Lab 1 Report
Name : Aravindhan Eswaran
Course : CS 5770 Software Vulnerabilities and Security

1. **Given** : Ciphertext (ycvejqwvhqtdtwvwu)
   Encryption method used : Shift cipher
   To find : Plaintext

Maximum possible shift which can be performed is 25. So for every possible shift value the corresponding plain text value is calculated and stored in the result array. Finally on analyzing the outputs the plain text was found to be 'watchoutforbrutus'

Plaintext : watchoutforbrutus

2. **Given** : Ciphertext (edsgickxhuklzveqzvkxwkzukcvuh)
   Encryption method used : Affine cipher
   To find : Plaintext

Since affine cipher is used. We need to calculate two values namely 'a' and 'b' because
(y = ax + b).

We know that $a*a^{-1} = 1 \bmod 26$. So the possible values of 'a' will be set of all co-primes from (1 - 25) with 26. Then using the above function we calculate the 'a^{-1}'.
The set of all values are given as follows:

All possible A^{-1} = [1, 9, 21, 15, 3, 19, 7, 23, 11, 5, 17, 25]

'b' is the normal shift operation values and it can be anywhere between 0 and 25.

So we calculate all the possible and store them in the output array. Also, given is the first two characters of the plaintext. With that data we find the output text to be 'ifyoucanreadthisthankateacher'

Plaintext : ifyoucanreadthisthankateacher

Another approach to solve the problem is as follows:

It is given that the plaintext has 'if' as the first two characters. So we can find from the given values that 'i' has become 'e' and 'f' has become 'd'. Writing them as equations we get:

8a + b = 4
5a + b = 3

Solving these equations we get a = 3 and b = 10. Using these values also we can find the plaintext.

3. **Given** : Alphabets with corresponding number representation

('A' – 0, 'C' – 1, 'G' – 2, 'T' - 3)

a. **To find** : Ciphertext with a shift of 1

There are four steps involved in this operation:
Step 1: Convert from string format to number format using the above representation
Step 2: Add a shift of +1 to every number in the array. If the value = 4 make it 0
Step 3: Produce string from the number array
Step 4: Display the ciphertext

b. **To find** : Cipher text after performing affine cipher

Step 1: Convert from string format to number format using the above representation
Step 2: Multiply every number with 'a' and shift by 'b'.
Step 3: Produce string from number array
Step 4: Display the ciphertext

Limitations of Affine Cipher:

- If a = 1, affince cipher become shift cipher
- If any two values of the ciphertext and the corresponding values of the plain text are known, it is easy to write them down and equations and solve them to obtain 'a' and 'b'
- Since all possible 'a' values are co-primes to 26, there are only 12 possible 'a' values. So the number of possible ciphertext combinations also reduce significantly.

4. **Given** : n = 718548065973745507
e = 3449
d = 543546506135745129
Encryption method used : RSA
To find : The factors (p and q) of n

Reference :

- NIST : http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf (Appendix C)
- Link : http://www.di-mgt.com.au/rsa_factorize_n.html
- Stackoverflow : http://stackoverflow.com/questions/2921406/calculate-primes-p-and-q-from-private-exponent-d-public-exponent-e-and-the

Steps:
Step 1: Calculate k = (d*e) – 1
Step 2: If k is even, go to step 3, else exit
Step 3: Choose a random g from [2, n-1] and set t = k
Step 4: If (t % 2 == 0) then step 5, else step 6
Step 5: t = t / 2, x = g ^ t , go to step 4
Step 6: If x > 1 , then go to step 7, else go to step 3
Step 7: y = gcd(x-1, n)
Step 8: p = y and q = n/p