**SYSTEM SECURITY**

**LAB-7**

**Name: Krushal Shah**

**P.R.N: 20190802058**

**1. What is the key length considered in implementing AES crypt?** The key length considered in implementing AES crypt is 256-bit.

**2. How many rounds of encryption are used in AES crypt?**

AES crypt uses 14 rounds of encryption.

**3. Which programming languages have been used to implement AES crypt? The programming languages that have been used to implement AES crypt are as follows:**

• C

• C++

• Java

• Go

• JavaScript

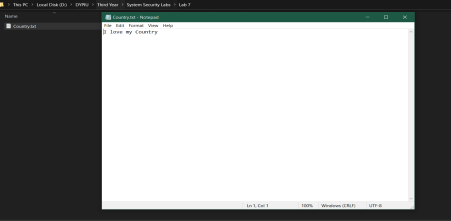
• C#

• PHP

**4. Create a file naming country.txt and write down a single line of text into it (i.e., I love my country). Your task is to provide this file as an input to the AES crypt. Write down what changes you have observed after applying AES encryption to it**

A simple txt file is created and named “country.txt” with I love my

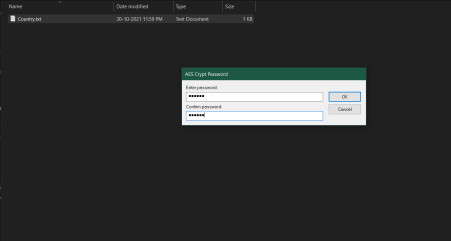
country as a content inside the file.



After right click, we find an encrypt option which we click and the

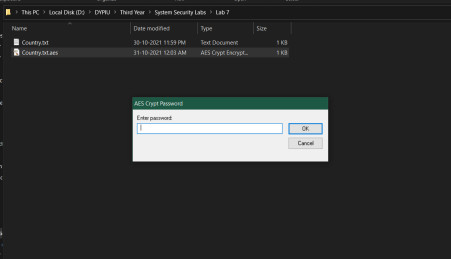
following shown dialog in the image appears where we set our new

password and confirm it and click ok to create an encrypted file with .AES extension.

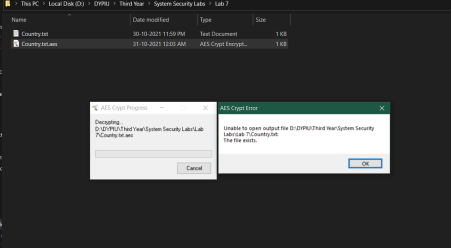


As we can see in the above image, the file with .aes file extension has

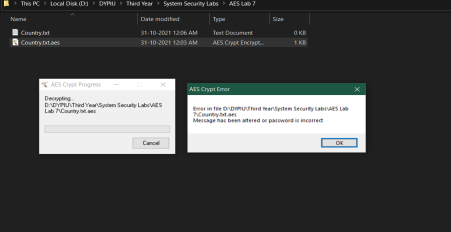
been created. Opening it on the spot will ask you for your password as follows:



After typing password, it will immediately throw an error as follows:

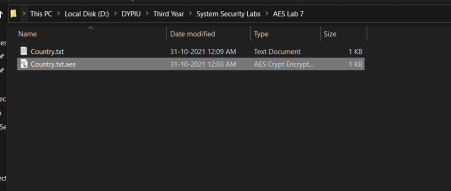
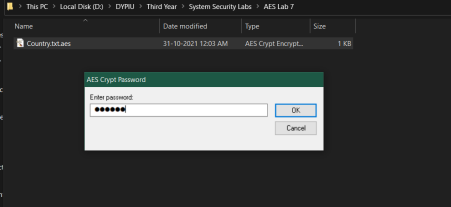
So, we cut and paste the encrypted file in another directory.

Then we double click the file to open it. The password dialog box appears to ask us for our password. If we give invalid password, the following error occurs: Even though we can briefly see our original file here, we cannot open it, delete it or do any other manipulations on the file. As soon as the error goes away, so does the original file as well. We need to put correct password or else we won’t be able to access the file.

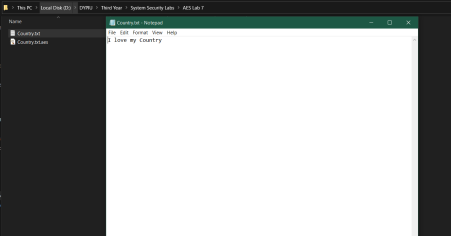


But if we give correct password, the original file stays permanently here and is now freely available for any manipulations the user wants to

perform.



The contents of the original file have been retrieved as you can see in the following image:



Thus, we have learned about AES software i.e., AES crypt and learned how to implement it.