

Observational Report LAB 8: Secret-Key Encryption

ACS 545| Cryptography and Network Security

March 20, 2024

Ashutosh Mishra

Professor: ZesHeng Chen

* Observation Criteria: -

Note: -

1. Used Ubuntu Seed (v20.04 Focal) on Google Cloud Platform
2. Used Real VNC Viewer to perform the actions on GUI
3. All actions are being performed under username – **seed**

* Task 1 (Frequency Analysis): -

For this task, I have run the provided code in freq.py inside Labsetup/Files folder.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

From the trigram we can observe that the most common is **ytn**. We can replace it with **THE** and **vup** is **AND. Let’s try that in command.**



A screenshot of a computer

Description automatically generated

Similarly, post trying and figuring the word the final output will look something like below.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Task 2 (Encryption using Different Ciphers and Modes): -

For this task we will be trying three different ciphers. Let’s quickly make a file in Labsetup/Files directory.

A screenshot of a computer

Description automatically generated

1. The first one is using AES ECB. In this we are only passing the Key.

A screenshot of a computer

Description automatically generated

1. The second one is AES CFB using a key and iv.

A screenshot of a computer

Description automatically generated

1. The third one is AES OFB. This also uses a key and iv.

A screenshot of a computer

Description automatically generated

* Task6 (Initial Vector (IV) and Common Mistakes): -
  + Task6.1 (IV Experiment): -

In this task, we will first encrypt the file plain.txt using two different **IVs**.

A screenshot of a computer

Description automatically generated

As we can see here both the encrypted files are different.

Now, let’s try using the same **IV** two times.

A screenshot of a computer

Description automatically generated

We can see that when the same **IV** is used, the issue is that the message is always the same. If a hacker gets hold of this, he/she will be able to decrypt the message on will. Hence, we should make sure that iv is not the same.

* + Task 6.2 (Common Mistake: Use the Same IV): -

In this task the code used is as shown below.

A screenshot of a computer

Description automatically generated

Now let’s run the output

A screenshot of a computer

Description automatically generated

As we can see from the output the text generated is Order: Launch a missile!

If we replace OFB with CFB then the attacker will not be able to recover the plaintext fully.

* + Task 6.3 (Common Mistake: Use a Predictable IV): -

In this task the code used is as shown below.

A screen shot of a computer

Description automatically generated

Now, let’s setup the environment using dcbuild, dcup and check the containers installed.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Now, in this subtask we will guess what Bob voted for. Let’s perform nc on db.

A screenshot of a computer

Description automatically generated

Let’s make a guess file with output as **Yes** and find the hex of that.

A screenshot of a computer

Description automatically generated

Now, we need to pad the generated hex value with  **The IV used** value.

A screenshot of a computer

Description automatically generated

Now, put the generated value with the **Next IV**.

A screenshot of a computer

Description automatically generated

Now take the generated value and put it in **Your plaintext**.

A screenshot of a computer

Description automatically generated

The generated answer is same as Bob’s secret message. Hence, our guess was right.

* Task 7 (Programming using the Crypto Library): -

For this task I have used the following code.

A screenshot of a computer

Description automatically generated

Now, post running the code, the answer was **Purdue##########.**

**A screenshot of a computer

Description automatically generated**

* Conclusion: -

The overall experience was exciting. I will be going deeper into the subject and try to discover new ways to handle how we had practiced in lab. Having a base knowledge of how Secret Key Encryption works, I would like to do a deep dive into this subject to find out more about how to protect the target machines from attacks that occur in a simple manner.