프로젝트 #1

소프트웨어학부 암호학

2020년 9월 24일

목표

키의 길이가 128 비트인 AES (Advanced Encryption Standard) 알고리즘을 표준스펙에 따라 구현한다. 자세한 스펙은 강의노트 또는 FIPS-197 문서를 참조한다.

정수형 타입

프로그램에 사용하는 모든 정수형 타입은 `uint8_t`, `int16_t`와 같이 부호의 유무와 비트의 크기를 명확하게 알 수 있도록 C언어 표준 정수형 타입을 사용한다.

전역 함수

외부에서 보이는 전역 함수를 아래 열거한 프로토타입을 사용하여 구현한다. 각 함수에 대한 요구사항은 다음과 같다.

- `void KeyExpansion(const uint8_t *key, uint32_t *roundKey)` – 길이가 16 바이트인 사용자 키에서 암복호에 사용할 라운드 키를 생성한다. `roundKey`의 길이는 44 워드이어야 한다.
- `void Cipher(uint8_t *state, const uint32_t *roundKey, int mode)` – 크기가 16 바이트인 `state`를 `roundKey`를 사용하여 암복호화한다. 이 때 `mode`가 `ENCRYPT`이면 암호화를 수행하고 `DECRYPT`이면 복호화를 수행한다.

지역 함수

내부에서만 사용하는 지역 함수는 별도로 지정하지 않고, 각자 필요에 맞게 작성한다. 다음에 열거한 함수와 프로토타입은 참고용이다.

- `static void AddRoundKey(uint8_t *state, const uint32_t *roundKey)` – 라운드 키를 XOR 연산을 사용하여 `state`에 더한다.
- `static void SubBytes(uint8_t *state, int mode)` – `mode`에 따라 순방향 또는 역방향으로 바이트를 치환한다.
- `static void ShiftRows(uint8_t *state, int mode)` – `mode`에 따라 순방향 또는 역방향으로 바이트의 위치를 변경한다.
- `static void MixColumns(uint8_t *state, int mode)` – 기약 다항식 $x^8 + x^4 + x^3 + x + 1$을 사용한 GF(2^8)에서 행렬곱셈을 수행한다. `mode`가 `DECRYPT`이면 역행렬을 곱한다.

골격 파일

구현에 필요한 골격파일 `aes_skeleton.c`와 함께 헤더파일 `aes.h`, 프로그램을 검증할 수 있는 `test.c`, 그리고 `Makefile`을 제공한다. 이 가운데 `test.c`를 제외한 나머지 파일은 용도에 맞게 자유롭게 수정할 수 있다.

테스트 벡터

알고리즘이 올바르게 구현되었다면 주어진 키와 평문에 대한 암호문과 라운드 키가 예시와 같이 일치해야 한다.

<키>
```
0f 15 71 c9 47 d9 e8 59 0c b7 ad d6 af 7f 67 98
```
<라운드 키>
```
0f 15 71 c9 47 d9 e8 59 0c b7 ad d6 af 7f 67 98
dc 90 37 b0 9b 49 df e9 97 fe 72 3f 38 81 15 a7
d2 c9 6b b7 49 80 b4 5e de 7e c6 61 e6 ff d3 c6
c0 af df 39 89 2f 6b 67 57 51 ad 06 b1 ae 7e c0
2c 5c 65 f1 a5 73 0e 96 f2 22 a3 90 43 8c dd 50
58 9d 36 eb fd ee 38 7d 0f cc 9b ed 4c 40 46 bd
71 c7 4c c2 8c 29 74 bf 83 e5 ef 52 cf a5 a9 ef
37 14 93 48 bb 3d e7 f7 38 d8 08 a5 f7 7d a1 4a
48 26 45 20 f3 1b a2 d7 cb c3 aa 72 3c be 0b 38
fd 0d 42 cb 0e 16 e0 1c c5 d5 4a 6e f9 6b 41 56
b4 8e f3 52 ba 98 13 4e 7f 4d 59 20 86 26 18 76
```
<평문>
```
01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10
```
<암호문>
```
ff 0b 84 4a 08 53 bf 7c 69 34 ab 43 64 14 8f b9
```

제출물

소스코드, 컴파일 과정과 실행결과를 보여주는 화면캡쳐, 그리고 자신의 결과를 보여주는데 필요한 부가 설명이나 기타 자료를 스스로 판단하여 제출한다. 모든 자료에는 학번과 이름을 명시하고, 소스코드를 제외한 나머지 제출물은 PDF 형식이어야 한다.

마감일

온라인 상으로 정해진 마감시간을 준수해야 하며, 늦게 제출한 과제는 받은 점수에서 50%를 감한다.

HK