INFSCI-2150 Information Security and Privacy

Programming Project Report

Chi-Heng Hung CHH162

1. Message Digest

```
Please type the word that will be hashed
Thequickbrownfoxjumpsoverthelazydog
Original text : Thequickbrownfoxjumpsoverthelazydog
MD5 digested  : 645a2c842335d4b53c68c6f7efc10ab6
SHA digested  : 03ee69ef5240311b4691b28509598faa5092f8a8
```

2. Crypto Techniques

i. Signature

ElGamal Alice:

```
Message : The quick brown fox jumps over the lazy dog.
Signature 607308723040631371670173568275434747999095542772395173378435997703727349844973
```

ElGamal Bob:

```
Message : The quick brown fox jumps over the lazy dog.
Do the signature matches the message? true
```

ii. Encryption

Cipher Client:

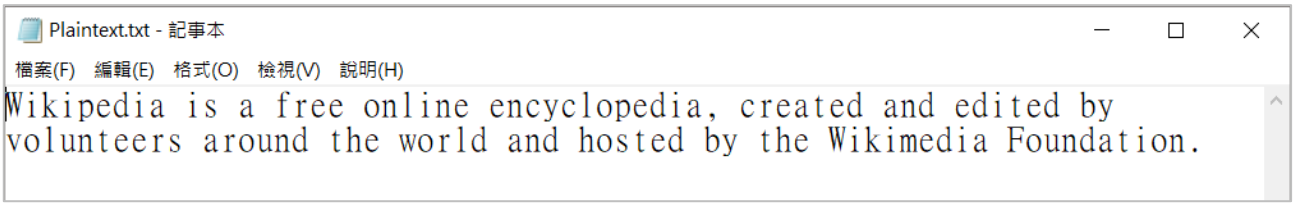
```
DES Key : [B@50675690
Plaintext : The quick brown fox jumps over the lazy dog.
Ciphertext : ?"g??'  %6s□鰍\?*?'□0wsG  +>  桧咀-  ??*□0□?□ZF2
```

Cipher Server:

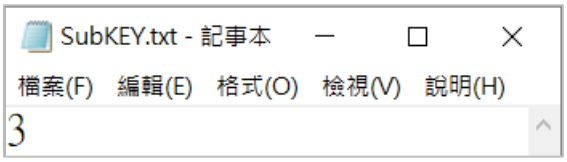
```
DES key : [B@50675690
Decrypt result : The quick brown fox jumps over the lazy dog.
```

3. Breaking a Substitution Cipher

Plaintext



Key



i. Substitution Encrypt & Decrypt

Substitution Encrypt

```
Plaintext : Wikipedia is a free online encyclopedia, created and edited by volunteers around the world and hosted by the Wikimedia Foundation.
Ciphertext : Zlnlshgld#lv#d#iuhh#rqolqh#hqfbforshgld/#fuhdwhg#dqg#hglwhg#eb#yroxqwhhuv#durxqg#wkh#zruog#dqg#krvwhg#eb#wkh#Zlnlphgld#Irxqgdwlrq1
```

Substitution Decrypt

```
Ciphertext : Zlnlshgld#lv#d#iuhh#rqolqh#hqfbforshgld/#fuhdwhg#dqg#hglwhg#eb#yroxqwhhuv#durxqg#wkh#zruog#dqg#krvwhg#eb#wkh#Zlnlphgld#Irxqgdwlrq1

Plaintext : Wikipedia is a free online encyclopedia, created and edited by volunteers around the world and hosted by the Wikimedia Foundation.
```

ii. Top 7 correlation values

```
1 result :
   Key : 3
   Plaintext : wikipedia is a free online encyclopedia, created and edited by volunteers around the world and hosted by the wikimedia foundation.

2 result :
   Key : 25
   Plaintext : xjljqfejb jt b gsff pomjof fodzdmpqfejb  dsfbufe boe fejufe cz wpmvouffst bspvoe uif xpsme boe iptufe cz uif xjljnfejb gpvoebujpo???
3 result :
   Key : 14
   Plaintext : jvxvcrqvn?vf?n?serr?bayvar?raplpybcrqvn ?perngrq?naq?rqvgrq?ol?ibyhagrref?nebhaq?gur?jbeyq?naq?ubfgrq?ol?gur?jvxvzrqvn?sbhaqngvba ?¯ ¢
4 result :
   Key : 18
   Plaintext : rdfdkzydv?dn?v?amzz?jigdiz?zixtxgjkzydv??xmzvozy?viy?zydozy?wt?qjgpiozzmn?vmjpiy?ocz?rjmgy?viy?cjnozy?wt?ocz?rdfdhzydv?ajpiyvodji????
5 result :
   Key : 13
   Plaintext : eqsqxmlqi?qa?i?nzmm?wvtqvm?mvkgktwxmlqi??kzmibml?ivl?mlqbml?jg?dwtcvbmmza?izwcvl?bpm?ewztl?ivl?pwabml?jg?bpm?eqsqumlqi?nwcvlibqwv????
6 result :
   Key : 7
   Plaintext : xjljqfejb?jt?b?gsff?pomjof?fodzdmpqfejb??dsfbufe?boe?fejufe?cz?wpmvouffst?bspvoe?uif?xpsme?boe?iptufe?cz?uif?xjljnfejb?gpvoebujpo£???
7 result :
   Key : 19
   Plaintext : eqsqxmlqi?qa?i?nzmm?wvtqvm?mvkgktwxmlqi??kzmibml?ivl?mlqbml?jg?dwtcvbmmza?izwcvl?bpm?ewztl?ivl?pwabml?jg?bpm?eqsqumlqi?nwcvlibqwv????
```