**Cryptography Principles Exam-1**

**Siem Hadish**

1. Provide an analysis detailing its strengths/weaknesses.

The affine cipher is an old encryption technique, which is an improvement to the substitution or the Ceasar cipher. The encryption algorithm as demonstrated in this exercise is not secure enough and it has more weaknesses than strengths. The strength it has over the Caesar cipher, the encryption technique that existed before this algorithm, is that it has a bigger keyspace than the Caesar cipher, which in the standard English letters has 26, however in the affine cipher, has 12 times 26, which is 312 keys, therefore takes longer to break.

The weakness of this encryption technique is that it still is easy to crack once the method is figured out, for the text given in the exercise, it did not take much to try out all 312 keys and crack it, making the algorithm weak and unusable for serious encryption tasks.

1. attempt to uncover the plaintext associated with the ciphertext;

Using the code submitted with the exercise, we can uncover the original plain text, which is:

THISONEISNOMOREDIFFICULTTHANTHEPREVIOUSONESTATISTICALANALYSISWORKSFORTHISENCRYPTIONSYSTEMTOOBUTCANYOUUSEYOURKNOWLEDGEOFLINEARALGEBRATOFINDTHESECRETKEYTOOTHENYOUWILLHAVETRULYCRACKEDTHESYSTEM.

1. attempt to determine the secret key (a, b) used.

Using brute force and a little bit of frequency analysis, we could uncover the keys a and b to be 7 and 18.