Week 3 Tuesday

Turn to someone sitting near you and introduce yourself!
Then take 5 minutes to discuss:

The following message was encrypted using a Caesar cipher whose shift is congruent to the *inverse* of 17 mod 26. What is the plaintext? Do you know where it's from?

`XIIJ FJPV TBOB QEBY LOLD LSBP`

Ignore the spaces; they're just there for your convenience and do not align with the spaces that should appear in the original message.

Affine Cipher, Simple Substitution, Polybius Square, Hill Cipher

1. Using the Polybius square on the right, what is the encryption of the phrase `Starry Dynamo`?

(A) `XG FF GA FD FD XV DG XV AV GA DX VX`

(B) `GX FF AG DF DF VX GD VX VA AG XD XV`

(C) None of the above

	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

2. Alice and Bob have agreed to use an affine cipher with $a = 3$ and $b = 10$. What is the decryption function?

(A) $D(y) = 9y - 10$

(B) $D(y) = 9(y - 10)$

(C) $D(y) = 3y + 10$

(D) None of the above

3. Alice encrypted the following ciphertext using an affine cipher with $a = 3$ and $b = 10$ (same as last problem!). What is the corresponding plaintext?

```
IXZI XIPE QKUW TAYX KXTM WPPR WTAV WJUW
```

The spaces are only inserted for convenience and do not necessarily correspond to the spaces in the original message. Feel free to split up the work amongst with your neighbors!

4. As of 2010, the Real Academia Española regards the Spanish alphabet as having 27 distinct letters (namely, the 26 that exist in English, plus Ñ). How many distinct affine encryption functions can be chosen for Spanish?

(A) 27^2

(B) $27 \cdot 18$

(C) $27 \cdot 13$

(D) None of the above

5. Which of the following matrices is invertible mod 26?

(A) $\begin{bmatrix} 7 & 5 \\ 3 & 3 \end{bmatrix}$

(B) $\begin{bmatrix} 8 & 1 \\ 3 & 2 \end{bmatrix}$

(C) $\begin{bmatrix} 4 & 2 \\ 1 & 2 \end{bmatrix}$

(D) $\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$

Follow-up. Find an inverse of the invertible one!

6. Use a Hill cipher with key

$$A = \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$

to encrypt the word AREA.

7. The matrix

$$A = \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$

was used to encrypt `CRZX`. What is the plaintext?