Cryptography and Codes Assignment 3

1. This message was encrypted using the original caesar cipher

2a) Brute Force since the shift is between 1 and 26

b) i) Key = 7

ii) This message was encrypted using the caesar cipher for the key seven

c) Jhlzhy jpwoly pz lhzfav iylhr!

3 a) Use Frequency analysis

b) i) This text helps as it increases how much cipher text we have to get better frequency analysis and it contains the alphabet in order which will decode to the key.

ii) Key = zyxwvutsrq ponm lkjihg fedcba

iii) This message was encrypted using a mono-alphabetic cipher with the key the permutation with maximum number of inversions

c) Gsv nlml-zokszyvgrx xrksvi rh vzhb gl yivzp!

4 a) $p=13$ $q=19$

$n=pq=13\cdot 19=247$

$\varnothing(247)=\varnothing(13)\varnothing(19)=12\cdot 18=216$

We'll choose $e=7$ and $\gcd(7,216)=1$

Inverse of 7:

$7d\equiv 1 \pmod{216}$

$7d\equiv 217 \pmod{216}$

$d\equiv 31 \pmod{216}$

Therefore:

$KU=(7,247)$

$KR=(31,247)$

Encode Message:

e2 7c 21 3c 7c 4e d2 35 f1 67 7c
c7 d8 41 7c 5a bc 7c da f1 2c bc
23 da 7c 5a 9c 35 d2 7c 3c da d2
21 67 da

b) Message was encoded with $(5,247)$

So:

$\varnothing(247)=216$

$5d\equiv 1 \pmod{216}$

$5d\equiv 865 \pmod{216}$

$d\equiv 173 \pmod{216}$

Decrypt Message:

The private key of the RSA algorithm is one hundred and seventy three, which can be discovered by finding the inverse of 5 in Z_m, where m is 216.

c) We can use brute force since $\varnothing(247)$ is easily calculable to 216 and therefore $0<d<216$ which is a small number of keys to attempt

5 a) $q = 131$

$\alpha = 31$

$Y_A = 23$

$Y_B = 125$

A

$Y_A \equiv \alpha^{X_A} \pmod{q}$

$23 \equiv 31^{X_A} \pmod{131}$

$X_A = 77$

$K = Y_B^{X_A} \bmod 131$

$= 125^{77} \bmod 131$

$= 7$

B

$Y_B \equiv \alpha^{X_B} \pmod{131}$

$125 \equiv 31^{X_B} \pmod{131}$

$X_B = 72$

$K = Y_A^{X_B} \bmod 131$

$= 23^{72} \bmod 131$

$= 7$

b) This message is also encrypted with a generalized Version of caesar cipher, but the key may be greater than twenty six as it is equivalent with its module mod twenty six

Decoded by $X - 7$ or $X + 19$ where $X \in \{A, \dots Z\}$

6 a) Show that this scheme works.

Proof:

Assume the signature is valid.

There fore $Y = (a^z)^h = a^x \mod q$

Also since $a < q$ and q is prime $\gcd(a, q) = 1$

Then $zh \equiv x \pmod{\varnothing(q)}$

$zh \equiv x \pmod{q-1}$ Since q is prime.

Therefore since we reselt in an equality we have proven the scheme works.

QED

b) Show that this scheme is unacceptable by forging techniq

Proof:

Calculate some z sukh that $z \times h \equiv 1 \pmod{q-1}$

Therefore $Y = (a^z)^h \equiv a$

$= ((a^z)^h)^x = a^x$

$= a^x = a^x$

Therefore we can forge the signiture and the scheme becomes unacceptable.

QED