MAT2440, Classwork43, Spring2025

ID:_____ Name:_____

1. Affine Cipher.

The shift ciphers can be generalized further to slightly enhance security by using a function of the form

$$f(p) = \underline{ap+b} \pmod{26},$$

where a and b are integers and $\underline{\gcd(a,26)=1}$ to ensure the existence of the decryption function. Such a cipher is called $\underline{\text{affine}}$ cipher.

2. Encrypt the plaintext "PARK" when function $f(p) = 7p + 3 \pmod{26}$ is used.

P	A	R	K
15	0	17	10
↓	↓	↓	↓
4	3	18	21
E	D	S	V

$f(15) = 7\cdot 15+3 \pmod{26} = 108 \pmod{26} = 4$

$f(0) = 7\cdot 0+3 \pmod{26} = 3 \pmod{26} = 3$

$f(17) = 7\cdot 17+3 \pmod{26} = 122 \pmod{26} = 18$

$f(10) = 7\cdot 10+3 \pmod{26} = 73 \pmod{26} = 21$

3. How to decrypt the message encrypted by using affine cipher $f(p) = ap + b \pmod{26}$?

✡ $\gcd(a,26)=1$. Let p be that message, c be the cipher letter

$f(p) \equiv a\cdot p+b \mod 26 = c$

encryption knowing p → finding c

decryption knowing c → finding p

That is, solving p in the equation

$$(ap+b) \bmod 26 = c \bmod 26$$

$$ap \bmod 26 = c-b \bmod 26 \quad (-b)$$

we can find inverse of a modulo 26 : $\bar{a}$ $(a\bar{a}\equiv 1 \bmod 26)$

($\gcd(a,26)=1$ guarantee the existance of $\bar{a}$)

$$\bar{a}ap \bmod 26 = \bar{a}(c-b) \bmod 26$$

$$p \bmod 26 = \bar{a}(c-b) \bmod 26$$

⇒ decryption function is $\boxed{g(c) = \bar{a}(c-b) \bmod 26}$

4. (a) Find the decryption function for $f(p) = 7p + 3 \pmod{26}$. (b) Decrypt the ciphertext message "EDSV" which is encrypted by using $f(p) = 7p + 3 \pmod{26}$.

(a) To find the inverse of 7 modulo 26.

$\gcd(7,26) = \gcd(7, 26 \bmod 7) = \gcd(7,5) = \gcd(7 \bmod 5, 5) = \gcd(2,5) = \gcd(2, 5 \bmod 2) = \gcd(2,1) = 1$

$26 = 7\times 3 + 5$ — (1)

$7 = 5\times 1 + 2$ — (2)

$5 = 2\times 2 + 1$ — (3)

(2): $2 = 7 - 5\times 1$

(3)

$1 = 5 - 2\times 2 = 5 - 2(7 - 5\times 1) = 5 - 2\times 7 + 5\times 2$

$= 5\times 3 - 2\times 7 = (26 - 7\times 3)\times 3 - 2\times 7 = 26\times 3 - 11\times 7$

(1): $5 = 26 - 7\times 3$

$\Rightarrow 1 = -11\times 7 + 26\times 3$

$\Rightarrow$ decryption function:

$g(C) \equiv -11(C-3) \pmod{26} = 15(C-3) \bmod 26$

b)

E	D	S	V
4	3	18	21
↓	↓	↓	↓
15	0	17	10
P	A	R	K

$g(4) \equiv -11(4-3) \bmod 26 = -11 \bmod 26 = 15$

$g(3) \equiv -11(3-3) \bmod 26 = 0 \bmod 26 = 0$

$g(18) \equiv -11(18-3) \bmod 26 = -165 \bmod 26 = 17$

$g(21) \equiv -11(21-3) \bmod 26 = -198 \bmod 26 = 10$

5. Public Key Cryptography.

Private key cryptosystems: shift cipher, affine cipher, etc.

Anyone who knows the key can both encrypt and decrypt message which make this cryptosystem simple but extremely vulnerable to cryptanalysis.

Public key cryptosystems: the RSA (Rivest, Shamir, Adleman) system, etc.

One who knowns how to encrypt the message does not help decrypt message. Everyone can have a publicly known encryption key but the decryption keys are kept secret.

6. RSA Encryption.

Let m be the message represented in the format of strings and (n, e) be the public key such that $n = pq$ is a product of two primes numbers and $\gcd(e, (p-1)(q-1)) = 1$. Then we have the encryption function

$$f(m) = m^e \pmod{n}.$$