System Security

Monsoon Semester V 2021-22

Lab - 7

Date: 26th October 2021

Topic: AES Crypt

AIM

Install an open-source software named AES crypt.

EXPERIMENT

Answer the following questions after studying the above software.

1) What is the key length considered in implementing AES crypt?

Ans. AES includes three block ciphers:

1. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
2. AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
3. AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.

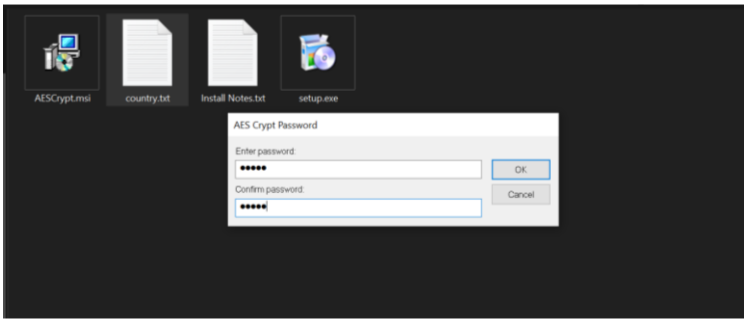
2) How many rounds of encryption are used in AES crypt?

Ans. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

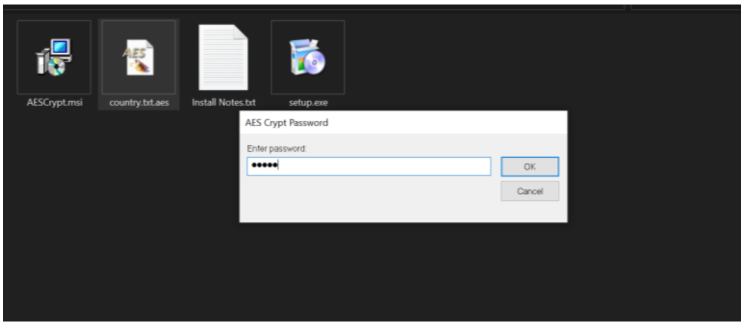
3) Which programming languages have been used to implement AES crypt?

Ans. AES algorithms were tested extensively in American National Standards Institute (ANSI), C and Java languages

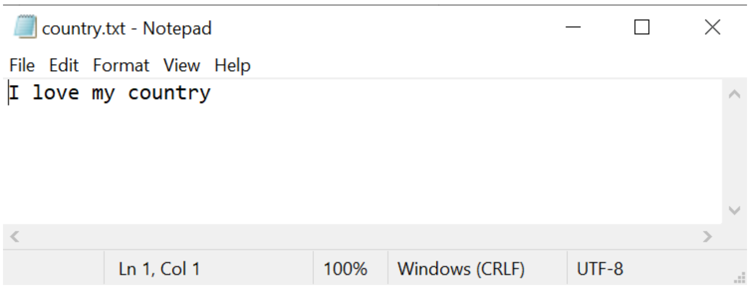
4) **Create a file naming *country.txt* and write down a single line of text into it (i.e., I love my country). Your task is to provide this file as an input to the AES crypt. Write down what changes you have observed after applying AES encryption to it.**



On applying AES encryption to the file a new file with the same name with .aes extension is created.



On decrypting the file with the set password we get the original file back.



```
I love my country
```

CONCLUSION

Hence, AES software was installed and the text file was encrypted successfully.