

Observational Report LAB 10: RSA Encryption and signature lab

ACS 545| Cryptography and Network Security

April 22, 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 (Deriving the Private Key): -

Note: - Firstly, we need to install libssl-dev. As I am using a cloud VM.

A screenshot of a computer

Description automatically generated

For this task, I have slightly modified the C code as below.

A screenshot of a computer code

Description automatically generated

Now we will compile the code as shown below and run the script.

A screenshot of a computer

Description automatically generated

The value of private key is Private key: 3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB

* Task 2 (Encrypt a Message): -

First, we generate the hex equivalent of the message “**A top secret!”.**

A screenshot of a computer

Description automatically generated

For this task, I have slightly modified the C code as below.

A screenshot of a computer

Description automatically generated

Now we will compile the code as shown below and run the script.

A screenshot of a computer

Description automatically generated

As we can see, the Original Message that’s decrypted is right. The encryption value was correct.

* Task3 (Decrypt a Message): -

In this task, we will be using the following C program.

A screenshot of a computer

Description automatically generated

Now we will compile the code as shown below and run the script.

A screenshot of a computer

Description automatically generated

Let’s decrypt this value using Python.

A screenshot of a computer

Description automatically generated

The decrypted message is “**Password is dees”**.

* Task 4 (Signing a Message): -

For this task first we find out the hex value of both the messages as shown below.

A screenshot of a computer

Description automatically generated

In this task, we will be using the following C program.

A screenshot of a computer

Description automatically generated

Now we will compile the code as shown below and run the script.

A screenshot of a computer

Description automatically generated

The signatures for both the strings are different even when one character was modified.

* Task 5 (Verifying a Signature): -

First, we need the hex value equivalent of “**Launch the missile.**”

A screenshot of a computer

Description automatically generated

In this task, we will be using the following C program.

A screenshot of a computer program

Description automatically generated

Now we will compile the code as shown below and run the script.

A screenshot of a computer

Description automatically generated

As we can see that for S1 the verified value and signature is same but for a slightly different value the verification fails.

* Task 6 (Manually Verifying an X.509 Certificate): -

1. **Step – 1: Download a certificate from a real web server**

We will fetch the certificate from below command.

A screenshot of a computer

Description automatically generated

I have saved both the certificates as c0.pem and c1.pem



1. **Step – 2: Extract the public key (e, n) from the issuer’s certificate**

The value for modulus (n) and exponent (e) is as shown below.

A screenshot of a computer code

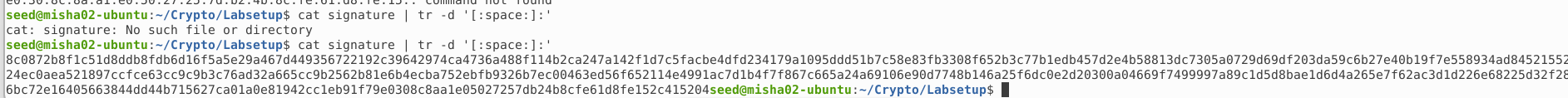
Description automatically generated

1. **Step – 3: Extract the signature from the server’s certificate**

A screen shot of a computer

Description automatically generated

Saving the signature file and running the following command



1. **Step – 4: Extract the body of the server’s certificate**

Now we run the following command

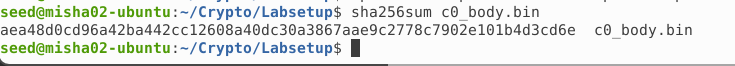
A screenshot of a computer

Description automatically generated

Now running the following command



Now run the next command



1. **Step – 5: Verify the signature**

The program is as shown below

A screenshot of a computer

Description automatically generated

Now compiling and running the output

A screen shot of a computer

Description automatically generated

The signature is verified.

* 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 RSA works, I would like to do a deep dive into this subject to find out more about the same.