Coleman Lyski

Dr. Boyang Wang

CS-5153 Network Security

19 February 2021

Project 1: Advanced Encryption Standard

Project Information

This project was written in Python 3.8 with no third-party libraries on a Windows 10 machine. To run the program, navigate to the `./src/` folder and run the command `python main.py`. This will print the output of every function to the terminal window where you ran the command as well as save the result in `./data/result.txt`.

`./src/main.py` is the main script that drives the program.

`./src/aes.py` contains all the AES related functions.

`./src/util.py` contains some utility functions, mostly for printing results.

The code for this project can also be found on my GitHub.

Output Screenshots

```
Plaintext: Two One Nine Two
SubKey0: 0x5468617473206d79204b756e67204675
SubKey1: 0xe232fcf191129188b159e4e6d679a293
```

Figure 1: The first output shows the plaintext and the two keys used

```
Initial State:
[   ['0x54', '0x4f', '0x4e', '0x20'],
    ['0x77', '0x6e', '0x69', '0x54'],
    ['0x6f', '0x65', '0x6e', '0x77'],
    ['0x20', '0x20', '0x65', '0x6f']]

SubKey0:
[   ['0x54', '0x73', '0x20', '0x67'],
    ['0x68', '0x20', '0x4b', '0x20'],
    ['0x61', '0x6d', '0x75', '0x46'],
    ['0x74', '0x79', '0x6e', '0x75']]

AddKey:
[   ['0x0', '0x3c', '0x6e', '0x47'],
    ['0x1f', '0x4e', '0x22', '0x74'],
    ['0xe', '0x8', '0x1b', '0x31'],
    ['0x54', '0x59', '0xb', '0x1a']]
```

Figure 2: The Initial State is generated from the plaintext, and then SubKey0 is added to the Initial State by the AddKey function

```
Start of Round 1:

SubBytes:
[   ['0x63', '0xeb', '0x9f', '0xa0'],
    ['0xc0', '0x2f', '0x93', '0x92'],
    ['0xab', '0x30', '0xaf', '0xc7'],
    ['0x20', '0xcb', '0x2b', '0xa2']]

ShiftRows:
[   ['0x63', '0xeb', '0x9f', '0xa0'],
    ['0x2f', '0x93', '0x92', '0xc0'],
    ['0xaf', '0xc7', '0xab', '0x30'],
    ['0xa2', '0x20', '0xcb', '0x2b']]

MixColumns:
[   ['0xba', '0x84', '0xe8', '0x1b'],
    ['0x75', '0xa4', '0x8d', '0x40'],
    ['0xf4', '0x8d', '0x6', '0x7d'],
    ['0x7a', '0x32', '0xe', '0x5d']]

AddKey:
[   ['0x58', '0x15', '0x59', '0xcd'],
    ['0x47', '0xb6', '0xd4', '0x39'],
    ['0x8', '0x1c', '0xe2', '0xdf'],
    ['0x8b', '0xba', '0xe8', '0xce']]
```

Figure 3: The first round of AES is performed

```
Round 1 Results:
0x5847088b15b61cba59d4e2e8cd39dfce
```

Figure 4: The resulting matrix is converted back to a 128-bit Hexadecimal value and printed to the screen

result.txt - Notepad

File Edit Format View Help

```
Plaintext: Two One Nine Two
SubKey0: 0x5468617473206d79204b756e67204675
SubKey1: 0xe232fcf191129188b159e4e6d679a293

Round 1 Results:
0x5847088b15b61cba59d4e2e8cd39dfce
```

Figure 5: A result text file is generated with just the starting values and the result after round one of AES