CIS 3362 Homework #3 Part A: Playfair, ADFGVX, Hill, Enigma
Due: Check WebCourses for the due date.

1) (10 pts) By hand, encrypt the plaintext "HELLOBYRONLOVELYDAY" with the keyword "BUILDINGBLOCK" and the padding character "Q".

2) (10 pts) Show the result of encrypting the plaintext

"THEQUICKBROWNFOXJUMPEDOVERTHE345679INSECTSIN2018"

Using the ADFGVX cipher with the 6 x 6 square shown below and the keyword "SPONGE".

	A	**D**	**F**	**G**	**V**	**X**
A	E	U	R	I	P	8
D	Letter O	H	W	D	K	G
F	2	N	5	Digit 0	6	V
G	Z	T	A	X	M	F
V	7	Y	Q	9	J	4
X	B	L	3	C	Digit 1	S

3) (10 pts) For the Hill cipher, the encryption key is $\begin{pmatrix} 19 & 16 \\ 14 & 3 \end{pmatrix}$, what is the corresponding decryption key? (Assume an alphabet size of 26.)

4) (10 pts) You've intercepted a message encrypted by the Hill cipher using a 2 x 2 key (alphabet size 26). You also know that the plaintext "TR" maps to the ciphertext "UR" and that the plaintext "AP" maps to the ciphertext "BX". What are the possible encryption keys?

5) (10 pts) The Enigma never allowed a character to encrypt to itself. If we consider an arbitrary substitution cipher for an alphabet of 5 letters, we know there are 5! = 120 possible keys. Of these 120 possible keys, how many of them map each plaintext letter to a different ciphertext letter?

6) (5 pts EC) Write a program **in Python** (due to simple big integer support), which reads in the number n, representing the number of characters in an alphabet, and then answers question #5 for the an alphabet size of n (instead of just solving the problem for n = 5). (If your program runs fast and solves the problem for up to 10, you'll get 2 pts, and if it runs fast enough up to 26, you'll get full credit!)