# Week 3 Thursday

## Historical Figure

Turn to someone sitting near you. Introduce yourselves to each other, and then discuss briefly:

If you could meet any historical figure, who would you choose and why?

# Playfair Cipher, Vignère Cipher, One-Time Pad

1. You are constructing a $5 \times 5$ grid for a Playfair cipher starting with the key word `FAJITAS`. What letter falls in the *very center* of the grid (ie, in the 3rd row and the 3rd column)?

(A) K

(B) L

(C) M

(D) None of the above

2. Encode the message "`Little Fluffy`" for encryption using a Playfair cipher. How many *pairs* of letters are in the encoded message?

(A) 6

(B) 7

(C) 8

(D) None of the above

3. Use a Playfair cipher with the $5 \times 5$ grid constructed using the key word `FAJITAS` to encrypt "`Little Fluffy`."

4. Use a Vignère cipher with keyword `AND` to encrypt the message "`Six Meals`."

Feel free to split up the work with your neighbors!

5. Use a Vignère cipher with keyword `AND` to decrypt:

`YBX SUD LYQ OGS AFV.`

Feel free to split up the work with your neighbors!

6. Suppose you want to encrypt a sequence of bits (ie, a sequence of 0s and 1s) using a $2 \times 2$ Hill cipher. How many different encryption functions are there? In other words, how many different congruence classes of $2 \times 2$ matrices can be used as a key for a Hill cipher?

(A) 2

(B) 6

(C) 16

(D) None of the above

7. Using the Polybius square on the right, decrypt the following message.

```
FF GV AX VG VX AV AX
GA AV DG VG AX FG AX
VG XG GA AV DG XG XG
FF FD AX FF DV GV GD
GA FD GA FV GA XV
```

Feel free to split up the work amongst with your neighbors!

| | **A** | **D** | **F** | **G** | **V** | **X** |
|---|---|---|---|---|---|---|
| **A** | 2 | 1 | J | U | N | E |
| **D** | 1 | 7 | 8 | D | C | M |
| **F** | B | R | T | V | W | X |
| **G** | A | F | 3 | G | H | 4 |
| **V** | I | 5 | K | L | 6 | O |
| **X** | P | Q | 9 | S | Y | Z |

8. Here is a key for a simple substitution cipher, where the first row is plaintext and the second row is ciphertext.

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| G | A | U | M | L | X | B | P | V | J | W | Q | E | Y | D | C | H | T | S | K | Z | F | N | O | R | I |

Decrypt the following message which was encrypted using this simple substitution.

```
VEGA QGUW DULG YQLG CVYB GYMN VMLN LQQV YBGY MSNL
QQVY BVAL GTVY KPLK VML
```

Feel free to split up the work amongst with your neighbors!