

1. Polyalphabetic Cipher

Each letter in the plaintext is encoded using a different alphabet (usually with some sort of repetition)

2. **Progressive Caesar Cipher / Sequential Shift:** Start with a Caesar cipher, and then shift one letter with each character you are encrypting.

	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
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

(a) Example: Begin with the shift cipher $A \rightarrow Q$, and encrypt the word HELLO

H E L L O
X V D E I

(b) Example: Suppose the ciphertext was encrypted with the above scheme. Decrypt the word FRJMS.

PARTY

3. **Vigenère Cipher** Choose a keyword, and use that keyword to determine a shift cipher for each letter. (Repeat the keyword over and over.)

	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
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
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
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

(a) Example: use the keyword DOG and encrypt the phrase WHERESMYFOOD.

WHERESMYFOOD
DOGDOGDOGDOG
ZVKUSYPMLRCJ

(b) Example: Suppose the keyword is DOG. Decrypt the ciphertext LZONSYQCC.

LZONSYQCC
DOGDOGDOG
ILIKESNOW