

Cryptography

History and Basics

Some simple examples

Breakable Encryption

Example 1

- `nuf si noitpyrcne`

Example 1

- nuf si noitpyrcne
- encryption is fun
- Algorithm: backwards

Example 2

ia_y ikel_ay ot_ay at_ea_y

pples_aa_y nda_ay ananas_ba_y

Example 2

iay ikelay otay atelay

I like to eta

pplesabay ndabay ananasbay

Apples and bananas

Pig Latin

Algorithm: move 1st letter to end,
add "ay" to end.

Example 3:

SUYOYUTSSOWLDBTE
TDFRORETYUILOETR

Example 3:

SUYOYUTSSOWLDBTE
TDFRORETYUILOETR

Hint: The first word is
"study".

Example 3:

SUYOYUTSSOWLDBTE
TDFRORETYUILOETR

Hint: The first word is
"study".

Example 3:

SUYOYUTSSOWLDBTE
TDFRORETYUILOETR

Example 3:

SUYOYUTSSOWLDBTE
TDFRORETYUILOETR

Study for your tests, you
will do better

Algorithm: Alternate lines.
Add in spaces as makes sense.

Example 4:

4-5-3-18-25-16-20-9-15-14

9-19 21-19-5-4 20-15

18-5-22-5-1-12 8-9-4-4-5-14

13-5-19-19-1-7-5-19

Example 4:

4-5-3-18-25-16-20-9-15-14

A = 1

D e c r y p t i o n

B = 2

9-19 21-19-5-4 20-15

C = 3

I s u s e d t o

D = 4

Etc.

18-5-22-5-1-12 8-9-4-4-5-14

R e v e a l h i d d e n

13-5-19-19-1-7-5-19

M e s s a g e s

Transposition Ciphers

Spartan Scytale





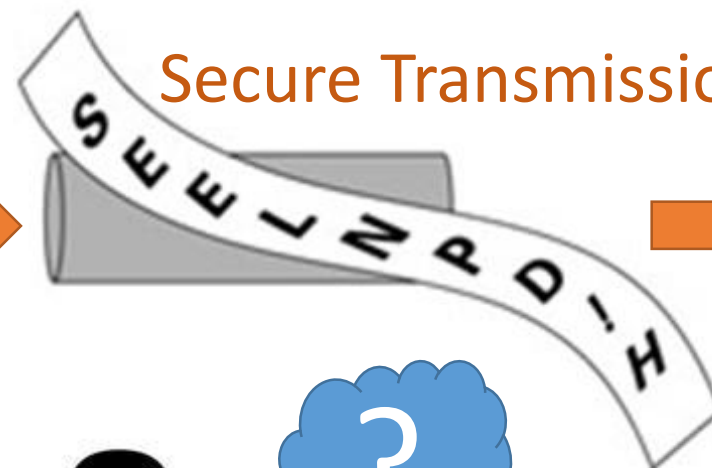
Alice

Send Help!

Encryption



Secure Transmission

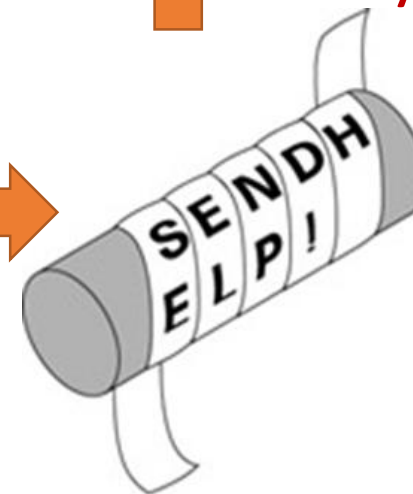


Send Help!



Bob

Decryption



Eve



A close-up photograph of a small, white piglet standing in a lush green field. The piglet is looking upwards and to the right, with its pink snout and dark eye clearly visible. The background is a soft-focus green landscape with some foliage and a hint of a building.

Pig

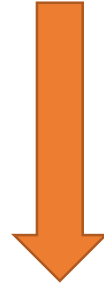
Latin



Alice

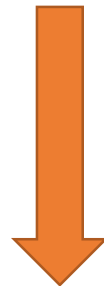


Plaintext



Algorithm: First letter to end AND add ay.

HELP ... ELP+H ... ELPH+AY



Ciphertext



Bob

Substitution Ciphers



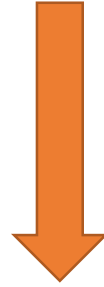
Caesar Shift



Alice

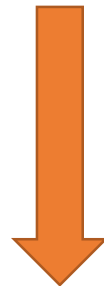


Plaintext



Key: shift of 1 letter

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMN O PQRSTUVWXYZ



Ciphertext



Bob



Alice

HELP



Encryption

Key: shift of 1 letter

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMNOPQRSTUVWXYZ

GDKO



Bob

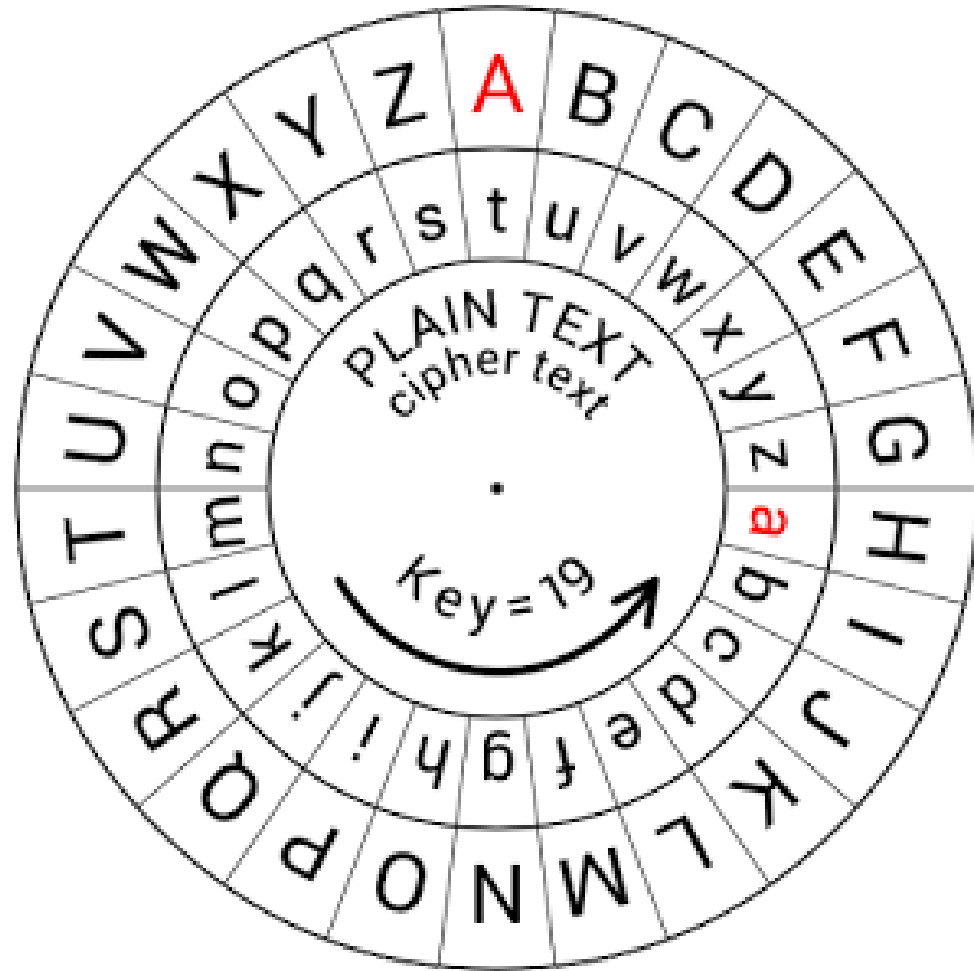
I know the key. I can decrypt the message.



Eve

I am so confused.

Yeah.
Not really.



	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?



Alice

HELP



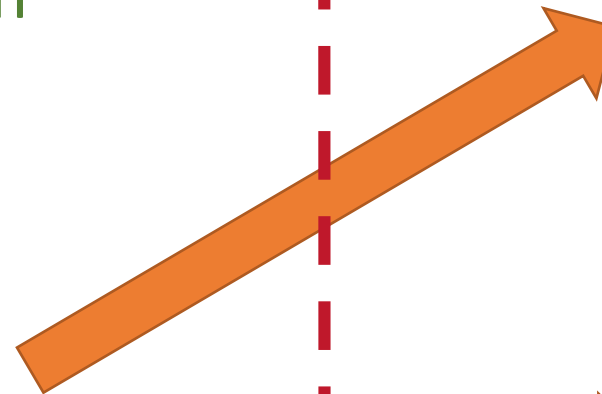
Encryption

Key: shift of 1 letter

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZABCDEFGHIJKLMNOPQRSTUVWXYZ

GDKO

Brute Force Attack



Bob

I know the key. I can decrypt the message.



Eve

I only need to try 25 keys. That's seconds. I can decrypt the message.

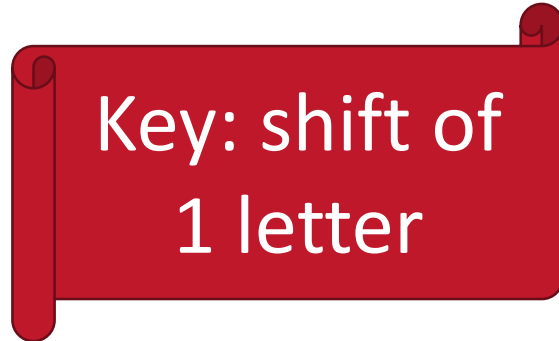
Key Distribution Problem



Alice



I need to
pick a key.

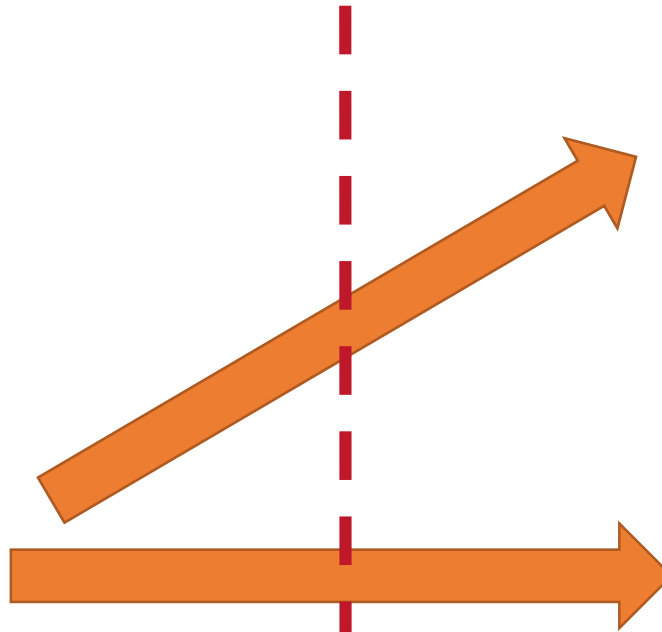


Send the key out.



Bob

I know the
key. I can
decrypt the
message.



Eve

Perfect. I
will save
the key for
later.

Mirror Writing



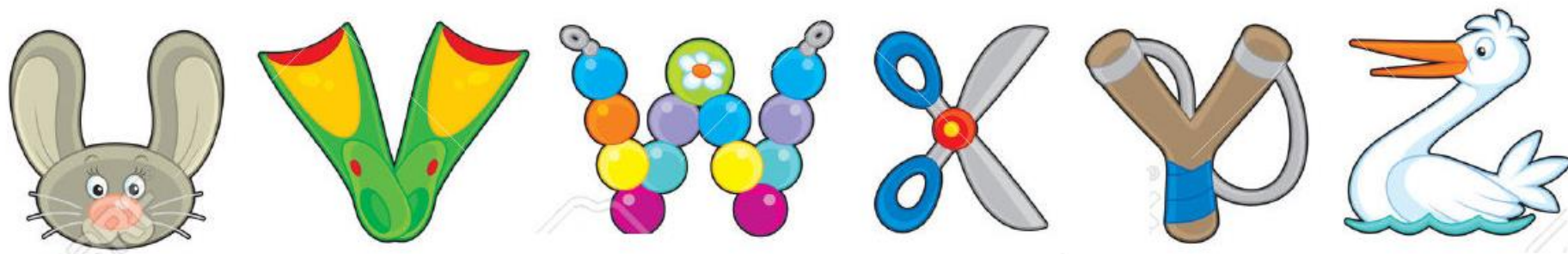
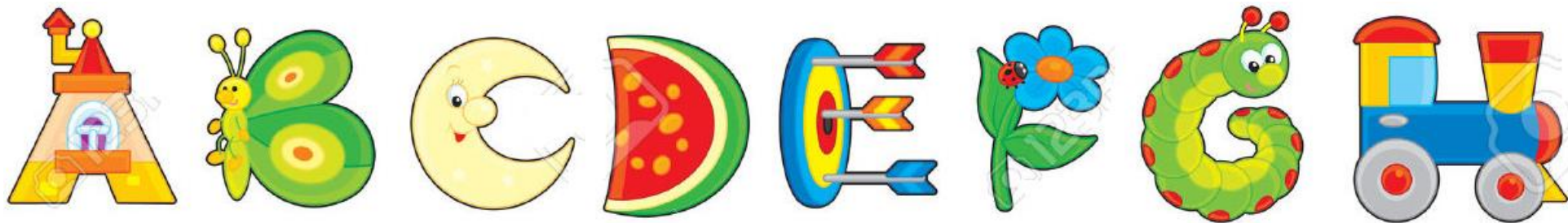
աբգ ը զհիկ լն ու փռ յտ
ստ յա ի ք լն ու փռ յտ

Now you try it.
Looks like
mirror writing
This is what

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



Seth Thompson.

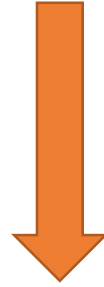




Alice

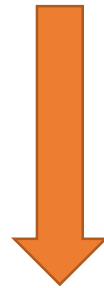


Plaintext



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



Bob



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

Key: the following alphabet

JKLAXUVWBCZFHIDQ TENOPGMRSY



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

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

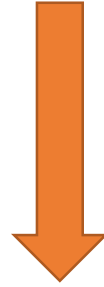




Alice

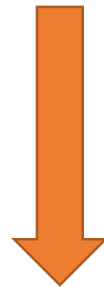
HELP

Plaintext



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



Ciphertext

WXFQ



Bob

How do you do decryption?

Decrypt this: **WXFFD**

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