INFORMATION ASSURANCE AND SECURITY

James Patrick L. Galvan

Cryptography

TODAY'S OBJECTIVE

1. Explain the basic principles of cryptography
2. Describe the operating principles of the most popular cryptographic tools
3. List and explicate the major protocols used for secure communications

Cryptography

Greek words **kryptos**, meaning **“hidden”,**
and **graphien**, meaning **“to write”.**

The process of making and using codes to secure the transmission of information.

Cryptology

The science concerned with
data communication and storage in secure and usually secret form.

Encompasses cryptography and cryptanalysis.

Plaintext

Cryptanalysis is the process of obtaining the original message.

Ciphertext

An encrypted message without knowing the algorithms and keys used to perform the encryption.

Encryption

The process of converting an original message into a form that is unreadable to unauthorized individual.

Decryption

The process of converting the ciphertext message back into plaintext so that it can be readily understood.

Rail Fence Cipher

The Rail Fence Cipher (also called a Zigzag Cipher) is an easy to apply transposition cipher that jumbles up the order of the letters of a message in a quick convenient way. It also has the security of a key to make it a little bit harder to break.

Example: Encipher **“CAN YOU READ THIS MESSAGE,”** using a rail fence cipher.

Rail Fence Cipher

An example of a “transposition cipher,” one which doesn’t change any letters when enciphered.

Example: Encipher “CAN YOU READ THIS MESSAGE,” using a rail fence cipher.

C N O R A T I M S A E
A Y U E D H S E S G

Plaintext : CAN YOU READ THIS MESSAGE
Ciphertext : CNORATIMSAE AYUEDHSESG

Rail Fence Cipher

“DO NOT DELAY IN ESCAPING”

Plaintext :
Ciphertext :
Rail Fence Cipher :

Rail Fence Cipher

“DO NOT DELAY IN ESCAPING”

Plaintext : DO NOT DELAY IN ESCAPING
Ciphertext : DNTEAIECPN OODLYNSAIG
Rail Fence Cipher :

D N T E A I E C P N
O O D L Y N S A I G

Rail Fence Cipher

“INFORMATION TECHNOLOGY”

Plaintext :
Ciphertext :
Rail Fence Cipher :

Rail Fence Cipher

“INFORMATION TECHNOLOGY”

Plaintext : INFORMATION TECHNOLOGY
Ciphertext : IFRAINEHOOY NOMTOTCNLG
Rail Fence Cipher :

I F R A I N E H O O Y
N O M T O T C N L G

Rail Fence Cipher

B T C A S S
L N P N I S R U E E S
U E L E L

Plaintext :
Ciphertext :
Rail Fence Cipher :

Rail Fence Cipher

B T C A S S
L N P N I S R U E E S
U E L E L

Plaintext : BLUNT PENCILS ARE USELESS
Ciphertext : BTCASS LNPNISRUEES UELEL
Rail Fence Cipher :

B T C A S S
L N P N I S R U E E S
U E L E L

Rail Fence Cipher

```
I     T     R     J     L     T     D     O
  M   W   D   U   I   E   I   N
N   E   I   S   M   D   T
  O   I   M   T   I   E   I
```

Plaintext :
Ciphertext :
Rail Fence Cipher :

Rail Fence Cipher

```
I     T     R     J     L     T     D     O
  M     W     D     U     I     E     I     N
N     E     I     S     M     D     T
  O     I     M     T     I     E     I
```

Plaintext : IM NOT WEIRD IM JUST LIMITED EDTION
Ciphertext : ITRJLTDO NWDUIEIN NEISMDT OIMTIEI
Rail Fence Cipher :

Rail Fence Cipher

ILMSEEEM FYMEWMCO OCONEOON NONSRRM

Plaintext :
Ciphertext :
Rail Fence Cipher :

Rail Fence Cipher

ILMSEEEM FYMEWMCO OCONEOON NONSRRM

Plaintext : IF ONLY COMMON SENSE WERE MORE COMMON
Ciphertext : ILMSEEEM FYMEWMCO OCONEOON NONSRRM
Rail Fence Cipher :

I L M S E E E M
F Y M E W M C O
O C O N E O O N
N O N S R R M

Rail Fence Cipher

I E E A O O I E

N V R P L G Z D

I M O R F R H T

A S R Y O T A

Plaintext :

Ciphertext :

Rail Fence Cipher :

Rail Fence Cipher

```
I       E       E       A       O       O       I       E
  N   V   R   P   L   G   Z   D
I   M   O   R   F   R   H   T
  A   S   R   Y   O   T   A
```

Plaintext : I NEVER APOLOGIZED I AM SORRY FOR THAT
Ciphertext : IEEAOOIE NVRPLGZD IMORFRHT ASRYOTA
Rail Fence Cipher :

Null Cipher

A null cipher, also known as concealment cipher, is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. Today it is regarded as a simple form of steganography, which can be used to hide ciphertext.

Null Cipher

Ciphertext :

WALK IN NEW NAP EARLS ROLLY SWINGS
NEVER EVER VAILS ETIQUETTE RIGHTS
QUAILS UNICORN IN THIS SHOES

Plaintext : **WINNERS NEVER QUITS**

Null Cipher

Ciphertext :

BXMT SSESSBW POE ILTWQS
ABM BXEZ RIA QBTNMAAD
OPMNIKQT RMI MNDLJ ALNN
BRIGH PIG ORHD LLTYQ

Plaintext : **MEET ME AT MIDNIGHT**

Null Cipher

Ciphertext :

AMY GLO ELYU BLANCA CLAIR GENE BLAIRE
DAIN MILO KLAIU BLING HANNAH

Plaintext : **YOU ARE ENOUGH**

Null Cipher

Ciphertext :

News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The [highway is not] knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

Plaintext : **Newt is upset because he thinks he is President**

CAESAR CIPHER

In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

CAESAR CIPHER

Using the key of shift of 3 to the right, encrypt the word **“CRYPTOGRAPHY”**

K = 3 RIGHT

CAESAR

Using the key of shift of 3 to the right, encrypt the word
“CRYPTOGRAPHY”

K = 3 RIGHT

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 Q R S T U V W X Y Z

Plaintext : CRYPTOGRAPHY
Ciphertext : FUBSWRJUDSKB

CAESAR

Decrypt the ciphertext, **“DOO LV ZHOO”** using the key of 3 shift to the left.

K = 3 LEFT

CAESAR

Decrypt the ciphertext, **“DOO LV ZHOO”** using the key of 3 shift to the left.

K = 3 LEFT

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 Q R S T U V W X Y Z

Plaintext : ALL IS WELL
Ciphertext : DOO LV ZHOO

Caesar Cipher

He who laughs last didn’t get it

Plaintext : HE WHO LAUGHS LAST DIDN’T GET IT
Ciphertext : KH ZKR ODXJKV ODVW GLGQW JHW LW

Smiles are contagious, be a carrier

Plaintext : SMILES ARE CONTAGIOUS BE A CARRIER
Ciphertext : VPLOHV DUH FRQWDJLRXV EH D FDUULHU

Caesar Cipher

Learn sign language, it’s very handy

Plaintext : LEARN SIGN LANGUAGE ITS VERY HANDY
Ciphertext : OHDUQ VLJQ ODQJXDJH LWV YHUB KDQGB

Life is always rocky when you’re a gem

Plaintext : LIFE IS ALWAYS ROCKY WHEN YOURE A GEM
Ciphertext : OLIH LV DOZDBV URFNB ZKHQ BRXUH D JHP

Caesar Cipher

Home: Where I can look ugly and not care

Plaintext : HOME WHERE I CAN LOOK UGLY AND NOT CARE
Ciphertext : KRPH ZKHUH L FDQ ORRN XJOB DQG QRW FDUH

Caesar Cipher

QHYHU MXGJH D ERRN EB LWV PRYLH

Plaintext : NEVER JUDGE A BOOK BY ITS MOVIE
Ciphertext : QHYHU MXGJH D ERRN EB LWV PRYLH

KRZ GR WUHHV DFFHVV WKH LQWHUQHW WKHB ORJ LQ

Plaintext : HOW DO TREES ACCESS THE INTERNET THEY LOG IN
Ciphertext : KRZ GR WUHHV DFFHVV WKH LQWHUQHW WKHB ORJ LQ

Caesar Cipher

VRPHWLPHV ZKHQ L FORVH PB HBHV L FDQW VHH

Plaintext : SOMETIMES WHEN I CLOSE MY EYES I CANT SEE
Ciphertext : VRPHWLPHV ZKHQ L FORVH PB HBHV L FDQW VHH

FKRFRODWHV PDNHV WKH ZRUOG JR URXQG

Plaintext : CHOCOLATES MAKES THE WORLD GO ROUND
Ciphertext : FKRFRODWHV PDNHV WKH ZRUOG JR URXQG

Caesar Cipher

DV ORQJ DV WKHUH DUH WHVW WKHUH ZLOO EH SUDBHU LQ VFKRROV

Plaintext : AS LONG AS THERE ARE TEST THERE WILL BE PRAYER IN SCHOOLS
Ciphertext : DV ORQJ DV WKHUH DUH WHVW WKHUH ZLOO EH SUDBHU LQ VFKRROV

Caesar Cipher

Thank God I’m an atheist (9)

Plaintext : THANK GOD IM AN ATHEIST
Ciphertext : KYRB XFU ZD YR RKYVZJK

Be strong, I whispered to my WiFi signal. (I3)

Plaintext : BE STRONG I WHISPERED TO MY WIFI SIGNAL
Ciphertext : OR FGEBAT V JUVFCRERQ GB ZL JVSV FVTANY

Caesar Cipher

GNWYMIFD HFPJ NX IJQNHNTZX (‘2I’)

Plaintext : BIRTHDAY CAKE IS DELICIOUS
Ciphertext : GNWYMIFD HFPJ NX IJQNHNTZX

XLVP XLYJ XPXZCTPD (‘I5’)

Plaintext : MAKE MANY MEMORIES
Ciphertext : XLVP XLYJ XPXZCTPD

Caesar Cipher

Mxwc unc hnbcnamjh cjtn dy cxx vdlq xo cxmjh(‘9’)

Plaintext : Dont let yesterday take up too much of today
Ciphertext : Mxwc unc hnbcnamjh cjtn dy cxx vdlq xo cxmjh

tw s jsaftgo af kgewgfw wdkwk udgmv (‘8’)

Plaintext : be a rainbow in someone elses cloud
Ciphertext : tw s jsaftgo af kgewgfw wdkwk udgmv

Caesar Cipher

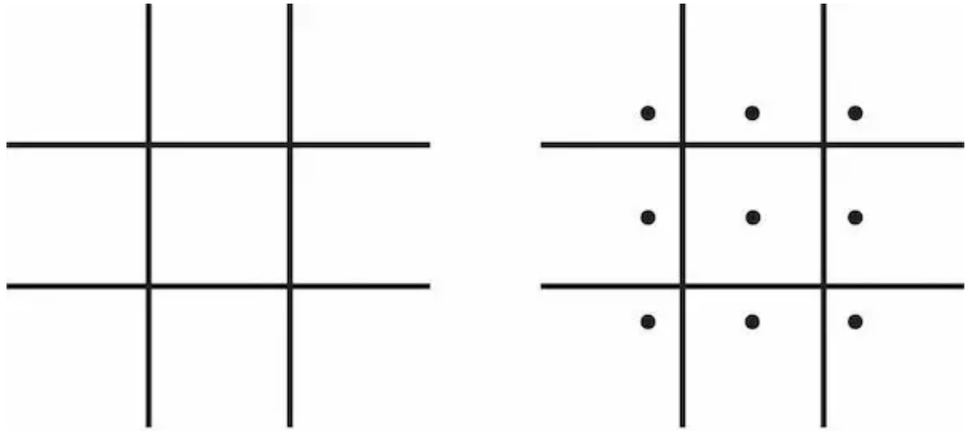
Qy gus yhwiohnyl guhs xyzyunm von qy gomn hin vy xyzyunyx. (20)

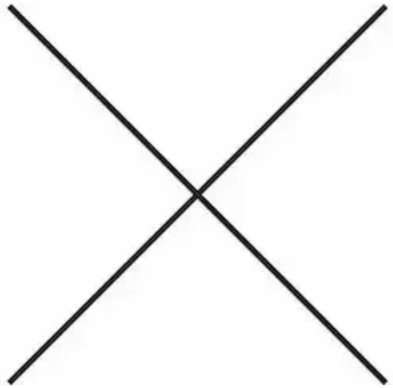
Plaintext : We may encounter many defeats but we must not be defeated
Ciphertext : Qy gus yhwiohnyl guhs xyzyunm von qy gomn hin vy xyzyunyx

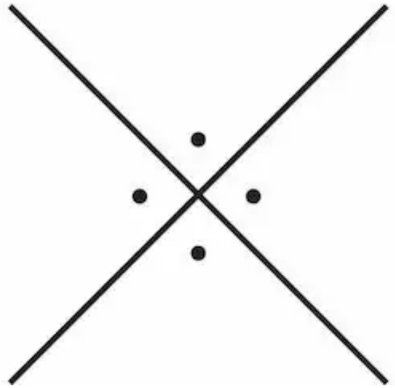
Pigpen Cipher

The pigpen cipher is a simple substitution cipher in which letters of an original message (plaintext) are substituted by geometric symbols creating a coded message (ciphertext).

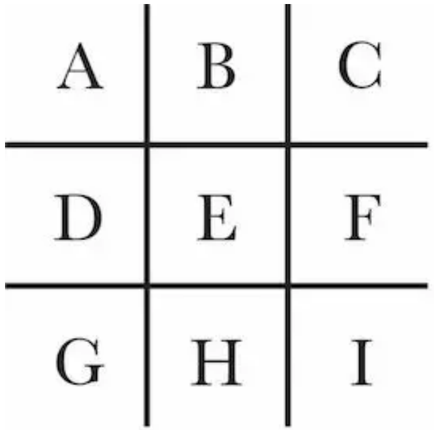
Pigpen Cipher

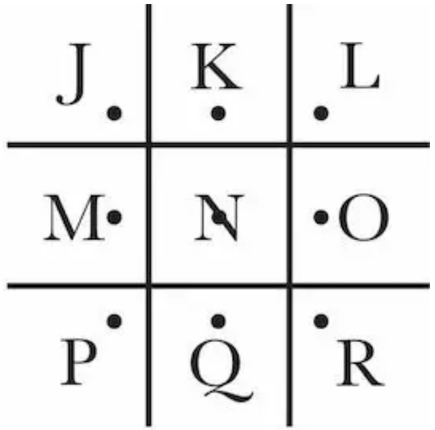




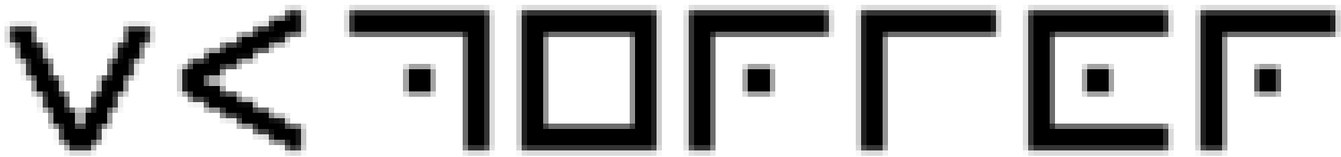


Pigpen Cipher





Pigpen Cipher



SUPERIOR

Pigpen Cipher

BRAIN DAMAGE

Pigpen Cipher

It takes guts to be an organ donor

Pigpen Cipher

fifty shades of tired

Pigpen Cipher

Keep the dream alive and hit the snooze button

Pigpen Cipher

I solemnly swear that I am up to no good

Pigpen Cipher

Life is short and so I am

Pigpen Cipher

A true friend stabs you in front

Pigpen Cipher

When nothing goes right, go left

Pigpen Cipher

I licked it so its mine

Pigpen Cipher

I am athletic I surf the Internet every day

Pigpen Cipher

Autocorrect has become my worst enema

Vigenere Cipher

Vigenere Cipher is an encryption and decryption algorithm. It is a type of polyalphabetic substitution cipher, which means that the cipher alphabet is changed regularly during the encryption process. Due to this, the cipher becomes less vulnerable to cryptanalysis.

	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

MAKE IT HAPPEN

K = BSIT

Vigenere Cipher

Conquer from within
K = best

Dsfjvij ysse pjxzbo

Vigenere Cipher

To be or not to be That is the question
K = hamlet

Ao np sk uof es ul Ttlx bz ttp unlsftsg

Vigenere Cipher

The quick brown fox jumps over the lazy dogs.
K = cat

Vhx subek utopp fhz jnopl qvxt tag ltby wqgl.

Morse Code

Morse code is a method used in telecommunication to encode text characters as standardized sequences of two different signal durations, called dots and dashes, or dits and dahs.

Morse Code

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 −−●●

Morse Code

Do It Now

-.. --- / .. - / -. --- .--

Morse Code

Yes You Can

-.-- . … / -.-- --- ..- / -.-. .- -.

Morse Code

Live love laugh

.-.. .. ...- . / .-.. --- ...- . / .-.. .- ..- --. ....

Morse Code

… . .. --.. . / - …. . / -.. .- -.--

seize the day

Morse Code

.. / .- -- / -.. .. ..-. ..-. . .-. . -. -

I am Different

Morse Code

--. --- --- -.. / ...- .. -... . ... / --- -. .-.. -.--

Good Vibes Only

Binary Cipher

A	00001	J	01010	S	10011
B	00010	K	01011	T	10100
C	00011	L	01100	U	10101
D	00100	M	01101	V	10110
E	00101	N	01110	W	10111
F	00110	O	01111	X	11000
G	00111	P	10000	Y	11001
H	01000	Q	10001	Z	11010
I	01001	R	10010		

Assignment

***Long Bond Paper**

10 Rail Fence Cipher (max of 10 words)

5 Ciphertext *(answerable by 2 lines)*

5 Rail Fence Cipher (2-4 lines)

5 null Cipher (max of 10 words)

5 Ciphertext

10 Caesar Cipher (key) (max of 15 words)

5 plaintext

5 ciphertext

10 Pigpen Cipher (max of 15 words)

5 plaintext
5 ciphertext

5 Vigenere Cipher (key) (max of 10 words)

5 plaintext

10 Morse Code (max of 10 words)

5 plaintext
5 ciphertext

10 Binary cipher (max of 5 words)

5 plaintext
5 ciphertext

Believe. We are in the middle line. Keep hustling to the finish line.

THANK YOU!

Have a great day ahead.