Advanced Cryptography

Assignment #1

Due date:2081/1/27

1. Evaluate the following
   a. 7503 mod 81
   b. -7503 mod 81
   c. 81 mod 7503
   d. -81 mod 7503
2. Use exhaustive key search to decrypt the following cipher text, which was encrypted using shift cipher:

   BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD.

3. Determine the number of key in affine cipher over Z_m for m=30, 100 and 1225.

4. 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 (diagrams). Each such diagrams are the encryption of a plain text diagrams and assume it in the encryption of a common diagrams for example, TH or ST. Each such guess, proceed as I the known plaintext attack, until the correct encryption matrix is found.

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

   LMQETXYEAGTXCTUIEWNCTXLZEWUAISPZYVAPEWLMGQWYA
   XFTCJMSQCADAGTXLMDXNXSNPJQSYVAPRIQSMHNOCVAXFV

5. Suppose we are told that the plaintext "breathtaking" yields the Ciphertext RUPOTENTOIFV where the Hill Cipher is used (but m is not specified). Determine the encryption matrix.
6. Decrypt the following Ciphertext, obtained from the Autokey Cipher, by using exhaustive key search:

   MALVVMAFBHBUQPTSOXALTGVWWRG

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.