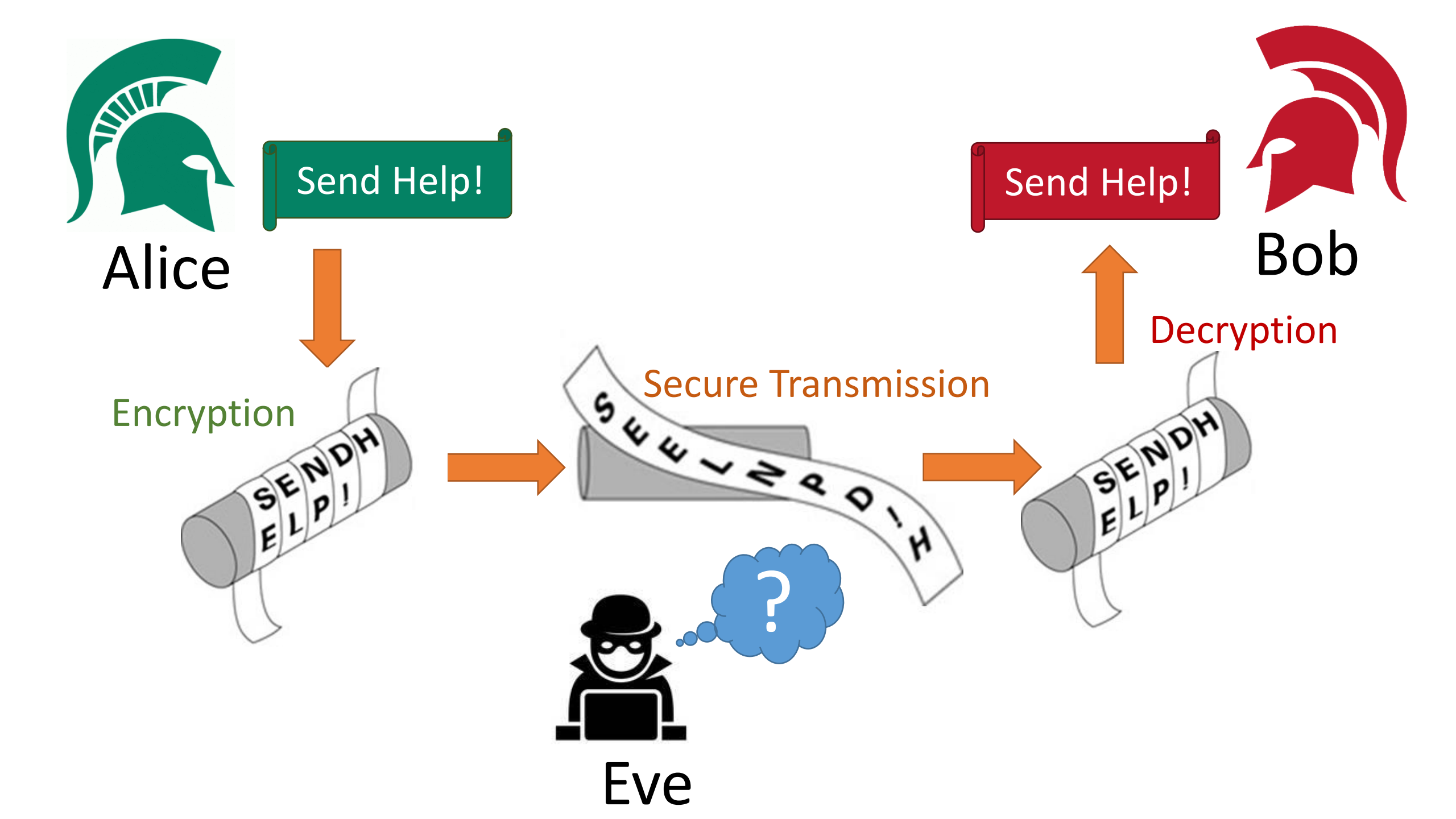
Cryptography

History and Basics

Transposition Ciphers

Spartan Scytale


Alice
Send Help!
Encryption
SENDH ELP!
Secure Transmission
SELNRD!H
?
Eve
Send Help!
Bob
Decryption


Pig
Latin

Alice

HELP

Plaintext

Algorithm: First letter to end AND add ay.

HELP … ELP+H … ELPH+AY

Ciphertext

ELPHAY

Bob

Substitution Ciphers


Caesar
Shift

Alice

HELP

Plaintext

Key: shift of 1 letter

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMNOPQRSTUVWXY

Ciphertext

GDKO

Bob

Alice

HELP

Encryption

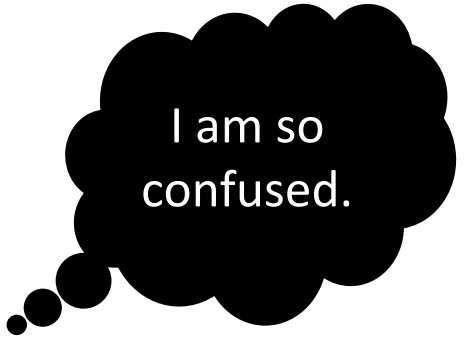
Key: shift of 1 letter

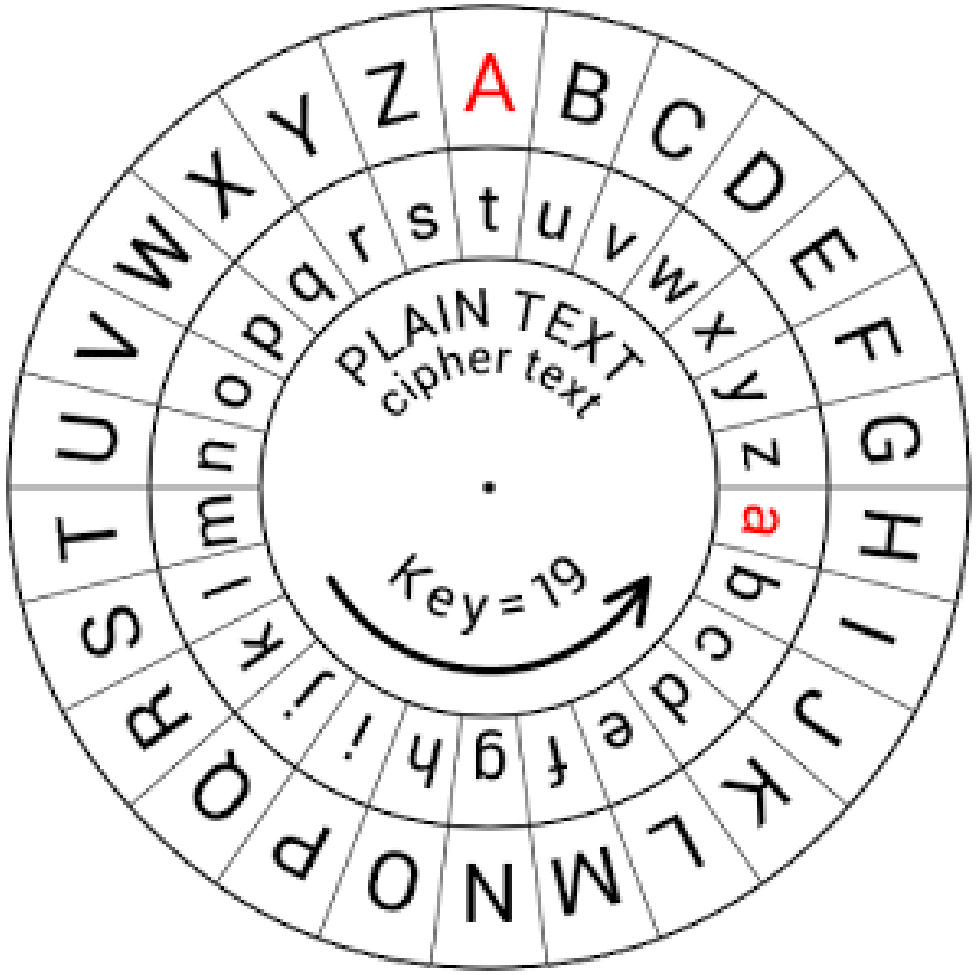
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMNOPQRSTUVWXY

GDKO

Bob

Eve




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
PLAIN TEXT
cipher text
Key = 19

	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	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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
27	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
28																										

There are only 26 possible keys… and one of them is very poor.

Why is that key so poor?

Brute Force Attack

Alice

HELP

Encryption

Key: shift of 1 letter

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMNOPQRSTUVWXY

GDKO

Bob

Eve

Key Distribution Problem

Alice

HELP

I need to pick a key.

Key: shift of 1 letter

Send the key out.

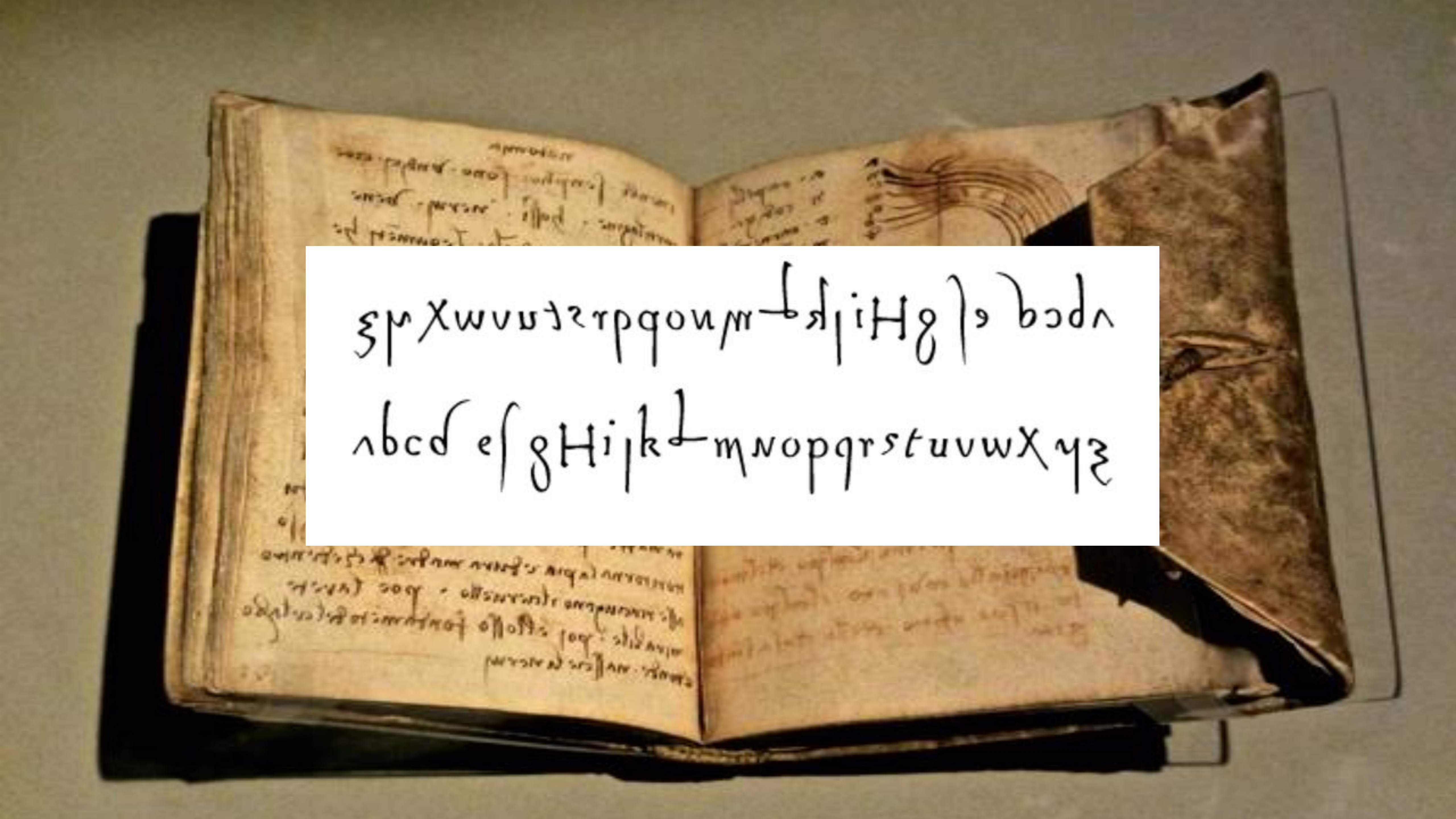
Bob

I know the key. I can decrypt the message.

Eve

Perfect. I will save the key for later.


Mirror Writing


abcd ef gHijkl mnopqrstuvwXyz

This is what
mirror writing
looks like!
Now you try it.


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

Alice

HELP

Plaintext

Algorithm: Position of Letter

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

Ciphertext

8 5 12 16

Bob

In a random alphabet cipher, you randomly scramble the alphabet. This makes a brute force attack harder for humans.

Key: the following alphabet

JKLAXUVWBCZFHIDQTENOPGMRSY

Then, to encrypt, you use the corresponding position of the letter you want in the next alphabet.

If you want B, you write K.

Key: second alphabet

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
JKLAXUVWBCZFHIDQTENOPGMRSY
```

Alice

HELP

Plaintext

Key: second alphabet

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
JKLAXUVWBCZFHIDQTENOPGMRSY
```

Ciphertext

WXFQ

Bob

How do you do decryption?

Decrypt this: WXFFD

Key: second alphabet

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
JKLAXUVWBCZFHIDQTENOPGMRSY
```