Cryptography

Cyber Security Fundamentals

Steganography = Hiding a message within a text

Example: **This is an actual message from a German spy**

Coding Rule: read second letter in each word

- The Message:

  " Apparently, neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affect pretext for embargo on by products, ejecting suets and vegetable oils".

- Apply the rule:

  "Apparently, neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affect pretext for embargo on by products, ejecting suets and vegetable oils."

- The hidden message:

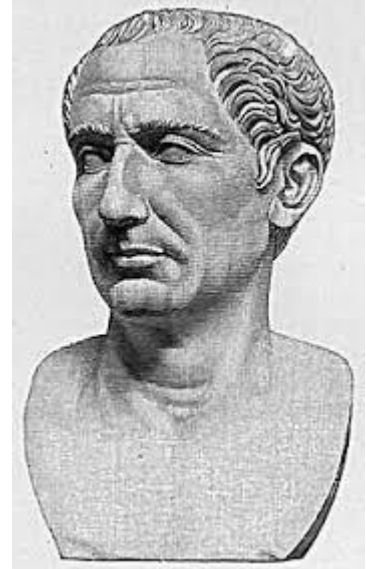 **"Pershing Sails from NY June 1"**

Caesar Cipher

= shifts each letter in the alphabet with the same distance

Example:

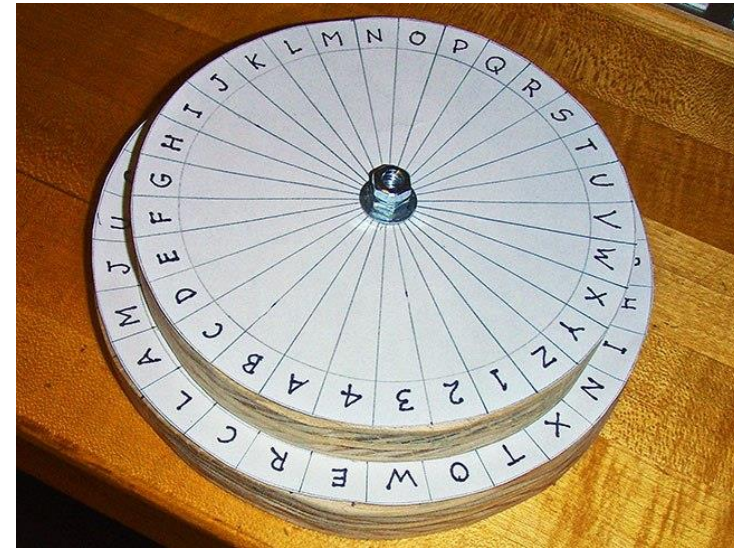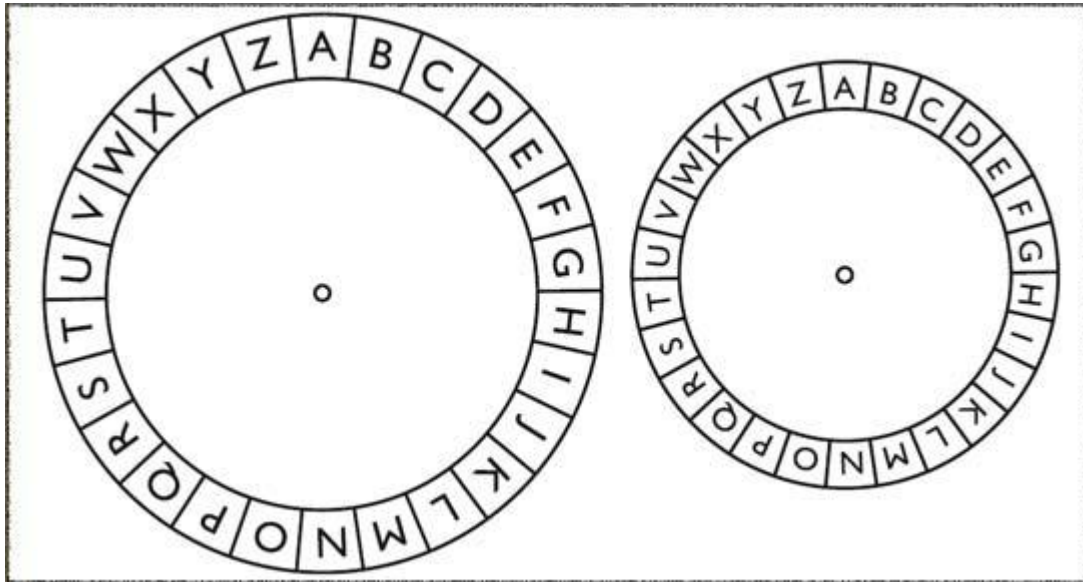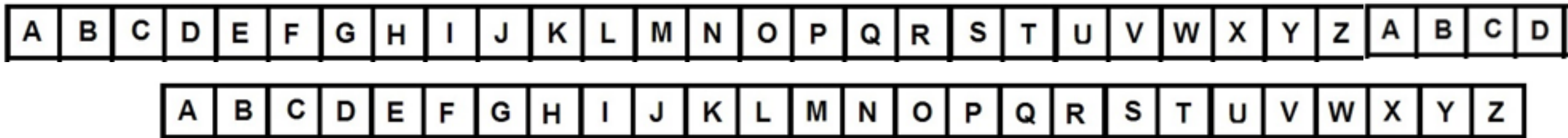| A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Alphabet shifted by 3 spaces.

- The Message:
  " **IF YOU CAN DREAM IT YOU CAN DO IT** ".

- Apply the rule:
  "**LI BRX FDQ GUHDP LW BRX FDQ GR LW**"

- The hidden message:
  "**LIBRXFDQGUHDPLWBRXFDQGRLW**"
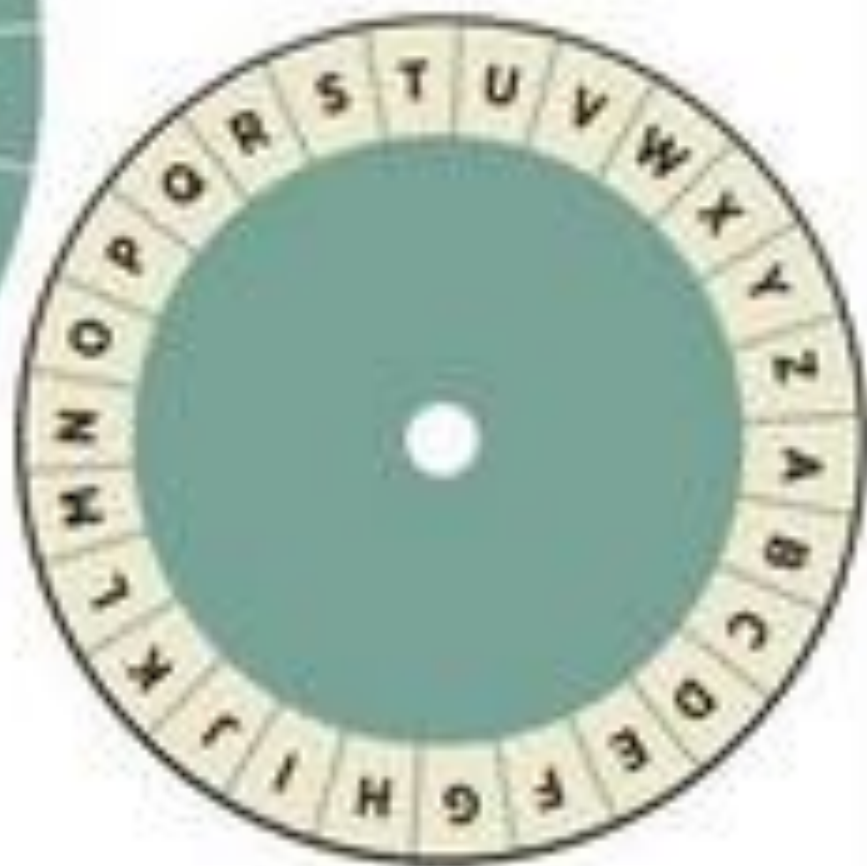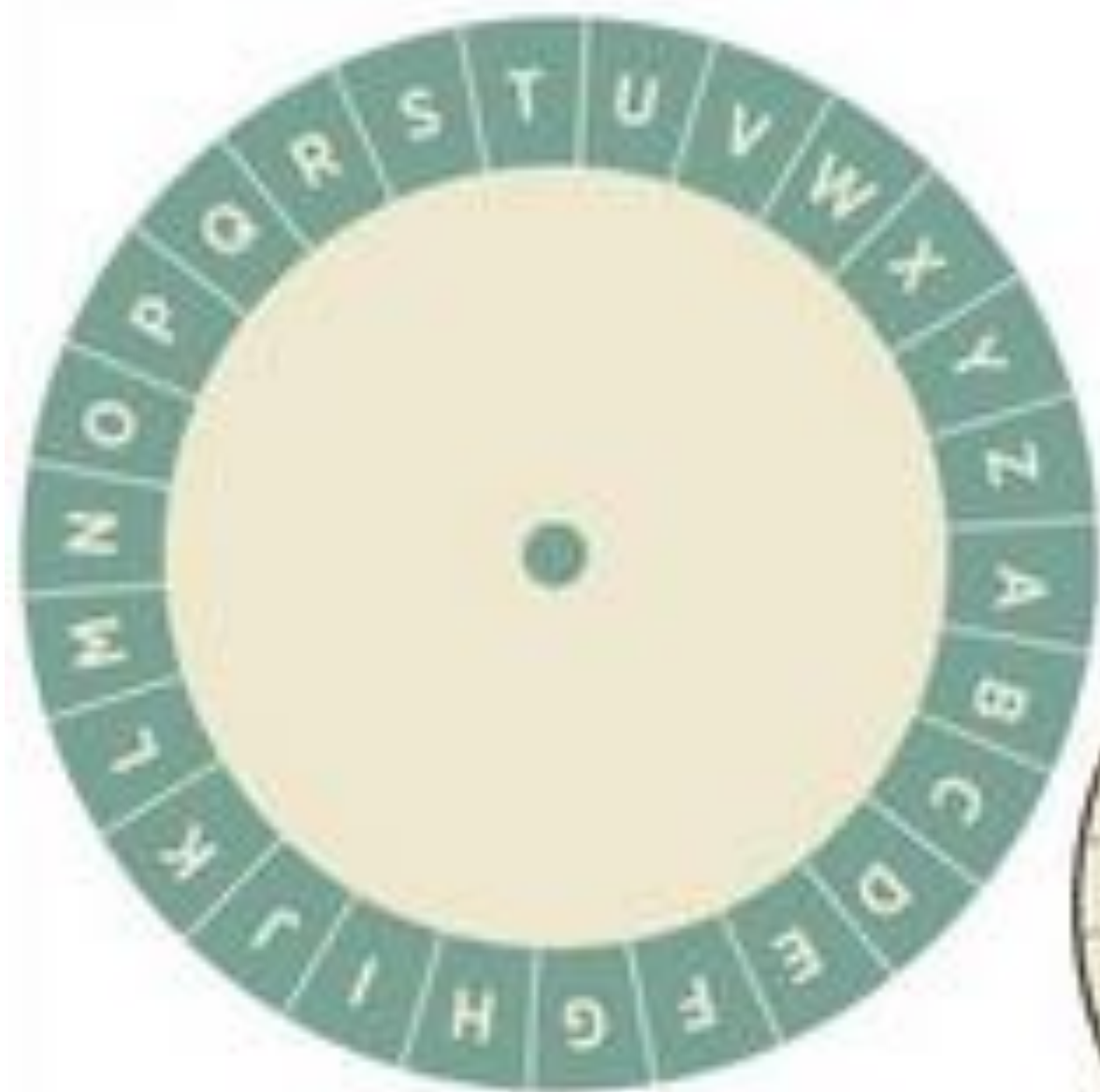
Build your own Caesar Cipher

A Caesar Cipher Disc:

Or a Caesar Cipher Sliding Ruler:

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	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	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	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	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	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	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	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	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

Can You Decode a Message with Caesar Cipher?

Assume two friends are meeting. The first one talking says:

KL! KRZ DUH BRX?

Can you tell what he was saying?

He used Caesar Cipher to code his message. What was the key number for the shift?

The ROUTE Cipher

= a type of transposition cipher
= write the text in a grid of a given dimension; use a specified rule to read the text

MESSAGE=   WE ARE DISCOVERED. FLEE AT ONCE

THE RULE:
Use a 3x9 grid
Read the text
       "*spiral inwards,*
       clockwise,
       starting from the top right"
Group letters in 9-letters groups.

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

ENCRIPTED MESSAGE=   EJXCTEDEC DAEWRIORF EONALEVSE

The RAIL Cipher

= a type of transposition cipher
= write the text in a grid of a given dimension; read the text on rows

MESSAGE= **WE ARE DISCOVERED. FLEE AT ONCE**

THE RULE:
Write the message on the grid in a zig-zag pattern.
Read the text on rows. Group the letters in 5 letters groups.

```
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 . .
```

ENCRIPTED MESSAGE= **WECRL TEERD SOEEF EAOCA IVDEN**

The Columnar Cipher

= a type of transposition cipher

= use a keyword for the grid; replace letters of the keyword with a number in alphabetical order; read the text on columns in the order specified by the numbers

MESSAGE=   WE ARE DISCOVERED. FLEE AT ONCE

THE RULE:
Keyword: **ZEBRAS ➔ 6-3-2-4-1-5**

Read the columns in order.
Group the letters in groups of 5 letters

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E					

ENCRIPTED MESSAGE=   EVLNA CDTES EAROF ODEEC WIREE