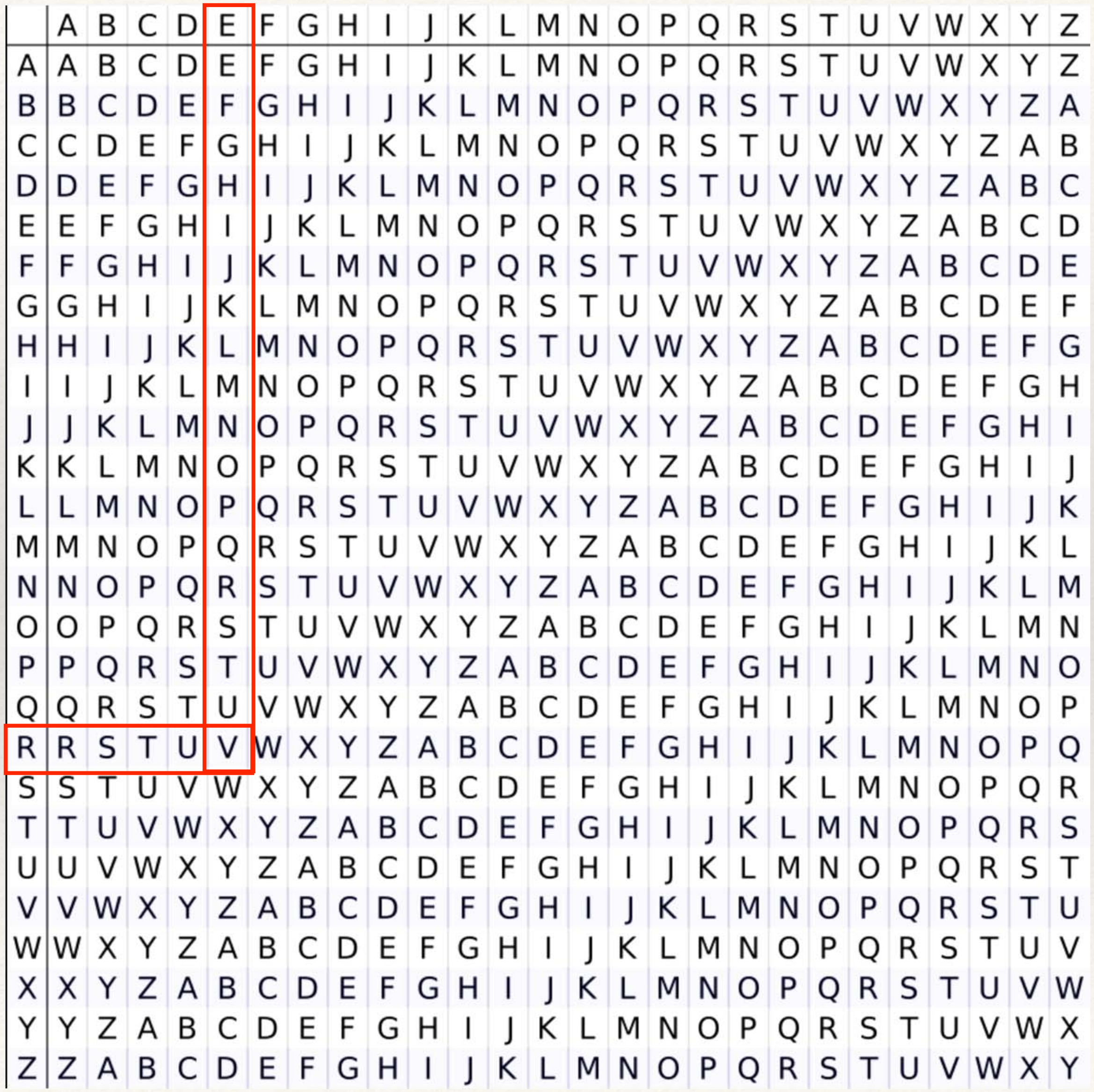


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Vigenere Cipher

- To encrypt:
  - Extend the key to be the length of the plaintext.
  - Use the Vigenere Table to get the ciphertext.
- Example:
  - Plaintext: NINE ONE ONE AND ONE ONE TWO
  - Key: FOUR FOU RFO URF OUR FOU RFO
  - Ciphertext: SWHV TBY FSS UEI CHV TBY KBC

Vigenere Cipher

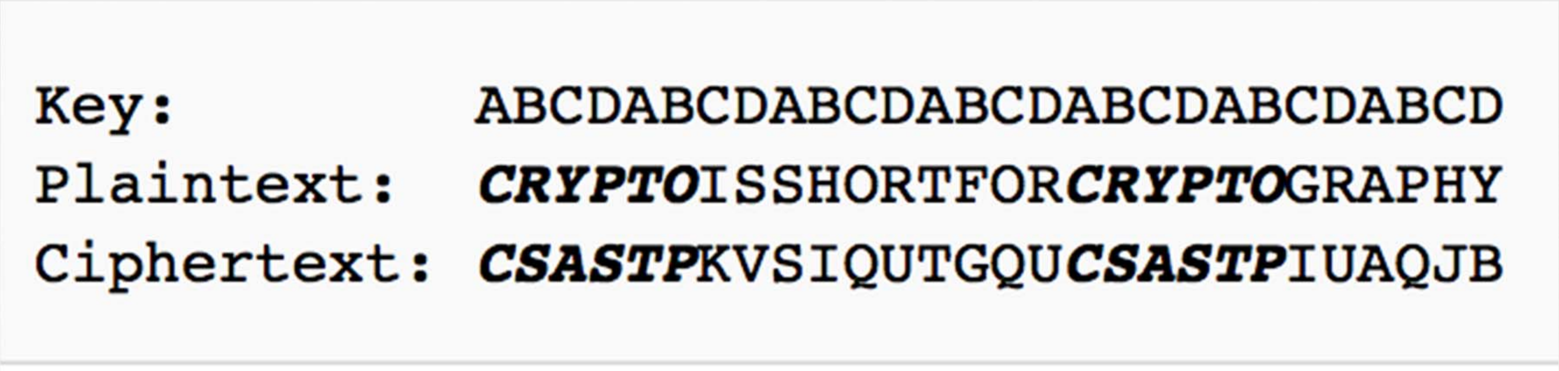


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Vigenere Cipher

Vigenere Cipher

- To break:
  - Look for group(s) of three characters that regularly repeat.
  - Find a common factor for the distance(s) between repeating groups.
  - Do frequency analysis of subsets of the characters.



Key: ABCDABCDABCDABCDABCDABCDABCD

Plaintext: ***CRYPTO***ISSHORTFOR***CRYPTO***GRAPHY

Ciphertext: ***CSASTP***KVSIQUTGQU***CSASTP***IUAQJB

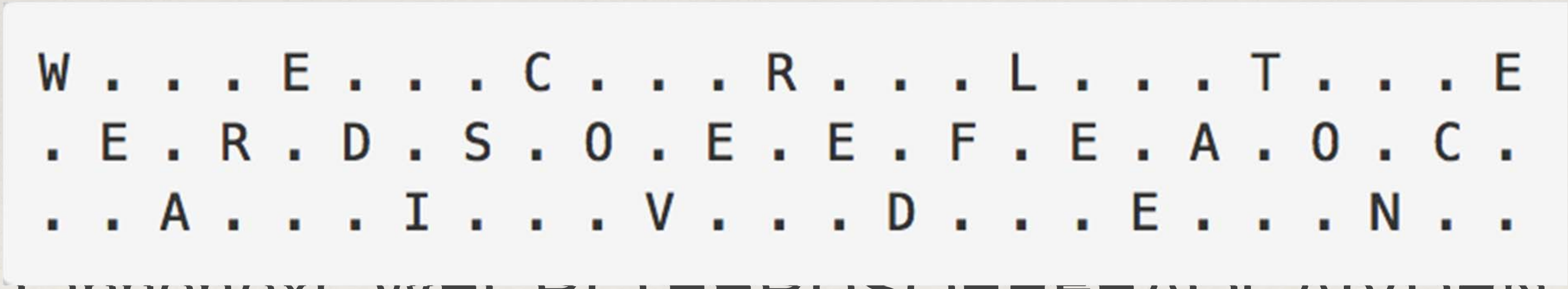
Transposition Ciphers

- Transposition Cipher - a cipher that shifts the original position of each plaintext character. The ciphertext is a permutation of the plaintext.
- Rail Fence Cipher
- Route Cipher

Rail Fence Cipher

- Plaintext is written downwards on “rails” of an imaginary fence, then written upwards when the bottom is reached.

- Plaintext: We are discovered. Flee at once.

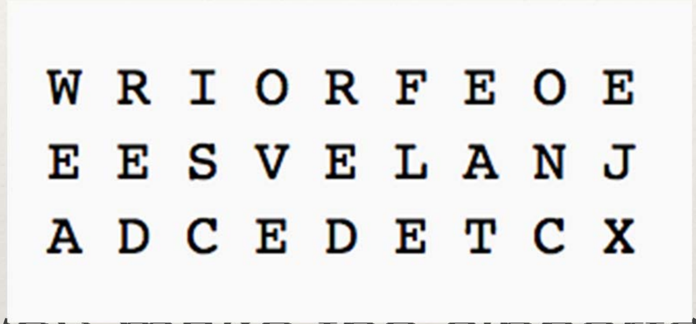


```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

- Ciphertext: WECRLTEERDSOEEFEAOCAIVDEN

Route Cipher

- The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

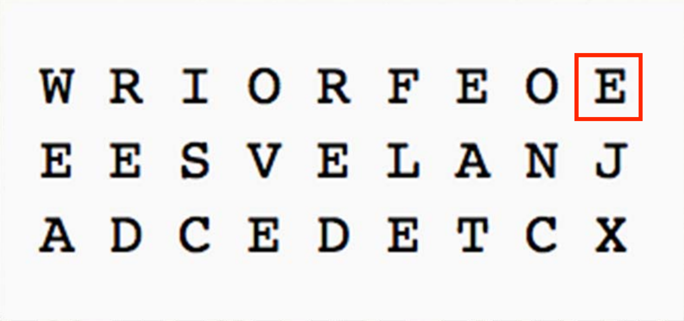


W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

- The key is how you make the ciphertext: “Spiral counter-clockwise, starting from the top right.”
- Ciphertext: EOEFROIRWEADCEDETCXJNALEVSE

Route Cipher

- The plaintext is written on a grid of given dimensions and padded with low-frequency characters.

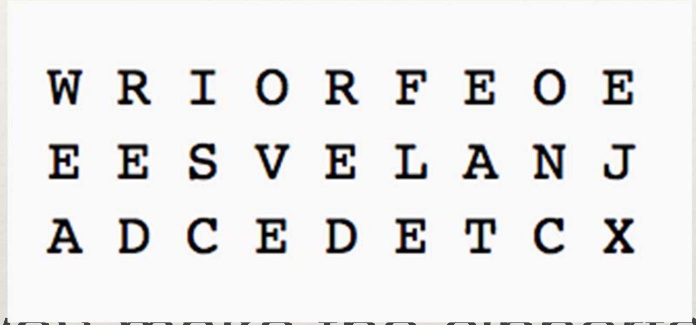


W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

- The key is how you make the ciphertext: “Spiral counter-clockwise, starting from the top right.”
- Ciphertext: EOEFROIRWEADCEDETCXJNALEVSE

Route Cipher

- The plaintext is written on a grid of given dimensions and padded with low-frequency characters.



W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

- The key is how you make the ciphertext: “Spiral counter-clockwise, starting from the top right.”
- Ciphertext: EOEFROIRWEADCEDETCXJNALEVSE

Hash Functions

- Used for integrity, signatures, and password storage.
- Given a bit string of any length, produces a bit string of length n.
- Properties of a good hash function:
  - It is impossible to reverse.
  - It gives a fixed-sized output.
  - Changing one bit of the message changes the hash completely.
  - Hard to find collisions.

Hash Functions

- md5
  - extremely vulnerable to collisions
  - vulnerable to rainbow tables
  - fast (bad)
- sha1
  - less vulnerable to collisions, but still vulnerable
  - also vulnerable to rainbow tables

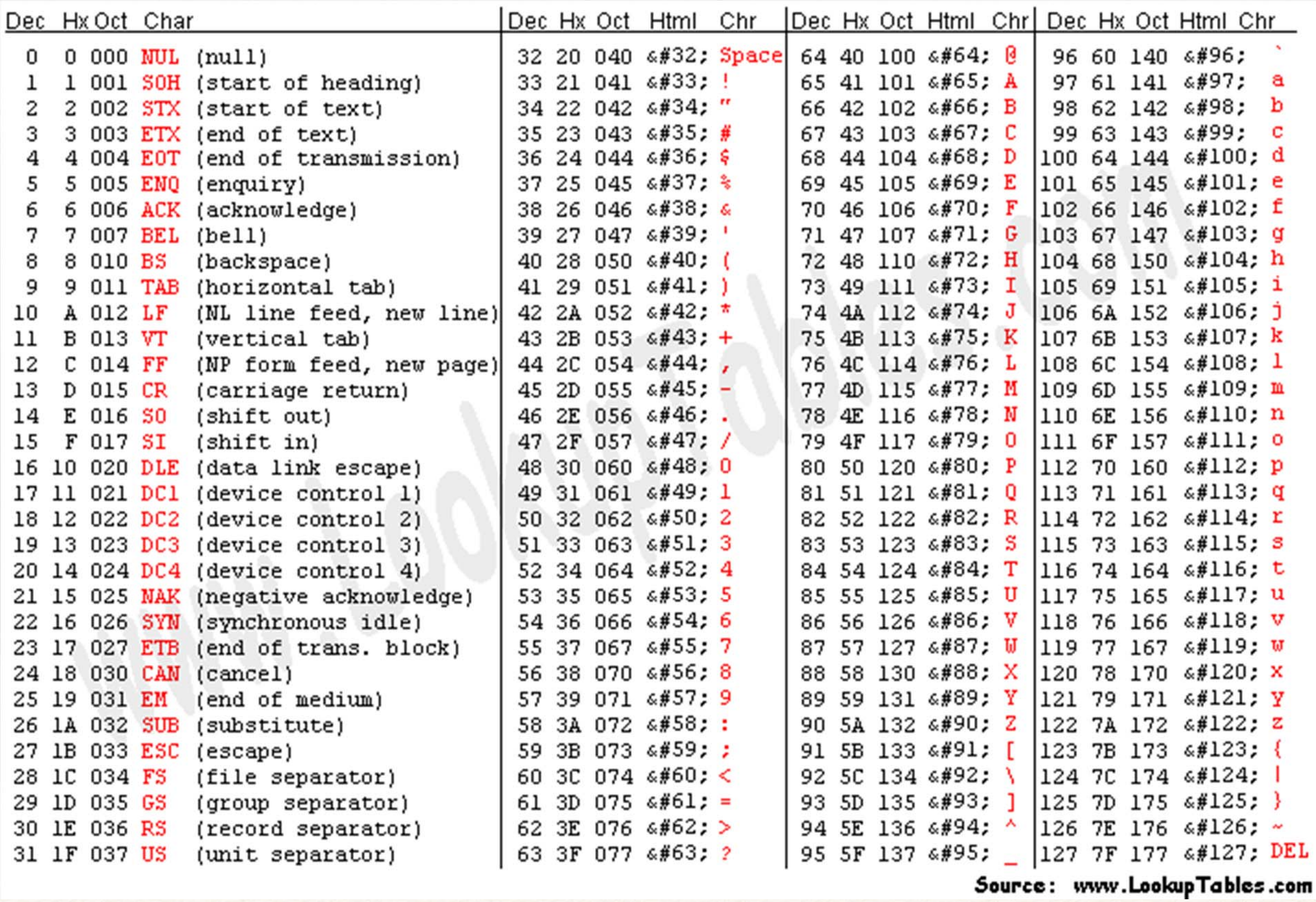
Hash Functions

- Password Storage - need slow hashing algorithm
  - bcrypt, PBKDF2
  - bcrypt - 156 guesses per second (from security.stackexchange)
  - md5 - over 1 billion guesses per second (from security.stackexchange)

Encodings

- Simple encodings of text
  - ASCII - hello
  - Binary - 01101000 01100101 01101100 01101100 01101111
  - Hex - \x68\x65\x6c\x6c\x6f
  - Base64 - aGVsbG8=

ASCII



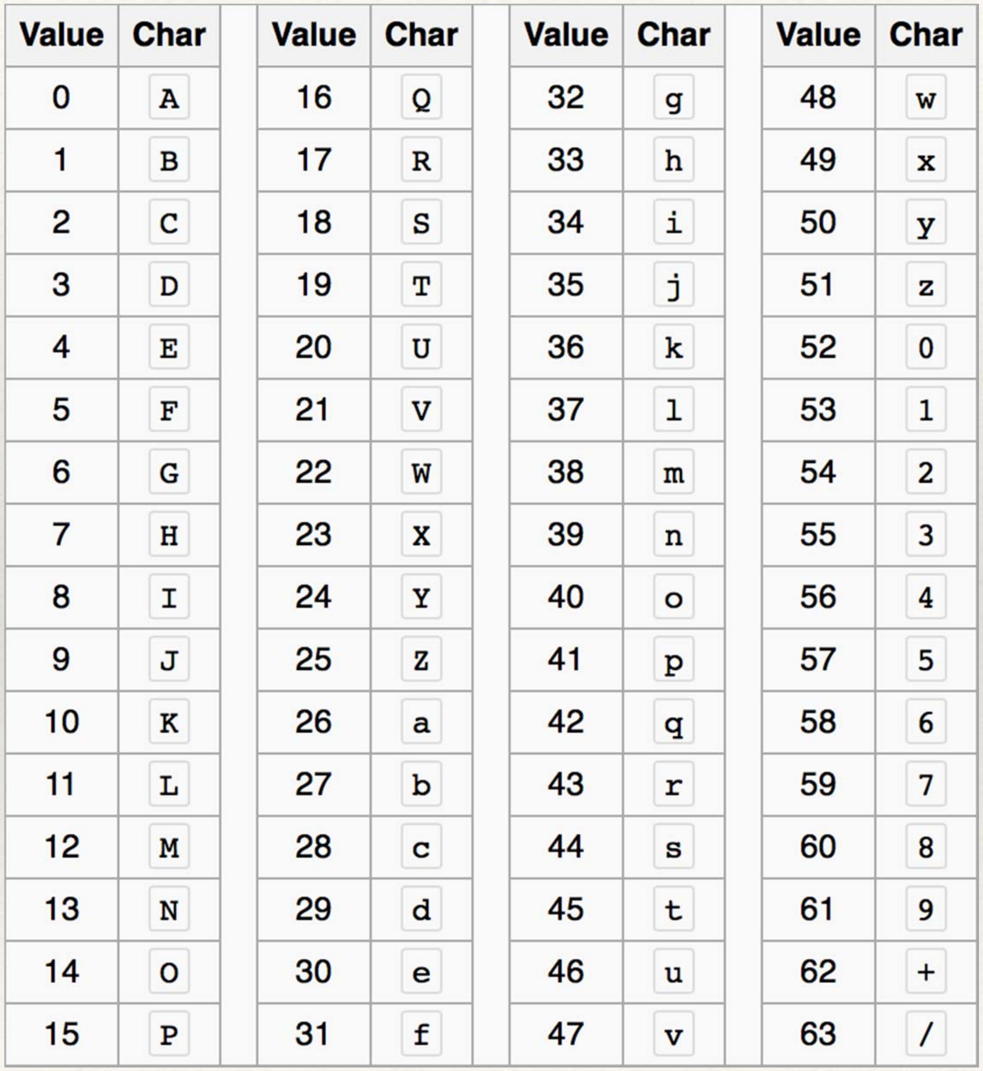
Dec	Hx	Oct	Char		Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL	(null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH	(start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX	(start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX	(end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT	(end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ	(enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK	(acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL	(bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS	(backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB	(horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF	(NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT	(vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF	(NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR	(carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO	(shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI	(shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE	(data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1	(device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2	(device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3	(device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4	(device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK	(negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN	(synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB	(end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN	(cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM	(end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB	(substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC	(escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS	(file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS	(group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS	(record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US	(unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Base64

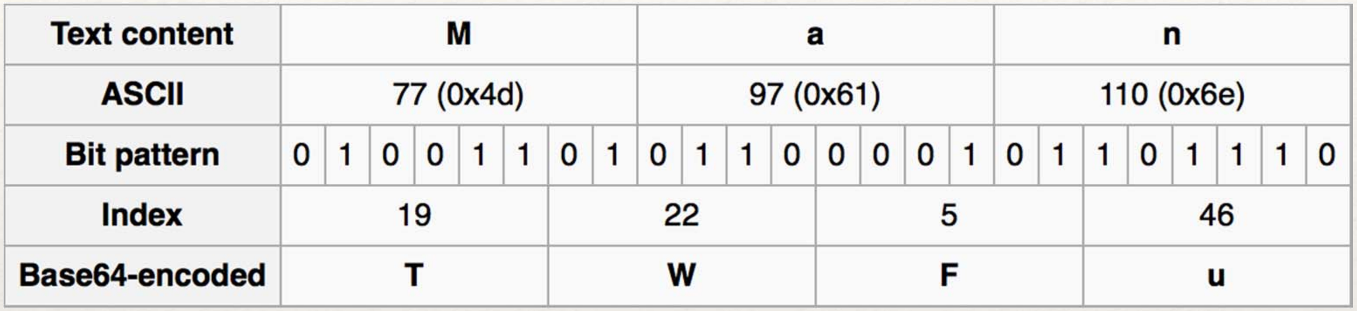
- Used to safely encode ASCII characters such as 10 and 13 (return and newline characters)
- Uses character set {A..Z, a..z, 1-9, +, /} and = for padding
- $2^6 = 64$
- To encode, ASCII is converted to hex, and every 6 bits of hex is converted to its Base64 character

Base64

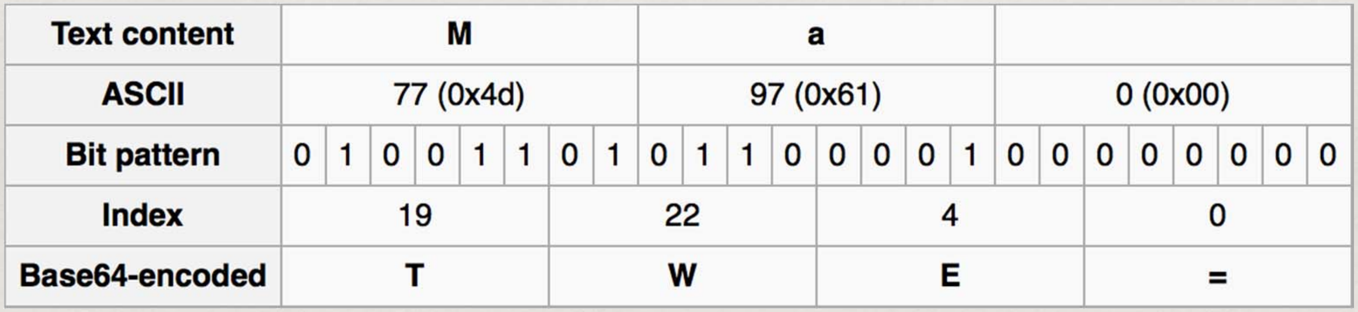


Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Base64



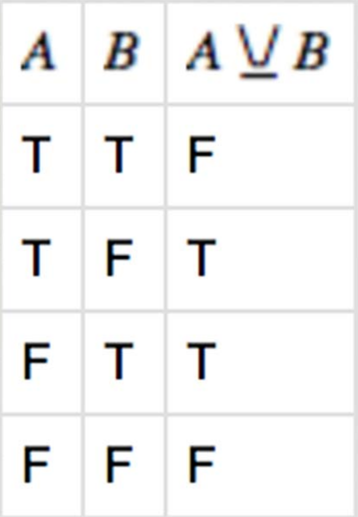
Text content	M								a								n							
ASCII	77 (0x4d)								97 (0x61)								110 (0x6e)							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
Index	19						22						5						46					
Base64-encoded	T						W						F						u					



Text content	M								a															
ASCII	77 (0x4d)								97 (0x61)								0 (0x00)							
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0
Index	19						22						4						0					
Base64-encoded	T						W						E						=					

XOR

- XOR = exclusive-OR
- A xor B = C <=> B xor C = A
- Plaintext xor Key = Ciphertext <=> Ciphertext xor Key = Plaintext <=> Plaintext xor Ciphertext = Key

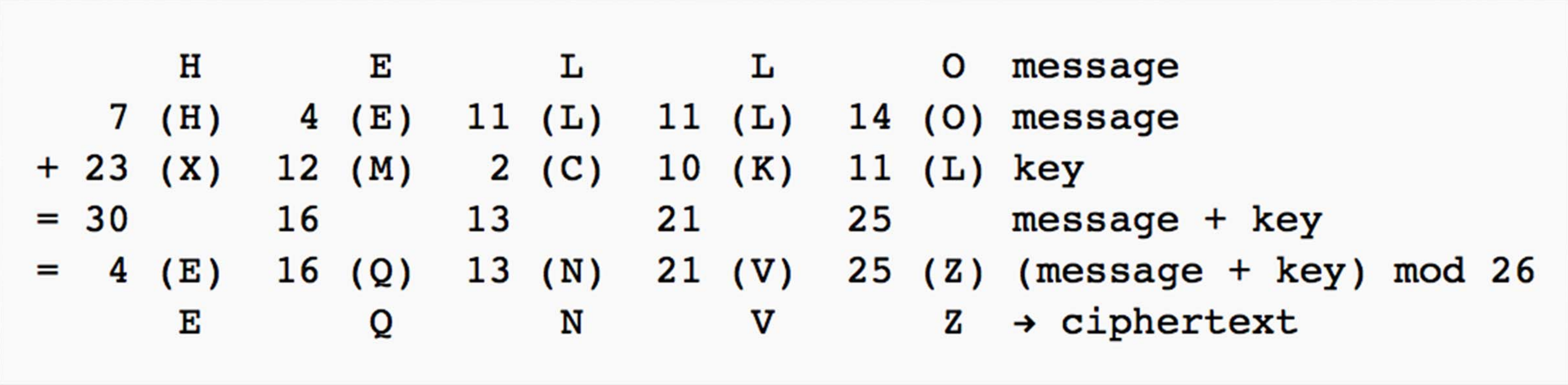


A	B	$A \underline{\vee} B$
T	T	F
T	F	T
F	T	T
F	F	F

One-Time Pad

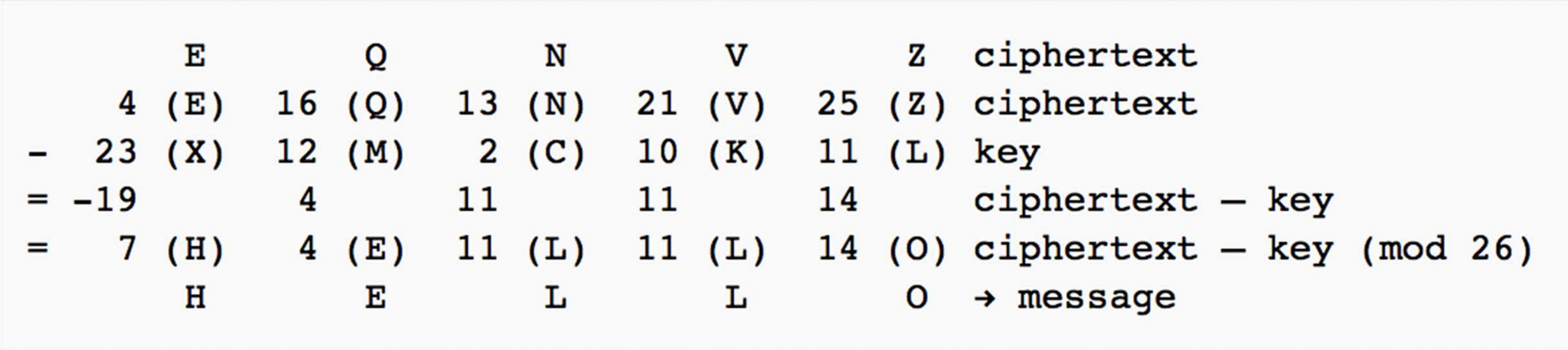
- Used with a random secret key.
- Both parties must have the key.
- The key must be the same length as the plaintext.
- Used by the NSA and KGB.

One-Time Pad



```
       H          E          L          L          O   message
     7 (H)      4 (E)     11 (L)     11 (L)     14 (O) message
+   23 (X)     12 (M)      2 (C)     10 (K)     11 (L) key
=   30         16         13         21         25     message + key
=    4 (E)     16 (Q)     13 (N)     21 (V)     25 (Z) (message + key) mod 26
       E          Q          N          V          Z   → ciphertext
```

One-Time Pad



```
       E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext – key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext – key (mod 26)
       H       E       L       L       O  → message
```

One-Time Pad Complications

- The key must be completely random.
- The key must be known by both parties.
- The key can only be used once, so if you want to send a message to n people, you will need n keys.
- The key must be kept secret.

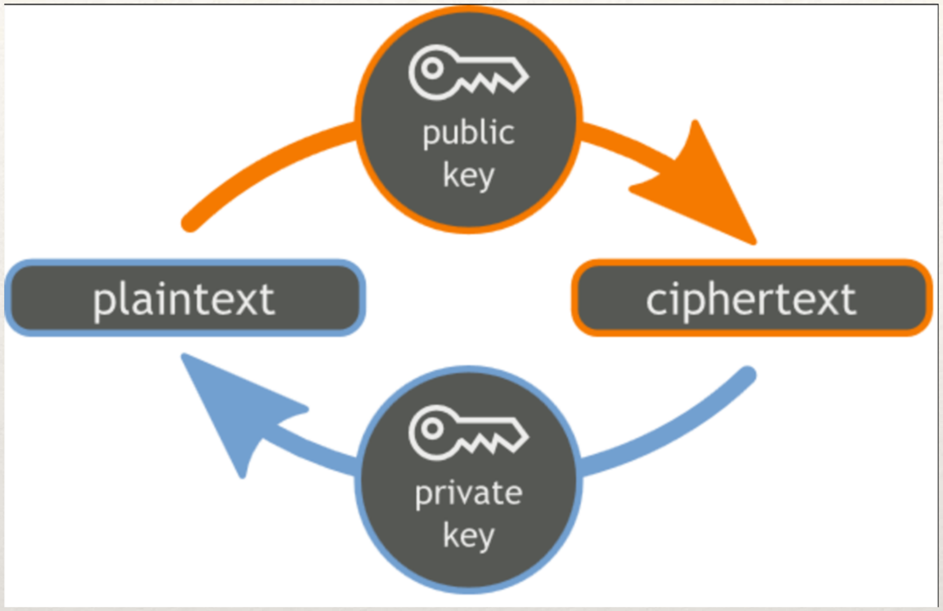
Modern Ciphers

- Symmetric Key Encryption
  - Uses the same key to encrypt and decrypt
  - Alice and Bob share the same key.
- Asymmetric Key Encryption
  - Uses two keys: one to encrypt and one to decrypt.
  - Alice has a public key and a private key.
  - Bob has a public key and a private key.

Symmetric Key Encryption

- Share a secret key among two or more parties
- DES (Data Encryption Standard)
  - Uses a 56-bit key
  - Standard from 1979 to 1990s
- AES (Advanced Encryption Standard)
  - Uses 128, 192, or 256-bit key
  - Standardized in 2001

Asymmetric Key Encryption



- Asymmetric Public Key Cryptography
- Used today to encrypt or sign messages
- Uses a private key and a public key

RSA Algorithm

- Relies on the complexity of factoring large numbers
- Take two primes, p, q, and find N = pq.
- Find Phi(N) = (p-1)(q-1).
- Choose e such that 1 < e < Phi(N) and e and N share no common factors.
- Find d such that (de) mod Phi(N) = 1.
- Public Key is (e, N).
- Private Key is (d, N).

RSA Encryption

- To encrypt, convert message M into hex/binary and calculate $C = M^e \bmod N$, where C is the ciphertext.
- To decrypt C: $M = C^d \bmod N$.
- Difficulty to crack depends on the key length.

Uses of RSA

- Encrypt email with the receiver's public key
- Sign email by encrypting with the sender's private key
- Bloat NSA servers
- Dependent upon the infeasibility of factor large numbers.
- Make sure you keep your private key a secret.

NOVEMBER 4 – 5

TexSAW

2016

6th ANNUAL

TEXAS SECURITY AWARENESS WEEK

ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE

Celebrating 30 Years

THE UNIVERSITY OF TEXAS AT DALLAS

Presenting Sponsor

StateFarm®

Supporting Sponsor

Raytheon

State Farm and the State Farm logo are registered trademarks of State Farm Mutual Automobile Insurance Company.