IS-2150/TEL2810: Information Security and Privacy, Spring 2016
Programming Project

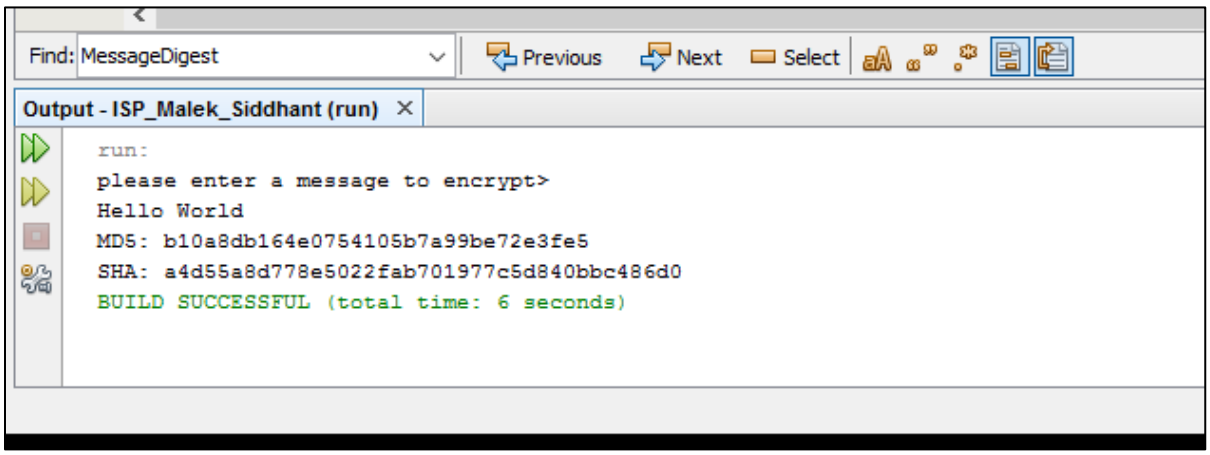
Malek Alahmadi & Siddhant Gupta

To run our programs, please open the file project "**ISP_Malek_Siddhant**" using a JAVA IDE platform (We used NetBeans 8.2 IDE).

1. Message Digest [15 Points]

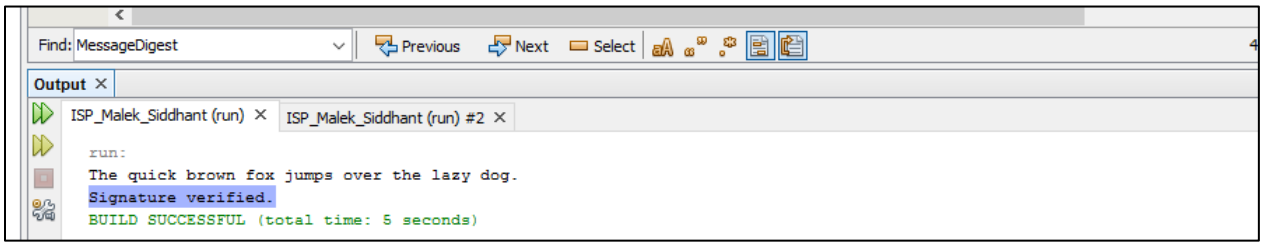
To Encrypt a string in one-way hash function:
1. Right click on the **MD5_SHA.java** file and choose **run file.**
2. Enter the text for encryption.
3. The program will show a MD5 and SHA encryption for this text.

In this example, we used the text: Hello World



2.1) Signature

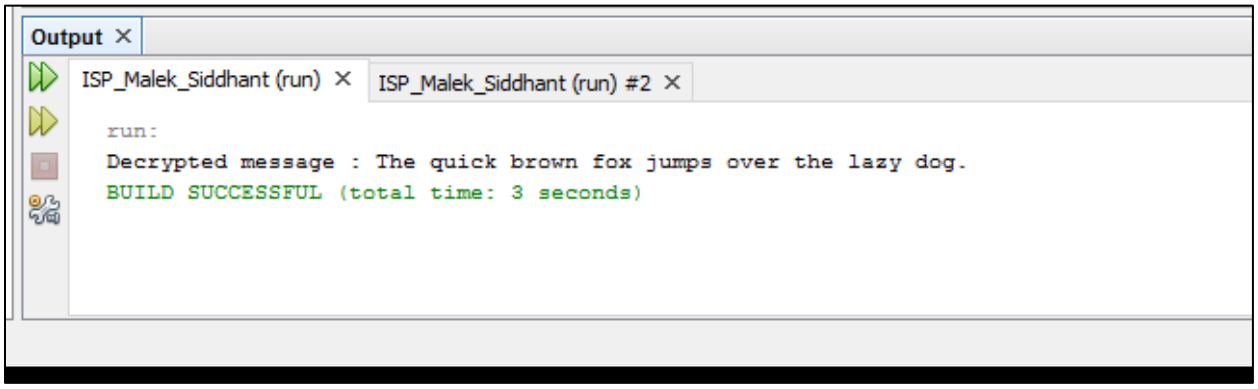
To run this program, we need to:
1. Right click on the **ElGamalBob.java** file first and choose **run file.**
2. Right click on the **ElGamalAlice.java** file second and choose **run file.**
3. **ElGamalBob.java** will show **Signature verified** after process is done.



2.2 Encryption [20 points]

To run this program, we need to:

1. Right click on the **CihperServer.java** file first and choose **run file.**
2. Right click on the **CippherClient.java** file second and choose **run file.**
3. **CihperServer.java** will decrypted the encrypted message sent by the client and show the output to the user.

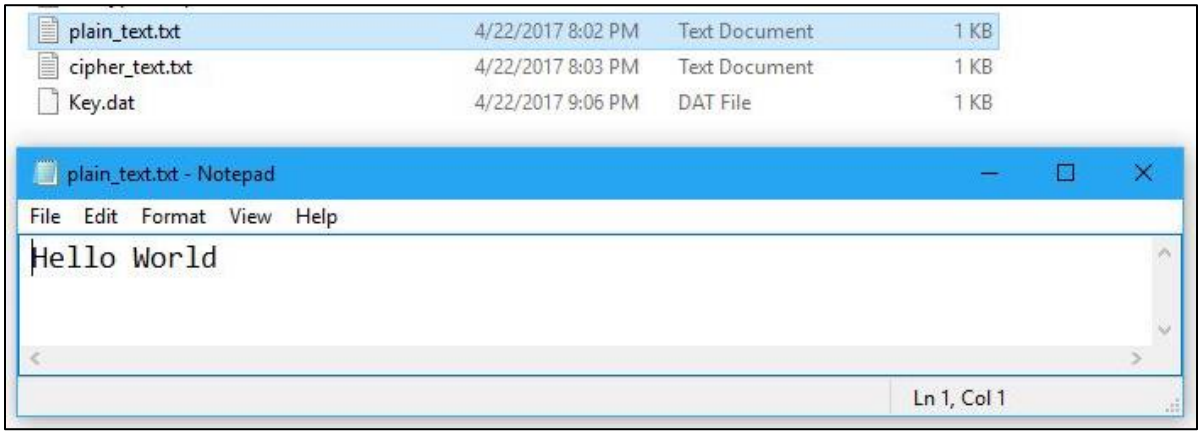


3. Breaking a Substitution Cipher

3.1:

To run this program, we need to:

1. Right click on the **Substitution_Enc.java** file first and choose **run file.** For this step to run successfully, we must have a text file called "**plain_text.txt**" in the project directory. The file is already provided in the project file.



In this example, we used "Hello World" as an input

2. Then, we need to enter a number 0-25 as a key for encryption. In this example, we used K = 3.

```
Output - ISP_Malek_Siddhant (run)
run:
Plain text: Hello World
Please enter a key number from 0 - 25 to encrypt your message>
3
Cipher text: Khoor Zruog
BUILD SUCCESSFUL (total time: 2 seconds)
```

As can be seen above, cipher text is: Khoor Zruog

Name	Date modified	Type	Size
nbproject	4/17/2017 9:20 PM	File folder	
src	4/17/2017 9:20 PM	File folder	
test	4/17/2017 9:47 PM	File folder	
build	4/22/2017 3:19 AM	File folder	
build.xml	4/17/2017 9:20 PM	XML Document	4 KB
manifest.mf	4/17/2017 9:20 PM	MF File	1 KB
Decrypted_cipher_text.txt	4/22/2017 7:50 PM	Text Document	1 KB
plain_text.txt	4/22/2017 8:02 PM	Text Document	1 KB
cipher_text.txt	4/22/2017 9:15 PM	Text Document	1 KB
Key.dat	4/22/2017 9:06 PM	DAT File	1 KB

cipher_text.txt is created.

3. Right click on the **Substitution_Dec.java** file second and choose **run file.** For this step to run successfully, we must have a text file called "**cipher_text.txt**" in the project directory. The file is created automatically by **Substitution_Enc.java** project file.
4. Then, we need to enter a number 0-25 as a key for decryption. In this example, we used K =3.

```
Output - ISP_Malek_Siddhant (run)
run:
Cipher text: Khoor Zruog
Please enter a key number from 0 - 25 to decrypt your message>
3
Plain text: Hello World
BUILD SUCCESSFUL (total time: 11 seconds)
```

As can be seen above, plain text is: Hello World

Name	Date modified	Type	Size
nbproject	4/17/2017 9:20 PM	File folder	
src	4/17/2017 9:20 PM	File folder	
test	4/17/2017 9:47 PM	File folder	
build	4/22/2017 3:19 AM	File folder	
build.xml	4/17/2017 9:20 PM	XML Document	4 KB
manifest.mf	4/17/2017 9:20 PM	MF File	1 KB
Decrypted_cipher_text.txt	4/22/2017 7:50 PM	Text Document	1 KB
plain_text.txt	4/22/2017 8:02 PM	Text Document	1 KB
cipher_text.txt	4/22/2017 9:15 PM	Text Document	1 KB
Key.dat	4/22/2017 9:06 PM	DAT File	1 KB

Decrypted_cipher_text.txt is created.

3.2:

To run this program, we need to:

1. Right click on the **cryptanalysis.java** file and choose **run file.** For this step to run successfully, we must have a text file called "**cipher_text.txt**" in the project directory. The file is created automatically by **Substitution_Enc.java** project file.
2. The program will show the top 7 probable plain texts. In this example, we used "Khoor Zruog" as an input.

```
Output - ISP_Malek_Siddhant (run)
run:
Cipher text: Khoor Zruog
Key= 6, ϕ(i)= 0.0660, Probable plain text: Ebiil Tloia
Key= 10, ϕ(i)= 0.0635, Probable plain text: Axeeh Phkew
Key= 3, ϕ(i)= 0.0575, Probable plain text: Hello World
Key= 14, ϕ(i)= 0.0535, Probable plain text: Wtaad Ldgas
Key= 13, ϕ(i)= 0.0520, Probable plain text: Xubbe Mehbt
Key= 21, ϕ(i)= 0.0517, Probable plain text: Pmttw Ewztl
Key= 0, ϕ(i)= 0.0482, Probable plain text: Khoor Zruog
BUILD SUCCESSFUL (total time: 0 seconds)
```

As seen above, "Hello World" was in the 3rd spot.

Team member evaluation:

We didn't face any major issues during our project. The project was challenging and full of tricks and obstacles but we enjoyed it so much. We enjoyed solving the problems one by one. This project helped us understanding more the encryption concept and strengthen our programming skills.