Assignment #1
CSE3029 암호학
2018-10-02

1. 목표

AES 암·복호화 알고리즘을 구현한다.

2. 문제

제한사항에서 제시한 함수를 작성하여 AES 암·복호화 알고리즘을 구현한다.

3. 제한사항

과제의 함수명과 변수명은 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 *state, int mode)
```

1) state: subBytes를 수행할 16바이트 입력 값, 수행 결과는 해당 배열에 바로 반영됨
2) mode: subBytes 수행 모드

```
BYTE* shiftRows(BYTE *state, int mode)
```

1) state: shiftRows를 수행할 16바이트 입력 값, 수행 결과는 해당 배열에 바로 반영됨
2) mode: shiftRows 수행 모드

```
BYTE* mixColumns(BYTE *state, int mode)
```

1) state: mixColumns를 수행할 16바이트 입력 값, 수행 결과는 해당 배열에 바로 반영됨
2) mode: mixColumns 수행 모드

```
BYTE* addRoundKey(BYTE *state, BYTE *roundKey)
```

1) state: addRoundKey를 수행할 16바이트 입력 값, 수행 결과는 해당 배열에 바로 반영됨
2) mode: addRoundKey 수행 모드

```
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: 암호문이 담길 바이트 배열, 호출하는 사용자가 사전에 메모리 할당
3) key: 128비트 암호키 (16바이트)

[DEC 모드]

1) input: 암호문 바이트 배열
2) output: 평문이 담길 바이트 배열, 호출하는 사용자가 사전에 메모리 할당
3) key: 128비트 암호키 (16바이트)

4. 참고사항

필요한 경우 추가로 코드를 작성한다.
'test_AES128.c'는 암·복호화 결과를 테스트 하기 위한 파일이므로
수정하거나 제출하지 않아도 된다.

5. 제출물

"학번_AES128.zip" 형태로 제출한다.
과제의 소스 파일 (AES128.c, AES128.h 등) 앞에도 "학번_"을 추가한다.
마감일을 엄수하여 BlackBoard로 제출한다.

6. 마감기한

1) 마감일: 2018년 10월 14일 (일요일) 자정 전까지
2) 마감일을 넘겨 제출할 경우, 하루 단위를 총점의 20%씩 감점된다.

7. 참고자료

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

8. 문의사항

hseun@hanyang.ac.kr, 메일 보낼 때 학번과 성명 표기해주세요

- 결과 예제