Implementing the Caesar Cipher

Introduction

Duke
UNIVERSITY

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

FIRST LEGION ATTACK EAST FLANK

ABCDEFGHIJKLMNOPQRSTUVWXYZ

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


      F
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK

 ABCDEFGHIJKLMNOPQRSTUVWXYZ
C
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

FIRST LEGION ATTACK EAST FLANK

ABCDEFGHIJKLMNOPQRSTUVWXYZ

C

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


              I
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
C
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CF
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

FIRST LEGION ATTACK EAST FLANK

ABCDEFGHIJKLMNOPQRSTUVWXYZ

CF

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


                          R
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CF
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFO
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFOPQ IBDFLK
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK

 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFOPQ IBDFLK
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


  A
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFOPQ IBDFLK
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK

                                A
 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFOPQ IBDFLK
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK


 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFOPQ IBDFLK X
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)

Caesar Cipher Overview

```
FIRST LEGION ATTACK EAST FLANK

 ABCDEFGHIJKLMNOPQRSTUVWXYZ
CFOPQ IBDFLK XQQXZH BXPQ CIXKH
```

- Named for Julius Caesar
- Encryption: substitute letter with (letter+N)
  - Caesar: N = 23 (i.e. 3 letters prior)
- Decryption: encrypt with 26 - N

Two Ways to Think About It

```
FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH
```

- One way: math on letters
  - Everything is a number
  - ‘F’ - 3 = ‘C’
  - ‘A’ - 3?
    - Need to wrap around…

Two Ways to Think About It

```
FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW
```

- Another way: pre-shift alphabet
  - Compute shifts of each letter at start
  - Lookup each letter

Two Ways to Think About It

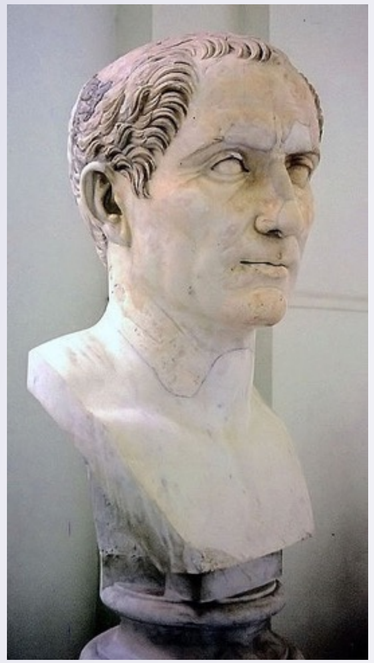
```
FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW
```

- Another way: pre-shift alphabet
  - Compute shifts of each letter at start
  - Lookup each letter

Two Ways to Think About It



FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW

- Another way: pre-shift alphabet
  - Compute shifts of each letter at start
  - Lookup each letter

Two Ways to Think About It

```
FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW
```

- Another way: pre-shift alphabet
  - Compute shifts of each letter at start
  - Lookup each letter

Two Ways to Think About It

```
FIRST LEGION ATTACK EAST FLANK

CFOPQ IBDFLK XQQXZH BXPQ CIXKH

ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW
```

- Another way: pre-shift alphabet
  - Compute shifts of each letter at start
  - Lookup each letter

A Few New Concepts

- A few new concepts before you implement
  - New String manipulations
  - for loops which count from over a range
    - Use number to index into data