

Cryptography Program #2

소프트웨어학부

2018044720 석예림

1. gf8_skeleton.c 소스코드

```
1  /*
2  * Copyright 2020. Heekuck Oh, all rights reserved
3  * 이 프로그램은 한양대학교 ERICA 소프트웨어학부 재학생을 위한 교육용으로 제작되었습니다.
4  */
5  #include <stdio.h>
6  #include <stdlib.h>
7
8  /*
9  * gf8_mul(a, b) - a * b mod x^8+x^4+x^3+x+1
10 *
11 * 7차식 다항식 a와 b를 곱하고 결과를 8차식 x^8+x^4+x^3+x+1로 나눈 나머지를 계산한다.
12 * x^8 = x^4+x^3+x+1 (mod x^8+x^4+x^3+x+1) 특성을 이용한다.
13 */
14 unsigned char gf8_mul(unsigned char a, unsigned char b)
15 {
16     u_int8_t r = 0;
17
18     while(b > 0) {
19         if(b & 1) r = r ^ a;
20         b = b >> 1;
21         a = ((a<<1)^((a>>7) & 1 ? 0x1B : 0));
22     }
23     return r;
24 }
25
26 /*
27 * gf8_pow(a,b) - a^b mod x^8+x^4+x^3+x+1
28 *
29 * 7차식 다항식 a를 b번 지수승한 결과를 8차식 x^8+x^4+x^3+x+1로 나눈 나머지를 계산한다.
30 * gf8_mul()과 "Square Multiplication" 알고리즘을 사용하여 구현한다.
31 */
32 unsigned char gf8_pow(unsigned char a, unsigned char b)
33 {
34     u_int8_t r = 1;
35
36     while(b > 0){
37         if(b & 1) r = gf8_mul(r, a);
38         a = gf8_mul(a, a);
39         b = b >> 1;
40     }
41     return r;
42 }
```

```

43
44 /*
45 * gf8_inv(a) -  $a^{-1} \bmod x^8+x^4+x^3+x+1$ 
46 *
47 * 모듈러  $x^8+x^4+x^3+x+1$ 에서 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  $a^{-1}$ 를 구하고  $a * a^{-1} = 1$ 인지 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. $a^b \bmod m$ 은($a \bmod m * a \bmod m * \dots * a \bmod m$) $\bmod m$ 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

```
yerim ~Downloads/2020 암호학/프로그래밍 #2/
> cd Downloads/2020 암호학/프로그래밍 #2/
> gcc gf8_skeleton.c
> ./a.out
28 * 7 = 84
127 * 68 = 21
a = 1, a^1 = 1, a^a^1 = 1
a = 2, a^1 = 141, a^a^1 = 1
a = 3, a^1 = 246, a^a^1 = 1
a = 4, a^1 = 203, a^a^1 = 1
a = 5, a^1 = 82, a^a^1 = 1
a = 6, a^1 = 123, a^a^1 = 1
a = 7, a^1 = 209, a^a^1 = 1
a = 8, a^1 = 232, a^a^1 = 1
a = 9, a^1 = 79, a^a^1 = 1
a = 10, a^1 = 41, a^a^1 = 1
a = 11, a^1 = 192, a^a^1 = 1
a = 12, a^1 = 176, a^a^1 = 1
a = 13, a^1 = 225, a^a^1 = 1
a = 14, a^1 = 229, a^a^1 = 1
a = 15, a^1 = 199, a^a^1 = 1
a = 16, a^1 = 116, a^a^1 = 1
a = 17, a^1 = 180, a^a^1 = 1
a = 18, a^1 = 170, a^a^1 = 1
a = 19, a^1 = 75, a^a^1 = 1
a = 20, a^1 = 153, a^a^1 = 1
a = 21, a^1 = 43, a^a^1 = 1
a = 22, a^1 = 96, a^a^1 = 1
a = 23, a^1 = 95, a^a^1 = 1
a = 24, a^1 = 88, a^a^1 = 1
a = 25, a^1 = 63, a^a^1 = 1
a = 26, a^1 = 253, a^a^1 = 1
a = 27, a^1 = 204, a^a^1 = 1
a = 28, a^1 = 255, a^a^1 = 1
a = 29, a^1 = 64, a^a^1 = 1
a = 30, a^1 = 238, a^a^1 = 1
a = 31, a^1 = 178, a^a^1 = 1
a = 32, a^1 = 58, a^a^1 = 1
a = 33, a^1 = 110, a^a^1 = 1
a = 34, a^1 = 90, a^a^1 = 1
a = 35, a^1 = 241, a^a^1 = 1
a = 36, a^1 = 85, a^a^1 = 1
a = 37, a^1 = 77, a^a^1 = 1
a = 38, a^1 = 168, a^a^1 = 1
a = 39, a^1 = 201, a^a^1 = 1
a = 40, a^1 = 193, a^a^1 = 1
a = 41, a^1 = 10, a^a^1 = 1
a = 42, a^1 = 152, a^a^1 = 1
a = 43, a^1 = 21, a^a^1 = 1
a = 44, a^1 = 48, a^a^1 = 1
a = 45, a^1 = 68, a^a^1 = 1
a = 46, a^1 = 162, a^a^1 = 1
a = 47, a^1 = 194, a^a^1 = 1
a = 48, a^1 = 44, a^a^1 = 1
a = 49, a^1 = 69, a^a^1 = 1
a = 50, a^1 = 146, a^a^1 = 1
a = 51, a^1 = 108, a^a^1 = 1
a = 52, a^1 = 243, a^a^1 = 1
a = 53, a^1 = 57, a^a^1 = 1
a = 54, a^1 = 102, a^a^1 = 1
a = 55, a^1 = 66, a^a^1 = 1
a = 56, a^1 = 242, a^a^1 = 1
a = 57, a^1 = 53, a^a^1 = 1
a = 58, a^1 = 32, a^a^1 = 1
a = 59, a^1 = 111, a^a^1 = 1
a = 60, a^1 = 119, a^a^1 = 1
a = 61, a^1 = 187, a^a^1 = 1
a = 62, a^1 = 89, a^a^1 = 1
a = 63, a^1 = 25, a^a^1 = 1
a = 64, a^1 = 29, a^a^1 = 1
a = 65, a^1 = 254, a^a^1 = 1
a = 66, a^1 = 55, a^a^1 = 1
a = 67, a^1 = 103, a^a^1 = 1
a = 68, a^1 = 45, a^a^1 = 1
a = 69, a^1 = 49, a^a^1 = 1
a = 70, a^1 = 245, a^a^1 = 1
a = 71, a^1 = 105, a^a^1 = 1
a = 72, a^1 = 167, a^a^1 = 1
a = 73, a^1 = 100, a^a^1 = 1
a = 74, a^1 = 171, a^a^1 = 1
a = 75, a^1 = 19, a^a^1 = 1
a = 76, a^1 = 84, a^a^1 = 1
a = 77, a^1 = 37, a^a^1 = 1
a = 78, a^1 = 233, a^a^1 = 1
a = 79, a^1 = 9, a^a^1 = 1
a = 80, a^1 = 237, a^a^1 = 1
a = 81, a^1 = 92, a^a^1 = 1
a = 82, a^1 = 5, a^a^1 = 1
a = 83, a^1 = 202, a^a^1 = 1
a = 84, a^1 = 76, a^a^1 = 1
a = 85, a^1 = 36, a^a^1 = 1
a = 86, a^1 = 135, a^a^1 = 1
a = 87, a^1 = 191, a^a^1 = 1
a = 88, a^1 = 24, a^a^1 = 1
a = 89, a^1 = 62, a^a^1 = 1
a = 90, a^1 = 34, a^a^1 = 1
a = 91, a^1 = 240, a^a^1 = 1
a = 92, a^1 = 81, a^a^1 = 1
a = 93, a^1 = 236, a^a^1 = 1
a = 94, a^1 = 97, a^a^1 = 1
a = 95, a^1 = 23, a^a^1 = 1
a = 96, a^1 = 22, a^a^1 = 1
a = 97, a^1 = 94, a^a^1 = 1
a = 98, a^1 = 175, a^a^1 = 1
a = 99, a^1 = 211, a^a^1 = 1
a = 100, a^1 = 73, a^a^1 = 1
a = 101, a^1 = 166, a^a^1 = 1
a = 102, a^1 = 54, a^a^1 = 1
a = 103, a^1 = 67, a^a^1 = 1
a = 104, a^1 = 244, a^a^1 = 1
a = 105, a^1 = 71, a^a^1 = 1
a = 106, a^1 = 145, a^a^1 = 1
a = 107, a^1 = 223, a^a^1 = 1
a = 108, a^1 = 51, a^a^1 = 1
a = 109, a^1 = 147, a^a^1 = 1
a = 110, a^1 = 33, a^a^1 = 1
a = 111, a^1 = 59, a^a^1 = 1
a = 112, a^1 = 121, a^a^1 = 1
a = 113, a^1 = 183, a^a^1 = 1
a = 114, a^1 = 151, a^a^1 = 1
a = 115, a^1 = 133, a^a^1 = 1
a = 116, a^1 = 16, a^a^1 = 1
a = 117, a^1 = 181, a^a^1 = 1
a = 118, a^1 = 186, a^a^1 = 1
a = 119, a^1 = 60, a^a^1 = 1
a = 120, a^1 = 182, a^a^1 = 1
a = 121, a^1 = 112, a^a^1 = 1
a = 122, a^1 = 208, a^a^1 = 1
a = 123, a^1 = 6, a^a^1 = 1
a = 124, a^1 = 161, a^a^1 = 1
a = 125, a^1 = 250, a^a^1 = 1
a = 126, a^1 = 129, a^a^1 = 1
a = 127, a^1 = 130, a^a^1 = 1
a = 128, a^1 = 131, a^a^1 = 1
a = 129, a^1 = 126, a^a^1 = 1
a = 130, a^1 = 127, a^a^1 = 1
a = 131, a^1 = 128, a^a^1 = 1
a = 132, a^1 = 150, a^a^1 = 1
a = 133, a^1 = 115, a^a^1 = 1
a = 134, a^1 = 190, a^a^1 = 1
a = 135, a^1 = 86, a^a^1 = 1
a = 136, a^1 = 155, a^a^1 = 1
a = 137, a^1 = 158, a^a^1 = 1
a = 138, a^1 = 149, a^a^1 = 1
a = 139, a^1 = 217, a^a^1 = 1
a = 140, a^1 = 247, a^a^1 = 1
a = 141, a^1 = 2, a^a^1 = 1
a = 142, a^1 = 185, a^a^1 = 1
a = 143, a^1 = 164, a^a^1 = 1
a = 144, a^1 = 222, a^a^1 = 1
a = 145, a^1 = 106, a^a^1 = 1
a = 146, a^1 = 50, a^a^1 = 1
a = 147, a^1 = 109, a^a^1 = 1
a = 148, a^1 = 216, a^a^1 = 1
a = 149, a^1 = 138, a^a^1 = 1
a = 150, a^1 = 132, a^a^1 = 1
a = 151, a^1 = 114, a^a^1 = 1
a = 152, a^1 = 42, a^a^1 = 1
a = 153, a^1 = 20, a^a^1 = 1
a = 154, a^1 = 159, a^a^1 = 1
a = 155, a^1 = 136, a^a^1 = 1
a = 156, a^1 = 249, a^a^1 = 1
a = 157, a^1 = 220, a^a^1 = 1
a = 158, a^1 = 137, a^a^1 = 1
a = 159, a^1 = 154, a^a^1 = 1
a = 160, a^1 = 251, a^a^1 = 1
a = 161, a^1 = 124, a^a^1 = 1
a = 162, a^1 = 46, a^a^1 = 1
a = 163, a^1 = 195, a^a^1 = 1
a = 164, a^1 = 143, a^a^1 = 1
a = 165, a^1 = 184, a^a^1 = 1
a = 166, a^1 = 101, a^a^1 = 1
a = 167, a^1 = 72, a^a^1 = 1
a = 168, a^1 = 38, a^a^1 = 1
a = 169, a^1 = 200, a^a^1 = 1
a = 170, a^1 = 18, a^a^1 = 1
a = 171, a^1 = 74, a^a^1 = 1
a = 172, a^1 = 206, a^a^1 = 1
a = 173, a^1 = 231, a^a^1 = 1
a = 174, a^1 = 210, a^a^1 = 1
a = 175, a^1 = 98, a^a^1 = 1
a = 176, a^1 = 12, a^a^1 = 1
a = 177, a^1 = 224, a^a^1 = 1
a = 178, a^1 = 31, a^a^1 = 1
a = 179, a^1 = 239, a^a^1 = 1
a = 180, a^1 = 17, a^a^1 = 1
a = 181, a^1 = 117, a^a^1 = 1
a = 182, a^1 = 120, a^a^1 = 1
a = 183, a^1 = 113, a^a^1 = 1
a = 184, a^1 = 165, a^a^1 = 1
a = 185, a^1 = 142, a^a^1 = 1
a = 186, a^1 = 118, a^a^1 = 1
a = 187, a^1 = 61, a^a^1 = 1
a = 188, a^1 = 189, a^a^1 = 1
a = 189, a^1 = 188, a^a^1 = 1
a = 190, a^1 = 134, a^a^1 = 1
a = 191, a^1 = 87, a^a^1 = 1
a = 192, a^1 = 11, a^a^1 = 1
a = 193, a^1 = 40, a^a^1 = 1
a = 194, a^1 = 47, a^a^1 = 1
a = 195, a^1 = 163, a^a^1 = 1
a = 196, a^1 = 218, a^a^1 = 1
a = 197, a^1 = 212, a^a^1 = 1
a = 198, a^1 = 228, a^a^1 = 1
a = 199, a^1 = 15, a^a^1 = 1
a = 200, a^1 = 169, a^a^1 = 1
a = 201, a^1 = 39, a^a^1 = 1
a = 202, a^1 = 83, a^a^1 = 1
a = 203, a^1 = 4, a^a^1 = 1
a = 204, a^1 = 27, a^a^1 = 1
a = 205, a^1 = 252, a^a^1 = 1
a = 206, a^1 = 172, a^a^1 = 1
a = 207, a^1 = 230, a^a^1 = 1
a = 208, a^1 = 122, a^a^1 = 1
a = 209, a^1 = 7, a^a^1 = 1
a = 210, a^1 = 174, a^a^1 = 1
a = 211, a^1 = 99, a^a^1 = 1
a = 212, a^1 = 197, a^a^1 = 1
a = 213, a^1 = 219, a^a^1 = 1
a = 214, a^1 = 226, a^a^1 = 1
a = 215, a^1 = 234, a^a^1 = 1
a = 216, a^1 = 148, a^a^1 = 1
a = 217, a^1 = 139, a^a^1 = 1
a = 218, a^1 = 196, a^a^1 = 1
a = 219, a^1 = 213, a^a^1 = 1
a = 220, a^1 = 157, a^a^1 = 1
a = 221, a^1 = 248, a^a^1 = 1
a = 222, a^1 = 144, a^a^1 = 1
a = 223, a^1 = 107, a^a^1 = 1
a = 224, a^1 = 187, a^a^1 = 1
a = 225, a^1 = 13, a^a^1 = 1
a = 226, a^1 = 214, a^a^1 = 1
a = 227, a^1 = 235, a^a^1 = 1
a = 228, a^1 = 198, a^a^1 = 1
a = 229, a^1 = 14, a^a^1 = 1
a = 230, a^1 = 207, a^a^1 = 1
a = 231, a^1 = 73, a^a^1 = 1
a = 232, a^1 = 18, a^a^1 = 1
a = 233, a^1 = 78, a^a^1 = 1
a = 234, a^1 = 215, a^a^1 = 1
a = 235, a^1 = 227, a^a^1 = 1
a = 236, a^1 = 93, a^a^1 = 1
a = 237, a^1 = 80, a^a^1 = 1
a = 238, a^1 = 30, a^a^1 = 1
a = 239, a^1 = 179, a^a^1 = 1
a = 240, a^1 = 91, a^a^1 = 1
a = 241, a^1 = 35, a^a^1 = 1
a = 242, a^1 = 56, a^a^1 = 1
a = 243, a^1 = 52, a^a^1 = 1
a = 244, a^1 = 104, a^a^1 = 1
a = 245, a^1 = 70, a^a^1 = 1
a = 246, a^1 = 3, a^a^1 = 1
a = 247, a^1 = 140, a^a^1 = 1
a = 248, a^1 = 221, a^a^1 = 1
a = 249, a^1 = 156, a^a^1 = 1
a = 250, a^1 = 125, a^a^1 = 1
a = 251, a^1 = 160, a^a^1 = 1
a = 252, a^1 = 205, a^a^1 = 1
a = 253, a^1 = 26, a^a^1 = 1
a = 254, a^1 = 65, a^a^1 = 1
a = 255, a^1 = 28, a^a^1 = 1
No error found
yerim ~Downloads/2020 암호학/프로그래밍 #2/
```