과제 #1
CSE3029 암호학
2017-09-27

1. 목표

AES 암·복호화 알고리즘을 구현한다.

2. 문제

제한사항에서 제시한 함수를 작성하여 AES 암·복호화 알고리즘을 구현한다.

3. 제한 사항

과제의 **함수명**과 **변수명**은 반드시 다음과 동일하게 구현한다.

void expandKey(BYTE *key, BYTE *roundKey)
1) key: 키 스케줄링을 수행할 16바이트 키
2) roundKey: 키 스케줄링의 결과인 176바이트 라운드 키가 담길 공간

BYTE* subBytes(BYTE *block, int mode)
1) block: SubBytes 수행할 16바이트 블록, 수행 결과는 해당 배열에 바로 반영
2) mode: SubByte 수행 모드

BYTE* shiftRows(BYTE *block, int mode)
1) block: ShiftRows 수행할 16바이트 블록, 수행 결과는 해당 배열에 바로 반영
2) mode: ShiftRows수행 모드

BYTE* mixColumns(BYTE *block, int mode)
1) block: MixColumns을 수행할 16바이트 블록, 수행 결과는 해당 배열에 바로 반영
2) mode: MixColumns의 수행 모드

BYTE* addRoundKey(BYTE *block, BYTE *rKey)
1) block: AddRoundKey를 수행할 16바이트 블록, 수행 결과는 해당 배열에 바로 반영
2) rKey: AddRoundKey를 수행할 16바이트 라운드키

void AES128(BYTE *input, BYTE *output, BYTE *key, int mode)
mode가 ENC일 경우 평문을 암호화하고, DEC일 경우 암호문을 복호화하는 함수

[ENC 모드]
1) input: 평문 바이트 배열
2) output: 결과(암호문)이 담길 바이트 배열
   호출하는 사용자가 사전에 메모리를 할당하여 파라미터로 넘김
3) key: 128비트 암호키 (16바이트)

[DEC 모드]
1) input: 암호문 바이트 배열
2) output: 결과(평문)이 담길 바이트 배열
   호출하는 사용자가 사전에 메모리를 할당하여 파라미터로 넘김
3) key: 128비트 암호키 (16바이트)

4. 참고 사항

필요한 경우 추가로 코드를 작성한다.

'test_AES128.c'는 암·복호화 결과를 테스트 위한 소스 파일로 수정하지 않으며, 제출하지 않아도 된다.

5. 제출물

"[학번_이름]_AES128.zip" - 과제의 소스 파일(AES128.c, AES128.h 또는 추가 구현 소스 파일)을 앞의 이름과 같이 압축해 마감일을 엄수하여 joontaechoi@gmail.com으로 제출한다.

6. 마감기한

가. 마감일: 2017년 10월 14일(토요일) 자정 전까지

나. 마감일을 넘겨 제출할 경우, 하루 단위로 총점의 20%씩 감점된다.

7. 참고자료

가. FIPS PUB 197, Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

8. 문의사항

가. 제 3 공학관 519-2호 정보보호연구실 최준태 조교

나. joontaechoi@gmail.com, 메일 보낼 시에 학번과 성명 표기해주세요

- 결과 예제

```
 - Plain Text :
6b c1 be e2 2e 40 9f 96 e9 3d 7e 11 73 93 17 2a
ae 2d 8a 57 1e 03 ac 9c 9e b7 6f ac 45 af 8e 51
30 c8 1c 46 a3 5c e4 11 e5 fb c1 19 1a 0a 52 ef
f6 9f 24 45 df 4f 9b 17 ad 2b 41 7b e6 6c 37 10
 - Encrypted Plain Text :
76 49 ab ac 81 19 b2 46 ce e9 8e 9b 12 e9 19 7d
50 86 cb 9b 50 72 19 ee 95 db 11 3a 91 76 78 b2
73 be d6 b8 e3 c1 74 3b 71 16 e6 9e 22 22 95 16
3f f1 ca a1 68 1f ac 09 12 0e ca 30 75 86 e1 a7
==================================
AES Encryption: SUCCESS!
==================================
 - Cipher Text :
76 49 ab ac 81 19 b2 46 ce e9 8e 9b 12 e9 19 7d
50 86 cb 9b 50 72 19 ee 95 db 11 3a 91 76 78 b2
73 be d6 b8 e3 c1 74 3b 71 16 e6 9e 22 22 95 16
3f f1 ca a1 68 1f ac 09 12 0e ca 30 75 86 e1 a7
 - Decrypted Cipher Text :
6b c1 be e2 2e 40 9f 96 e9 3d 7e 11 73 93 17 2a
ae 2d 8a 57 1e 03 ac 9c 9e b7 6f ac 45 af 8e 51
30 c8 1c 46 a3 5c e4 11 e5 fb c1 19 1a 0a 52 ef
f6 9f 24 45 df 4f 9b 17 ad 2b 41 7b e6 6c 37 10
==================================
AES Decryption: SUCCESS!
==================================
```