2

Substitution Ciphers

Data is often encoded, or converted into a different

form using a set of rules, and then decoded and changed

back into its original state.

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

2

Example 1

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Using the rules above where A = 1, B = 2, C = 3 etc. decode the following message

20-8-9-19 9-19 6-21-14
THIS IS FUN

2

Why Encode and then Decode Data?
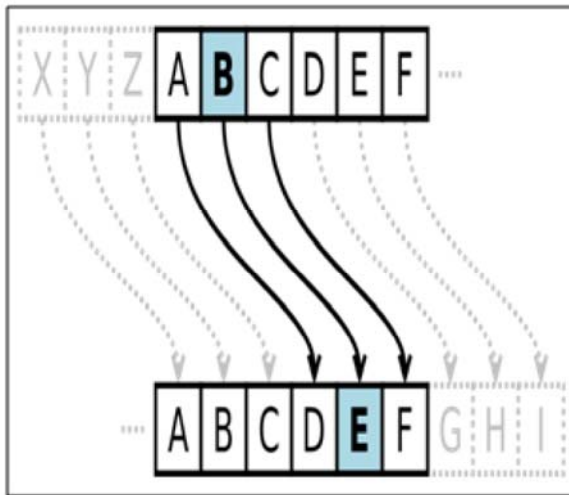
Encoding data allows only for people who know the pattern to decode and understand the data. This comes in handy when you want a specific person to get your message, but want to keep it a secret to everyone else.

2

Example 2

Encoded	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
Decoded	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

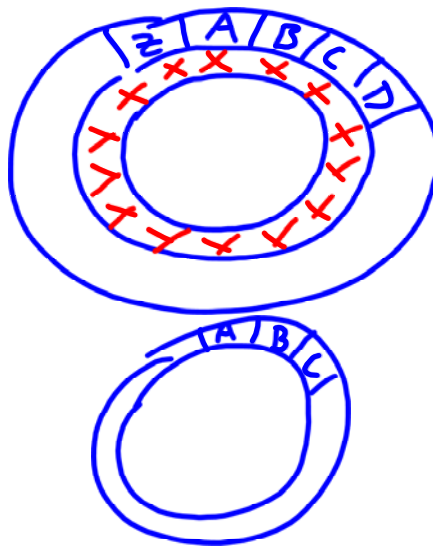Using the code above, decode the following message

ZPV   EJE   JU
YOU   DID   IT

> **2** <u>Caesar cipher:</u> a coding system in which letters are replaced by letters a certain distance ahead in the alphabet.
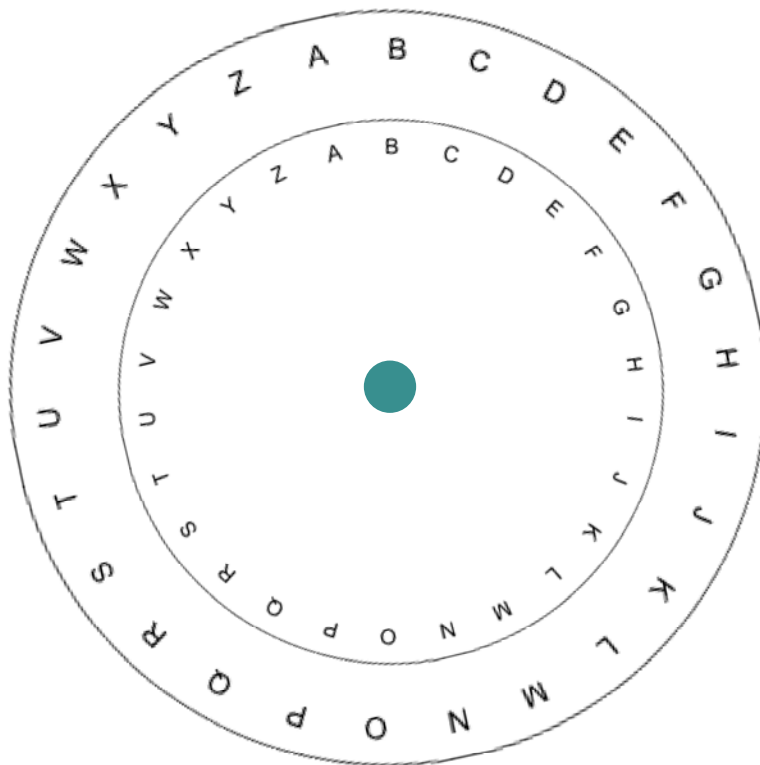
Encode "I love coding" with a key of 3

L oryh frglqj

Decode "hqfxx nx tajw" with a key of 5

Class is over

2

The Caesar Shift Wheel helps a coder to perform a specific "shift" of the alphabet.

Activity