

Introduction to Advance Encryption Standard (AES)

CS681 & CS392 Computer Security

Fall 2004

Due 09/22/2004

September 9, 2004

1 Objective

The object of this assignment is to build a part of the file encryption and decryption module for FEAU.

2 AES

You should be familiar with the AES algorithm. The algorithm was briefly described in class.

- You can learn more about AES from: <http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>
- Download AES code from: <http://fp.gladman.plus.com/AES/aes.zip>
- Get familiarized with AES key generation, encryption, and decryption functions and the test code

2.1 Warm Up

It is a good development practice to make sure you understand the code you are using before you dive in and start to develop applications with it. The following questions would help you understand AES in algorithm in general and the AES code.

1. What is NIST, FIPS, and Rijndael?
2. What is the name of the file in the AES package which contains the test or example code? (If you get this question wrong, you fail the lab :))
3. What encryption modes does the given AES code support? and how does one specify which mode to use?
4. Which function encrypts a block of code and what does it return?
5. Which function decrypts a block of code and what does it return?
6. Describe the process for specifying the key used for encryption/decryption.
7. Does the test code or core AES code handle error? If yes what kind of errors can it handle and how is it handling them?
8. What is the purpose of S-box in AES and how is it implemented in the code? (i.e. Describe the s-box implementation using flowchart)
9. What is the purpose of `aes_encrypt_ctx` and `aes_decrypt_ctx` structures in the AES code?
10. How are round keys generated and used for encryption and decryption in the AES code? (Use flowchart)

2.2 File Encryption

First take a break..... Now that you are an expert in AES, apply your expertise to develop a part of the file encryption and decryption module for FEAU. Basically, you will be adding enc and dec command to the shell you have created in the last assignment.

enc - Encrypt file

Synopsis - enc [file] [key]

Description enc encrypts the contents of the file, store the encrypted file with the same name as before with .aes appended to it in the end, and delete the source file.

dec - Decrypt file

Synopsis - dec [file] [key]

Description dec decrypts the contents of the file, delete the source file, and move the decrypted file to its original location.

Please note the above specifications for enc and dec are different from the specifications in FEAU project document. It is different because the final version of enc and dec will use more than one crypto system to encrypt/decrypt file and directories. It will be a lot more complex than simple file encryption.

3 What and how to Handin

For this assignment you must submit answers for all of the above section on or before midnight 09/22/2004. We prefer you to e-mail your submission to vikram@isis.poly.edu with subject line "CS392 lab 1 <your name>" with out the quotes. Subject line is very important if you want to receive any credits.