Ciphers and Number Theory 1

1. Encode the message `the pirates are coming` using a Caesar cipher with shift 7.

2. Decode the message `ALSAM PPKYE VHXLI IRXVE RGI` using a Caesar cipher with shift 4.

3. If a message is not written in a uniform manner (eg as blocks of 5 letters at a time) then it can be significantly easier to crack. Crack each of the following messages, which have been encoded using two different Caesar ciphers.

   (a) `IWXH XH P HXBEAT BTHHPVT ID RGPRZ`.

   (b) `FJBCQ RBCNG CJURC CUNQJ AMNA`.

4. Eve intercepts the following message `HCCKH CFWKG CBTHR TMWY`. She know that it is encoded with a monoalphabetic cipher, and either says `meet me at the airfield` or `meet me in the compound`. Where is the meeting to take place?

5. Encode the message `your cover has been blown` using a keyword cipher with keyword GALOIS.

6. Decode the message `SCAQU EJFPD KACFQ QUPTF RAMDK SCACF PELUP` encoded using a keyword cipher with keyword FERMAT.

7. Encode the message `all of our agents must return home at once` using a railfence cipher with 4 rows.

8. Decode the message `OPSPN ERRHA EEHIE ACDOT SNSSF OE` which has been encoded using a 5 row railfence cipher.

9. Consider the cipher which takes A,B,C to 2, D,E,F to 3, G,H,I to 4, J,K,L to 5, M,N,O to 6, P,Q,R,S to 7, T,U,V to 8, W,X,Y,Z to 9. For example, the message `DO NOT TRUST THE NEW RECRUIT` would become `36668 87878 84363 97327 848`.

   (a) Encode the message `the meeting is cancelled`.

   (b) What problems do we have with this cipher? You may wish to consider the message `84474 74273 86332 633`.

   (c) Where is this cipher commonly used?