MAT2440, Classwork42, Spring2025

ID:_____ Name:_____

1. Caesar's Cipher

Encryption: shift each English letter 3 letters forward.

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	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

Example of encryption:

CITY→F L W B

Decryption: shift each English letter 3 letters back ward.

Example of decryption:

SDUN→P A P K

2. If we assign a number from 0 to 25 to each letter:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Then, mathematically, the encryption in 1. can be expressed as a function

$$f(p) = \underline{\quad p+3 \quad} \pmod{26},$$

and decryption can be represented as a function

$$g(p) = \underline{\quad p-3 \quad} \pmod{26}.$$

For example, to encrypt the given letters by $f(p)$:

"C"= 2, we have $f(2) = 2 + 3 \pmod{26} = 5 \pmod{26} = 5$ which means the encryption of "C" is "F".

"X" = 23, we have $f(23) = 23+3 \pmod{26} = 26 \pmod{26} = 0$ which means the encryption of "X" is "A"

For example, to decrypt the given letters by $g(p)$:

"S"= 18, we have $g(18) = 18 - 3 \pmod{26} = 15 \pmod{26} = 15$ which means the de encryption of "S" is "P".

"D" = 3, we have $g(3) = 3-3 \pmod{26} = 0 \pmod{26} = 0$ which means the decryption of "D" is "A".

3. Shift Cipher and the Key.

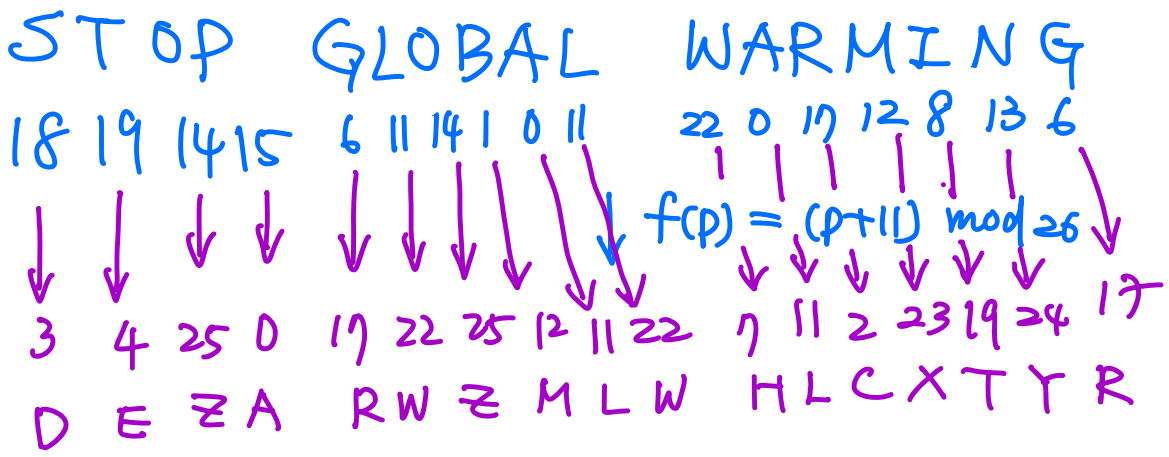
The Caesar's cipher is a special case of the shift cipher. In a shift cipher, the shift can be any integer k. Then we have the shift cipher

encryption: $f(p) =$ p+k $\pmod{26}$,

decryption: $g(p) = f^{-1}(p) =$ p−k $\pmod{26}$,

Here the integer k is called a key.

4. Encrypt the plaintext message "STOP GLOBAL WARMING" using the shift cipher with key $k = 11$. $f(p) = p + 11 \pmod{26}$



5. Decrypt the ciphertext message "NYLHA LEWLYPLUJL" that was encrypted via the shift cipher with key $k = 7$. $g(p) = p - 7 \pmod{26}$