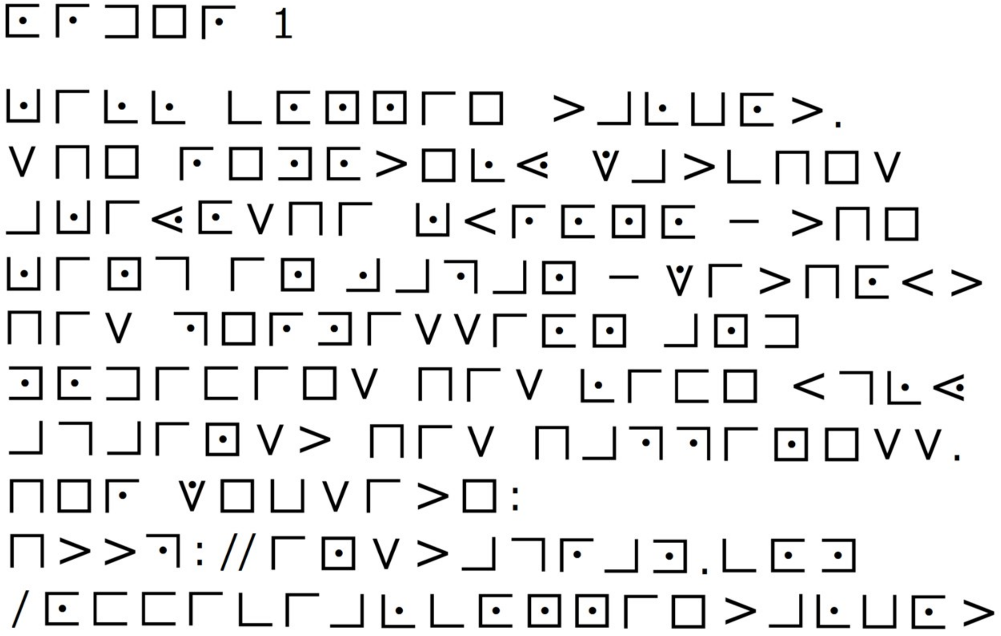
Codes and Cryptography

Let's investigate the Atbash Cipher, the Caesar Shift and the Vigenère Cipher.

Ιπποπόταμος
WoLLoW the HiPPo

The World of Languages
and Languages of the World

Talk to your partner...



This Photo by Unknown author is licensed under CC BY-SA.

- **What codes have you heard of?**
- Morse code or The enigma code.

- **What is a substitution code**?
- Substitution ciphers simply use one letter to stand for another letter.

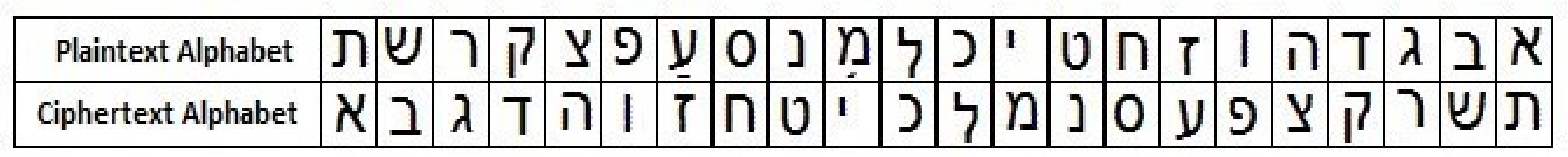
- **What is the difference between a code and a cipher?**
- A **code** affects words,
  a **cipher** affects letters.

Ιπποπόταμος
WoLLoW the HiPPo

The Atbash Cipher

The Atbash Cipher was originally substitution cipher used for the Hebrew alphabet. It is one of the earliest known substitution ciphers to have been used.

The Atbash Cipher simply reverses the plaintext alphabet to create the ciphertext alphabet. That is, the first letter of the alphabet is encrypted to the last letter of the alphabet, the second letter to the penultimate letter and so forth.



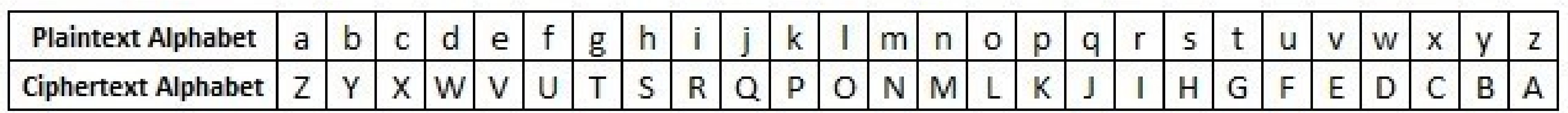
Plaintext Alphabet	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א
Ciphertext Alphabet	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת

This Photo by Unknown author is lic

Ιπποπόταμος
WoLLoW the HiPPo

Can you decrypt my secret messages?

The Roman alphabet would look like this.



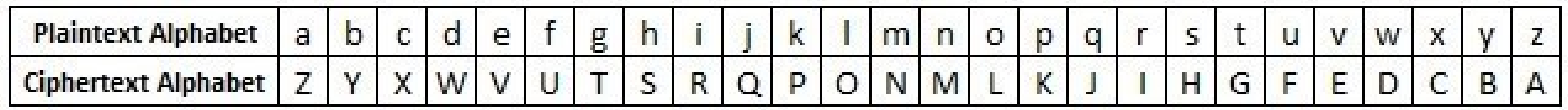
Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

1. ZIHVMZO ZIV GSV YVHG
2. GSV ZGYZHS XCJSVI RH VZHB
3. BLF SZEV MRXV SZRI
4. R DZMG GL YV RM GSV NLFMGZRMS
5. BLFI GVZXSVI RH ZNZARMT

Ιπποπόταμος
WoLLoW the HiPPo

The Atbash Cipher

What could be the problem with this cipher?

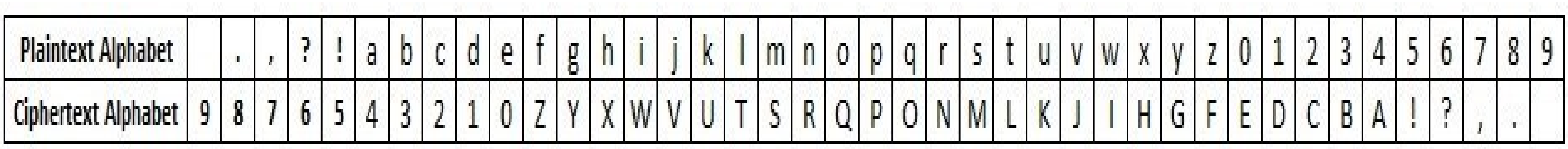


Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

It's too easy!

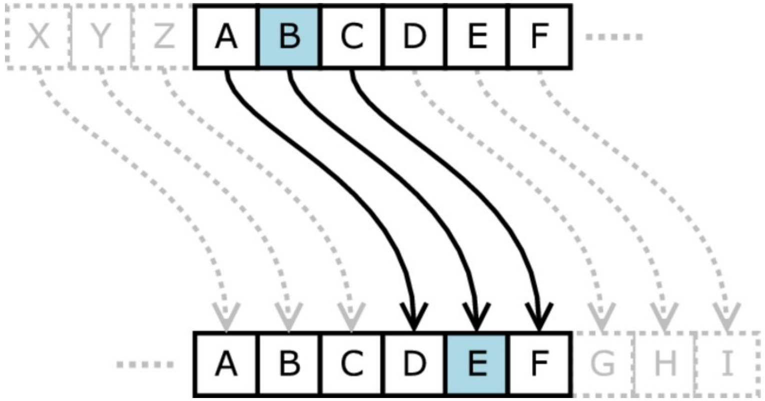
It's a weak substitution cipher.

We could add in punctuation or numbers to make it har



Plaintext 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	0	1	2	3	4	5	6	7	8	9
Ciphertext Alphabet	9	8	7	6	5	4	3	2	1	0	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	!	?	,	.	

This Photo by Un
author is license
CC BY-NC-ND.



Can you work out the rule for the Caesar Shift Cipher?
Talk with your partner.

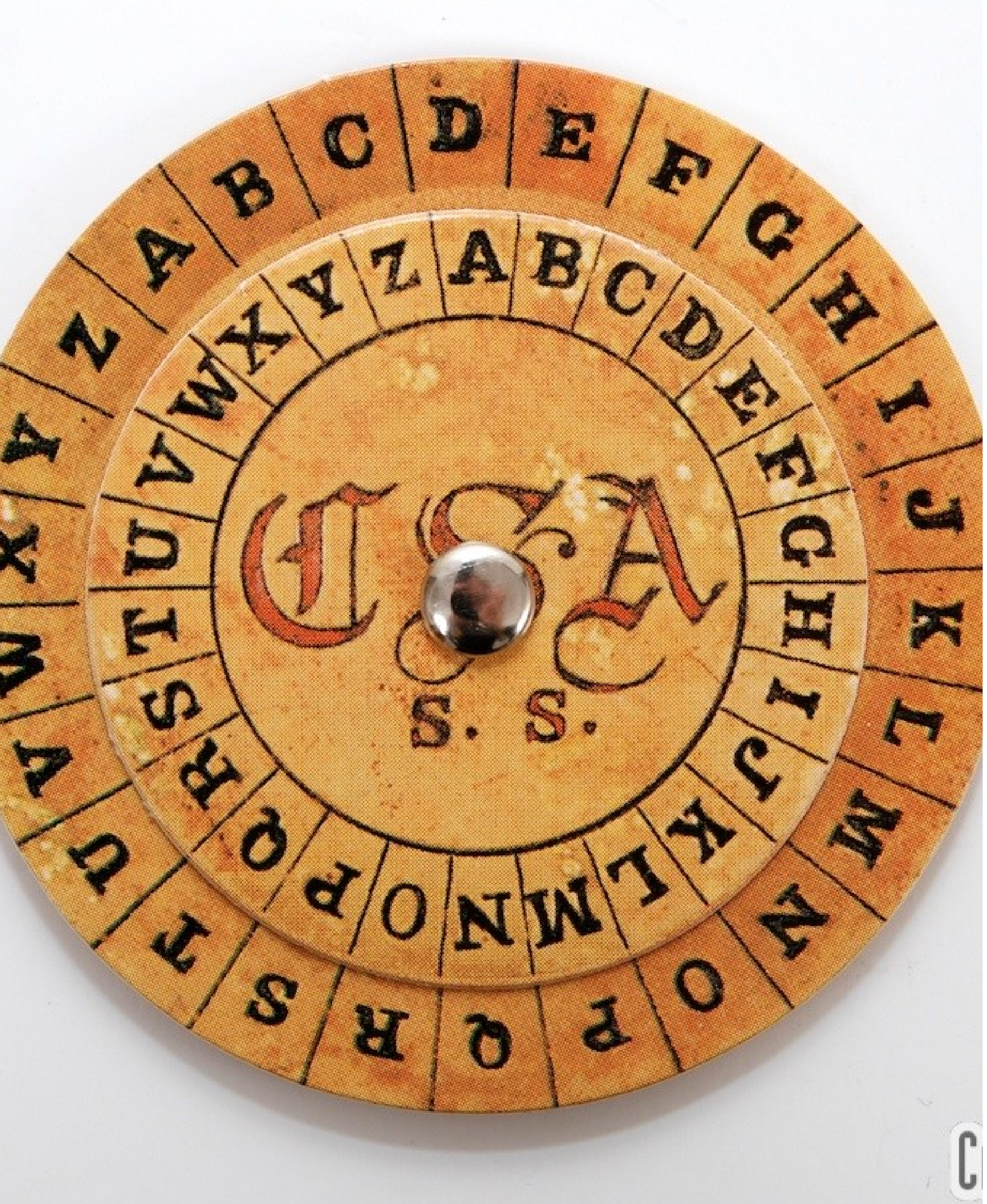
Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher:
XYZABCDEFGHIJKLMNOPQRSTUVW

This example is a Caesar cipher using a rotation of three places i.e. move the letter in the cipher three letters along.

This Photo by Unknown author is licensed under CC BY-SA.

Ιπποπόταμος
WoLLoW the HiPPo



The Vigenère Cipher

- Can you work out how this cipher works?

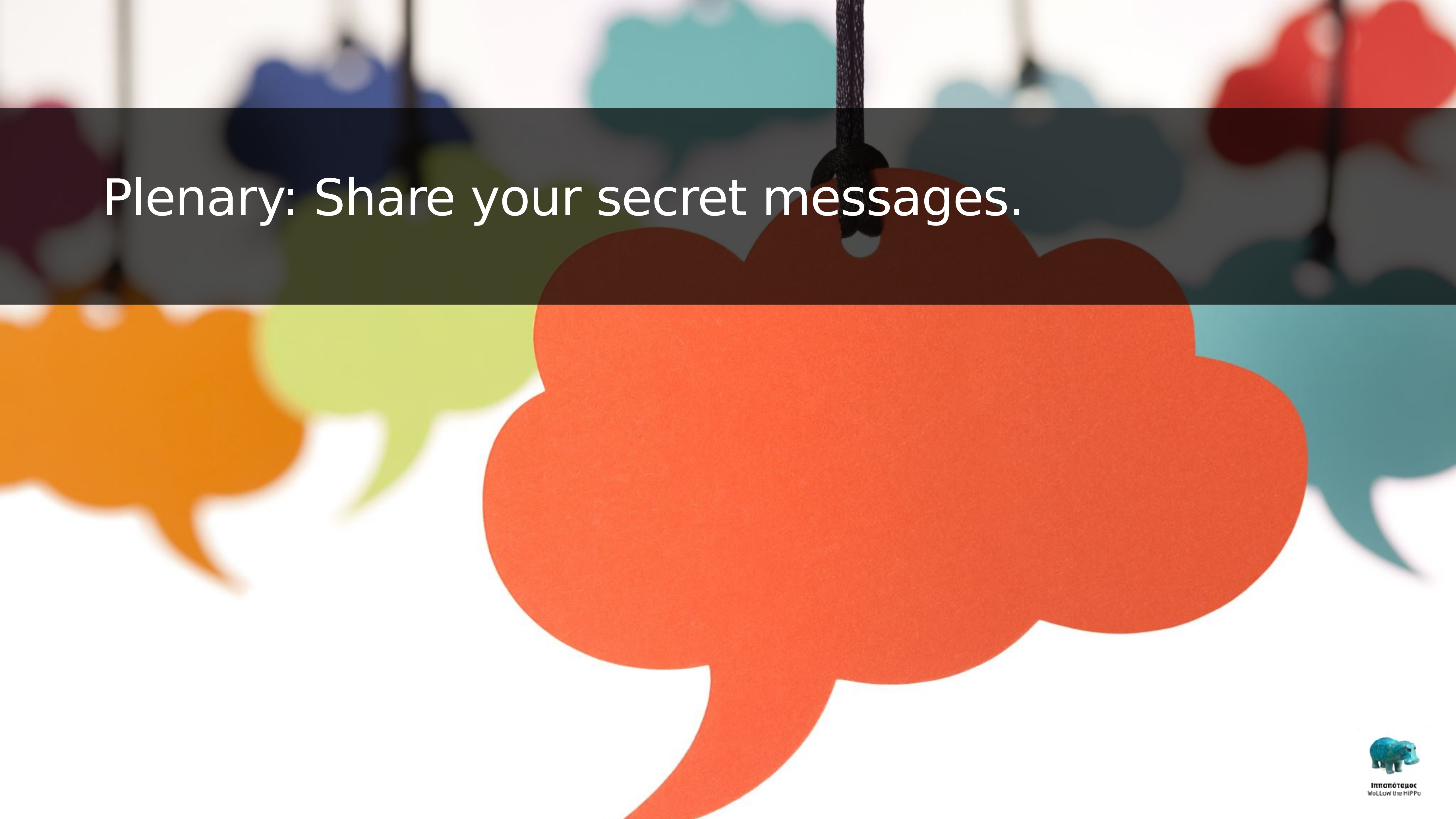
Your go!

Create your own substitution cipher. Work through the worksheet.

Write 3 encrypted messages to your friend along with the secret key.

Swap your secret messages and your secret keys. Can you decrypt them?

Ιπποπόταμος
WoLLoW the HiPPo



Plenary: Share your secret messages.

Ιπποπόταμος
WoLLoW the HiPPo

Acknowledgements

- With thanks to Mary Wenham