SCI 2000
Introduction to Encryption, Assignment 1
Due January 23rd at the start of class.

Questions will be marked both on correctness and clarity of presentation. Poor writing and sloppy/illegible presentation both impact the clarity of your work and so will be penalized. You must show all steps in your computations to get credit, though you are welcome to use computational aids for this assignment, contrary to what I wrote in the syllabus. However, you will not have this luxury on tests, so please be capable of doing everything "by hand".

The following table will be useful:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Question 1: Encrypt the phrase "CRYPTO" using:

(a) A Caesar cipher with a shift of $n = 16$.

(b) An affine cipher with a key of $(11, 4)$.

(c) A Vignère cipher with a key of "cat".

(d) A block permutation cipher using the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

Question 2: The message IWUTP NIWGZ has been encrypted using a Hill cipher with the key

$$A = \begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}.$$

Find $A^{-1} \mod 26$ and decrypt the message.

Question 3: Wikipedia lists the Rotokas language as having the shortest alphabet in the world, with 12 letters. How many fewer states would an enigma machine built to accommodate a 12-letter alphabet have than the standard enigma machine, built to use a 26-letter alphabet? (I.e., assume the plugboard has 12 letters, the three rotors have 12 inputs and outputs, and the reflector plate has 12 inputs. Compute the new number of states, explaining the steps and your reasoning, and say how much smaller it is than number of states for a "usual" enigma machine).

Question 4: Repeat the previous question with an alphabet having 13 letters. Omit details when steps are the same, but highlight the main differences (Hint: Carefully analyze the plugboard and reflector plate).