Cryptography Program #2

소프트웨어학부

2018044720 석예림

1. gt8_skeleton.c 소스코드

```c
/*
 * Copyright 2020. Heekuck Oh, all rights reserved
 * 이 프로그램은 한양대학교 ERICA 소프트웨어학부 재학생을 위한 교육용으로 제작되었습니다.
 */
#include <stdio.h>
#include <stdlib.h>

/*
 * gf8_mul(a, b) - a * b mod x^8+x^4+x^3+x+1
 *
 * 7차식 다항식 a와 b를 곱하고 결과를 8차식 x^8+x^4+x^3+x+1로 나눈 나머지를 계산한다.
 * x^8 = x^4+x^3+x+1 (mod x^8+x^4+x^3+x+1) 특성을 이용한다.
 */
unsigned char gf8_mul(unsigned char a, unsigned char b)
{
    u_int8_t r = 0;

    while(b > 0) {
        if(b & 1) r = r ^ a;
        b = b >> 1;
        a = ((a<<1)^((a>>7) & 1 ? 0x1B : 0));
    }
    return r;
}

/*
 * gf8_pow(a,b) - a^b mod x^8+x^4+x^3+x+1
 *
 * 7차식 다항식 a을 b번 지수승한 결과를 8차식 x^8+x^4+x^3+x+1로 나눈 나머지를 계산한다.
 * gf8_mul()과 "Square Multiplication" 알고리즘을 사용하여 구현한다.
 */
unsigned char gf8_pow(unsigned char a, unsigned char b)
{
    u_int8_t r = 1;

    while(b > 0){
        if(b & 1) r = gf8_mul(r, a);
        a = gf8_mul(a, a);
        b = b >> 1;
    }
    return r;
}
```

```
43
44  /*
45   * gf8_inv(a) - a^-1 mod x^8+x^4+x^3+x+1
46   *
47   * 모듈러 x^8+x^4+x^3+x+1에서 a의 역을 구한다.
48   * 역을 구하는 가장 효율적인 방법은 다항식 확장유클리드 알고리즘을 사용하는 것이다.
49   * 다만 여기서는 복잡성을 피하기 위해 느리지만 알기 쉬운 지수를 사용하여 구현하였다.
50   */
51  unsigned char gf8_inv(unsigned char a)
52  {
53      return gf8_pow(a, 0xfe);
54  }
55
56  int main(void)
57  {
58      int a, b;
59
60      /*
61       * 간단한 시험
62       */
63      a = 28; b = 7;
64      printf("%d * %d = %d\n", a, b, gf8_mul(a,b));
65      a = 127; b = 68;
66      printf("%d * %d = %d\n", a, b, gf8_mul(a,b));
67      /*
68       * a를 1부터 255까지 a^-1를 구하고 a * a^-1 = 1인지 확인한다.
69       */
70      for (a = 1; a < 256; ++a) {
71          if (a == 0) continue;
72          b = gf8_inv(a);
73          printf("a = %d, a^-1 = %d, a*a^-1 = %d\n", a, b, gf8_mul(a,b));
74          if (gf8_mul(a,b) != 1) {
75              printf("Logic error\n");
76              exit(1);
77          }
78      }
79      printf("No error found\n");
80      return 0;
81  }
```

2. 코드 내 함수 설명

- gf8_mul() : 7 차 다항식 a 와 b 를 곱하고 결과를 8 차식 x^8+x^4+x^3+x+1 로 나눈 나머지를 계산한다. b 의 마지막 비트와 1 의 And 연산 값이 1 일때 나머지와 a 를 XOR 연산하고, b 의 비트 값을 오른쪽으로 하나 이동하여 준다. 그 다음 a 의 차수를 하나 높여 주며 b 의 값이 0 보다 작아질 때 까지 계산해 준다.
- gt8_pow() : 7 차식 다항식 a 을 b 번 지수제곱한 결과를 8 차식 x^8+x^4+x^3+x+1 로 나눈 나머지를 계산한다. a^b modulo m 은(a mod m * a mod m * … * a mod m) mod m 으로 계산되기 때문에 gt8_mul()함수를 사용하여 a 의 지수제곱한 결과에 modulo m 해준 값을 b 의 비트가 1 일때 나머지와 a 를 곱해 나머지를 계산한다.

3. 실행 결과