CRYPTOGRAPHY HANDOUT 01

SHIFT AND AFFINE CIPHERS

1. Shift (Caesar) Cipher

Assign each letter a number:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example. (Caesar's cipher) Shift each letter by three places.

a	b	c	d	e	f	g	h	i	j	k	l	m
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
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- We can think of encryption as $x \mapsto x + \kappa (\mathrm{mod} 26)$ where $\kappa = 3$.
  Plaintext: "caesar"
  `CIPHERTEXT`:

- Decryption is $x \mapsto x - \kappa (\mathrm{mod} 26)$ where $\kappa = 3$.

Example. Encrypt "conquer" using $\kappa = 6$.

Example. Decrypt "`GPISTEXVE`" using $\kappa = 4$.

2. Affine Ciphers

Example. Use $x \mapsto 9x + 2 (\text{mod} 26)$.

- We can think of encryption as $x \mapsto \alpha x + \beta (\text{mod} 26)$ where $\alpha = 9$ and $\beta = 2$.
  Plaintext: "caesar"
  `CIPHERTEXT`:

- Decryption uses the inverse function:

$$\begin{aligned} 9x + 2 &= y \\ 9x &= y - 2 \\ x &= \frac{1}{9}(y - 2) \\ x &= 9^{-1}(y - 2) \\ x &= 3(y - 2) \\ x &= 3y - 6 \\ x &= 3y + 20 \end{aligned}$$

- Check the decryption:

Example. Encrypt "rome" using $x \mapsto 3x + 1$ and then find the inverse function.