Week 2 Friday

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

The following message was encrypted using a rectangular transposition cipher with keyword `FRIDAY` followed by a Caesar cipher with shift congruent to the inverse of 17 mod 26. What is the plaintext?

```
FJXI IJOB PTVB LYQB EOBS LLDP
```

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

More Simple Substitition Ciphers

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 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. 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 XV 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

6. 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!