Advanced Cryptography

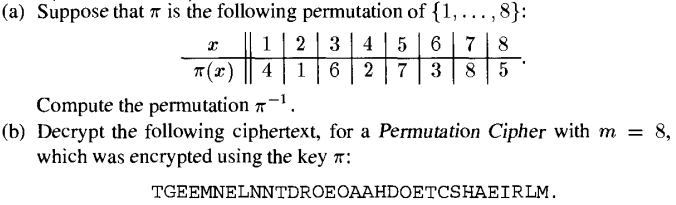
**Assignment #1**

Due date:2077/07/20

1. Evaluate the following
2. 7503 mod 81
3. -7503 mod 81
4. 81 mod 7503
5. -81 mod 7503
6. Use exhaustive key search to decrypt the following cipher text, which was encrypted using shift cipher:



1. Determine the number of key in affine cipher over Zm for m=30, and 1225.



1. Here is how we might cryptanalyze the Hill Cipher using a cipher text only attack. Suppose that we know that m=2. Break the cipher text into blocks of length two letters (digrams). Each such digrams are the encryption of a plain text digrams and assume it in the encryption of a common digrams for example, TH or ST. Each such guess, proceed as in the known plaintext attack, until the correct encryption matrix is found.

Here is a sample of cipher text to decrypt using this method:



*Note: Student has to submit their assignment individually. Hand written and Softcopy both are accepted. But for the Softcopy, if two assignments are found identical, both are marked Zero. Submission after due date is not accepted.*