정보보호 과제2

학　　번 : 20164269
이　　름 : 이현호
제 출 일 : 2020.05.12

①키 생성-1

1. 두 개의 큰 소수 p와 q를 선택하고, 이들의 곱 n을 계산합니다. p=29, q=31
   -> n=899
2. φ(n)=(p-1) ×(q-1)을 계산합니다.
   -> φ(n) = 840
3. 1<e<φ(n)를 만족하고 φ(n)과 서로소인 수 e를 선택합니다. e=571
4. d×e mod φ(n) = 1을 만족하는 d를 찾습니다. (조건 : 확장 유클리드 호제법 사용)

840과 571은 서로소이므로 확장 유클리드 호제법에 따라 1 = 840x+571y 형태로 표현할 수 있다.

(1) Euclidean algorithm

840 = 1 × 571 + 269	269 = 840 – 1 × 571
571 = 2 × 269 + 33	33 = 571 - 2 × 269
269 = 8 × 33 + 5	5 = 269 - 8 ×33
33 = 6× 5 + 3	3 = 33 - 6 × 5
5 = 1 × 3 + 2	2 = 5 – 1 × 3
3 = 1 × 2 + 1	1 = 1 × 2

(2) Back substitution

$1 = 3 - 1 \times \underline{2}$
$1 = 3 - 1 \times (5 - 3) = 2 \times \underline{3} - 5$
$1 = 2 \times (33 - 6 \times 5) - 5 = 2 \times 33 - \underline{5} \times 13$
$1 = 2 \times 33 - (269 - 8 \times 33) \times 13 = 106 \times \underline{33} - 269 \times 13$
$1 = 106 \times (571 - 2 \times 269) - 269 \times 13$
$1 = 106 \times 571 - 225 \times \underline{269}$
$1 = 106 \times 571 - 225 \times (840 - 571)$
$1 = 331 \times 571 - 225 \times 840$

$\therefore d = 331$

①키 생성-2

이전 슬라이드의 연산부분을 소스로 구현하기는 까다롭습니다.
따라서 강의자료[4장_정수론의 기본개념-2] 26번 슬라이드의 다음 식을 이용합니다.

$$x_i = x_{i-2} - qx_{i-1}$$
$$y_i = y_{i-2} - qy_{i-1}$$

i	r_i	q_i	x_i	y_i
-1	840		1	0
0	571		0	1
1	269	1	1	-1
2	33	2	-2	3
3	5	8	17	-25
4	3	6	-104	153
5	2	1	121	-178
6	1	1	-225	331

<공개키> n, e -> 899, 571
<개인키> n, d -> 899, 331

②암호화-1

$p=29$
$q=31$
$n=899$
$\varphi(n)=840$
$e=571$
$d=331$

$c = m^e \pmod n$
m=115, e=571 이므로 115^{571} mod899 의 값이 암호문입니다.

115를 571번 곱하는 것은 상당히 비효율적이고,
115를 거듭제곱한 값은 매우 큰 폭으로 증가하기 때문에 치명적으로 연산 중 오버플로우가 발생할 수 있습니다.

구하려고 하는 값이 115^{571}이 아닌 모듈로 값이기 때문에 모듈로 연산의 성질인 다음 식을 사용할 수 있습니다.

$$(A \times B) \bmod C = (A \bmod C \times B \bmod C) \bmod C$$

지수인 571을 이진법으로 바꿔보겠습니다.

$$571 = 1000111011_{(2)}$$

그리고 571을 2의 거듭제곱으로 표현하면 $2^0+2^1+2^3+2^4+2^5+2^9$입니다.

2의 거듭제곱으로 표현한 571을 이용해 위의 식 115^{571} mod899 을 다시 한 번 쓰면

$$115^{571} \bmod 899 = 115^{(1+2+8+16+32+512)} \bmod 899$$

②암호화-2

p=29
q=31
n=899
φ(n)=840
e=571
d=331

①$115^1$ mod 899 = 115
②$115^2$ mod 899 = 639
③$115^8$ mod 899 = 59
④$115^{16}$ mod 899 = 784
⑤$115^{32}$ mod 899 = 639
⑥$115^{512}$ mod 899 = 639

$115^{(1+2+8+16+32+512)}$ mod899
=(115×639×59×784×639×639) mod899
=(115×639) mod899 × (59×784×639×639) mod899
=(666×59) mod899 × (784×639×639) mod899
=(637×784) mod899 × (639×639) mod899
=(463×639) mod899 × 639 mod 899
=(86×639) mod899
=115 (암호화된 데이터)

이 과정에서 $115^{2\wedge k}$ mod899 값을 구하기 위해서는 $115^{2\wedge(k-1)}$ mod899의 값을 알아야 하며,
지수가 2의 거듭제곱이 아닌 수의 모듈로 값은 연산할 필요 없다는 것을 알 수 있습니다.

따라서 모듈로 연산을 하고자 하는 수 m의 지수를
① 2진수로 바꾸어 배열에 저장합니다.
② 최상위 비트가 몇 번째 자리인지 파악하여 $m^{2\wedge k}$ mod n 까지만 계산하여 새로운 배열 mod에 저장합니다.
③ 루프를 돌며 ①에서 저장한 배열의 원소가 1이면 result에 result×mod[i]을 덮어씁니다.

③복호화

$p=29$
$q=31$
$n=899$
$\varphi(n)=840$
$e=571$
$d=331$

$m = c^d \pmod{n}$
$c=115$, $d=331$ 이므로 115^{331} mod899 의 값이 복호문입니다.

5번 슬라이드에서 알아낸 것을 이용해, 분할 정복하여 계산합니다.

$$331 = 101001011_{(2)}$$
$$115^{331} = 115^{(1+2+8+64+256)}$$

①$115^1 \bmod 899 = 115$

②$115^2 \bmod 899 = 639$

③$115^8 \bmod 899 = 59$

④$115^{64} \bmod 899 = 175$

⑤$115^{256} \bmod 899 = 784$

$$(115\times639\times59\times175\times784) \bmod 899$$

①mod 899
②mod 899
③ mod 899
④mod 899

복호문은 115로, 암호화 이전의 데이터와 동일하게 나옵니다.