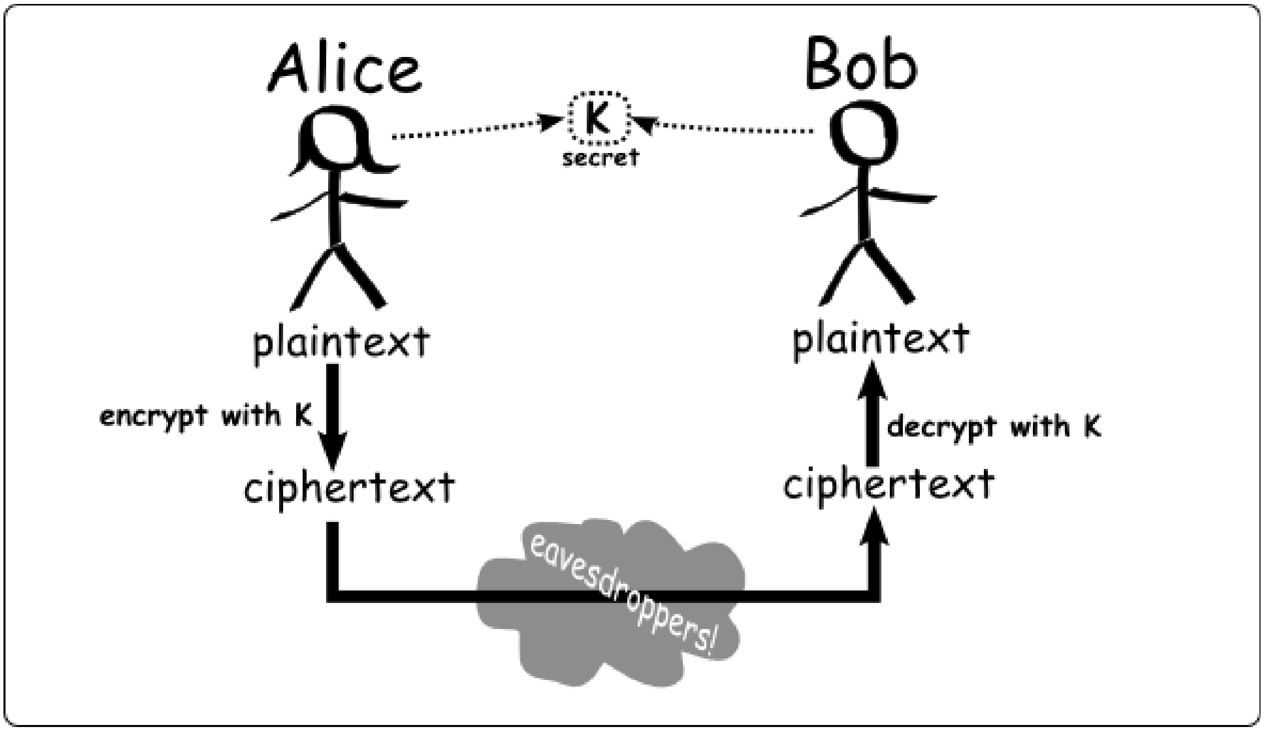
Symmetric Cryptography

general idea

- when the same key is used for both encryption and decryption
- the common key must be agreed upon before transferring messages
- security depends on the key

working mechanism

- if E and D are encryption and decryption functions respectively, then:
  - $E_k(P)=C$
  - $D_k(C)=P$
- k is some common key for both encryption and decryption



stream cipher vs. block cipher

- stream cipher: encrypts/decrypts one bit or byte at a time; takes stream of bits as input
- block cipher: encrypts/decrypts one block of data at a time; block size varies (some number of bytes)

substitution cipher

- each character is substituted by another character
- the alphabet can vary (i.e., it doesn't need to just be the 26 letters of the alphabet)
- four common types of substitution ciphers:
  - simple substitution cipher
    - mono-alphabetic: one character substitutes another character
    - Caesar cipher and keyword cipher are the common examples
  - homophonic substitution cipher
    - one character may map to more than one character
    - e.g.: A may map to R or & or $ or #
    - the repetition frequency of a character can be flattened a little by doing this
  - polygram cipher
    - blocks of characters are substituted to encrypt in groups, instead of each character

e.g.: “and” maps to “pan”, “in” maps to “xv”, and so on

polyalphabetic substitution cipher

each character may map to different characters (i.e., multiple substitutions)
Vigenère cipher is an example

Caesar Cipher

uses a number as a key – which gives a shift value for substitution

plaintext characters:

```
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
```

key: 4

ciphertext characters:

```
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
```

plaintext:

```
WORLD
```

ciphertext:

```
ASVPH
```

backwards:

ciphertext characters:

```
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
```

plaintext characters:

```
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:

```
ASVPH
```

plaintext:

```
WORLD
```

key: ?

```
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
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
```

key: 22

but we're decrypting, so 26 – 22 = 4 (the original key)
26 is the size of the alphabet

keyword cipher

numerous shift values, based on which word has been chosen as the key

plaintext characters:

```
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
```

key: HELP

ciphertext characters:

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

plaintext:

```
WORLD
```

ciphertext:

```
WNRJP
```

Vigenère cipher

based on a table that represents all possible shifts

plaintext

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

plaintext:	IF I DROPPED OUTTA SCHOOL WOULD I BECOME BILL GATES
key:	SURE
key:	SU R ESURESU RESUR ESURES URESU R ESURES URES URESU
ciphertext:	AZ Z HJIGTWX FYLNR WUBFSD QFYDX Z FWWFQW VZPD ARXWM

encryption:

choose a key and repeat it to make it as long as the input plaintext

take one character from the plaintext and look it up at the top of the table

take one corresponding character from the key and look it up at the left of the table

the character represented by the intersection of the two is the resulting ciphertext character

e.g.:

plaintext character: F and key character: M -> ciphertext character R

decryption:

simply reverse what was done during encryption

take one character from the key and look it up at the left of the table

scroll to the right in that row until you reach the corresponding character of the ciphertext

scroll up from that position until you reach the resulting plaintext character all ciphers discussed here (and the OTP and XOR ciphers discussed previously) are examples of symmetric cryptography