Cryptography. (Elementary Number Theory and its Applications (Rosen) Chp. 8).

Idea: Send encrypted messages across an unsecure channel to a recipient so that if the message does get intercepted by an eavesdropper, they will not be able to decode it, but the intended recipient should be able to decode the message.

We begin with character cipher (also known as monographic ciphers). In these ciphers, each letter is replaced by another letter by substitution.

Our first example is a Caesar cipher named after Julius Caesar. He used a substitution of a shift by 3 to send messages.

Throughout, let P be the numerical equivalent of a letter in plaintext (message) and let C be the numerical equivalent corresponding to ciphertext (encrypted message). Then the original Caesar cipher used is described by

$$C \equiv P+3 \mod 26 \qquad 0 \leq C \leq 25$$

Ex:

	A	P	P	L	E
P:	00	15	15	11	04
C:	03	18	18	14	07
	D	S	S	O	H

Example: Encrypt the message

TO BE OR NOT TO BE

using the original Caesar cipher $C \equiv P + 3 \pmod{26}$. For reference, you may use

	A	B	C	D	E	F	G	H	I	J	K	L	M
P	00	01	02	03	04	05	06	07	08	09	10	11	12
C	03	04	05	06	07	08	09	10	11	12	13	14	15
	D	E	F	G	H	I	J	K	L	M	N	O	P
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	13	14	15	16	17	18	19	20	21	22	23	24	25
C	16	17	18	19	20	21	22	23	24	25	00	01	02
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

TOBE O RNOTT OBE

WREHR UQRWW REH.

Now decipher the message

WKLVL VKRZZ HGHFL SKHU

using the same encryption scheme above

THISI SHOWW EDECI PHER

Pros of Caesar Cipher

- Easy to encrypt and decrypt.
- Not convoluted.
- Provides <u>some</u> primitive security.
- key size is small (easy to transmit).

Cons of Caesar Cipher

- Too primitive: suffers from frequency analysis attacks (not very secure).
- Not enough shifting possibilities (only 26 keys)
- Key size is small (easily hacked/guessed)
- How do we transmit the key?

How can we generalize this?

(1) Make the encryption more complicated by using an Affine Transformation.

$$C \equiv aP + b \mod 26 \quad \text{for } a, b \in \mathbb{Z}/26\mathbb{Z}.$$

(2) Make a different encryption for each letter (and we can make this dependent position)

$$c_i = a_i P_i + b_i \quad \text{where } i \text{ is a position index.}$$

These are called Vigenère ciphers

For the Affine Transformation cipher to work, I need to be able to isolate for P in

$$\begin{aligned} C &\equiv aP + b \mod 26. \\ C - b &= aP \mod 26. \\ a^{-1}(C-b) &= P \mod 26. \end{aligned}$$

<u>So</u> a needs to be invertible. This occurs when $\gcd(a, 26) = 1$. This leaves $\phi(26) = \phi(2)\phi(13) = 12$ possibilities.

In total we have 12 possibilities for a and 26 for b. So $12 \cdot 26 = 312$ possibilities.

Example: Encrypt the message

PLEASE SEND MONEY

using the Affine Transformation cipher $C \equiv 7P + 10 \pmod{26}$. For reference, you may use

	A	B	C	D	E	F	G	H	I	J	K	L	M
P	00	01	02	03	04	05	06	07	08	09	10	11	12
C	10	17	24	05	12	19	00	07	14	21	02	09	16
	K	R	Y	F	M	T	A	H	O	V	C	J	Q
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	13	14	15	16	17	18	19	20	21	22	23	24	25
C	23	04	11	18	25	6	13	20	01	08	15	22	03
	X	E	L	S	Z	G	N	U	B	I	P	W	D

P = 4.

$C \equiv 7(4) + 10 \equiv 28 + 10 \equiv 2 + 10 \equiv 12 \pmod{26}$.

PLEASE ESEND MONEY

LJMKG MGMXF QEXMW.

Now decipher the message

FEXEN ZMBMK JNHMG MYZMN

using the same encryption scheme above

DONOT REVEA LTHES ECRET

To invert a, can either use Euclidean Algorithm and back substitution OR use Euler's Theorem

$a^{\varphi(26)} \equiv 1 \pmod{26}$

$a^{12} \equiv 1 \pmod{26}$.

$a(a^{11}) \equiv 1 \pmod{26}$ So $a^{-1} \equiv a^{11} \pmod{26}$.

$a a^{-1} \equiv 1 \pmod{26}$