

CIS 3362 8/18/25

- 1) Decoding Activity
- 2) Class webpage
- 3) Shift Cipher

Shift cipher

A=0, B=1, C=2, ... Z=25

msg: H E L L O  
7, 4, 11, 11, 14

|             |    |                                    |                    |
|-------------|----|------------------------------------|--------------------|
| key(secret) | IS | <u>HISTHISTHISTHIS</u>             |                    |
|             |    | 22, 19, <u>26</u> , <u>26</u> , 29 | take result mod 26 |
| CIPHER      |    | 22 19 0 0 3                        |                    |
| TEXT        |    |                                    |                    |

→ W T A A D

encryption  $f_k(x) = (x+k) \bmod 26$

decrypt  $f_k^{-1}(x) = (x-k+26) \bmod 26$  and back

NOT SECURE: SMALL KEYS SPACE

BRUTE FORCE: Try all keys!

Python: ord, chr

C, C++, Java, - 'a', + 'a', - 'A', + 'A'  
as needed.

Convert from char to int (0-25)