Challenge: Coding Cesar

Write C++ program to encrypt & decrypt strings using Cesar cipher.

- Use good programming practices
- Create proper modules
- Your solution MUST work correctly for any key value
- Assume all message contains only lower-case alphabet characters (a..z)
- Message is one string

Test Message: “hello there everyone how are you doing”

Test Key: 10 (only for testing)

Encrypted Message: “rovvy drobo ofobiyxo ryg kbo iye nysxq”

Want to Impress?

- Encryption calculation in 1 line of code
- Decryption calculation in 2 lines of code, no if statements (or better?)

Programming Cesar, The Simple Way

- Mathematically give each letter a number 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

- But, ‘a’ is actually 97 (ASCII of ‘a’)
  - subtract ASCII to get the proper sequence

- When encoding, the shifted value may be > 25 (ex: 21+7=28)
  - 28 mod 26 = 2 □ c

- When decoding, the decoded value maybe negative (ex: 2-7 = -5)
  - This means you need to wrap around from the left
  - When negative, add 26 : (-5 + 26 = 21) □ v

- But 21 is not ‘v’ ??
  - of course not… you need to put it back in the proper ASCII range
  - add ‘a’ (or 97)

Homework

Modify previous program to be able to:

1. Account for the space character when decrypting
   1. (i.e. the decrypted message should look exactly like the original message)
2. Encrypt (and later decrypt) messages containing any characters and numbers. [a..z][A..Z][0..9]
   1. Decrypted message need not to preserve the case of original message
   2. Numbers need not to be encrypted/decrypted (bonus points if you do)
3. Ask the user to input the desired key and operation
   1. (1. encrypt, 2. decrypt)

4. Encrypt: Use file “message.txt” to read messages to be encrypted, output encrypted lines to screen & file “encrypted.txt”
5. Decrypt: read from file “encrypted.txt” and output to screen and file “decrypted.txt”