(1. RSA 소개

RSA 공개키 방식은 실생활에서 가장 많이 사용되고 있는 대표적인 양방향 데이터 암호화 기법이다.

양방향 암호화란? 양방향 알고리즘은 암호화된 암호문을 복호화 할 수 있는 알고리즘을 의미한다. 반대로 단방향 알고리즘은 암호화를 수행하지만 절대로 복호화가 불가능한 알고리즘을 말한다.

양방향 알고리즘 : 암호화, 복호화 가능

단방향 알고리즘 : 암호화 가능, 복호화 불가

(2. RSA 암호 알고리즘이란?

Rivet, Shamir, Adelman 세사람의 첫이름을 따 RSA라고 만든 암호 알고리즘을 보고자 한다.

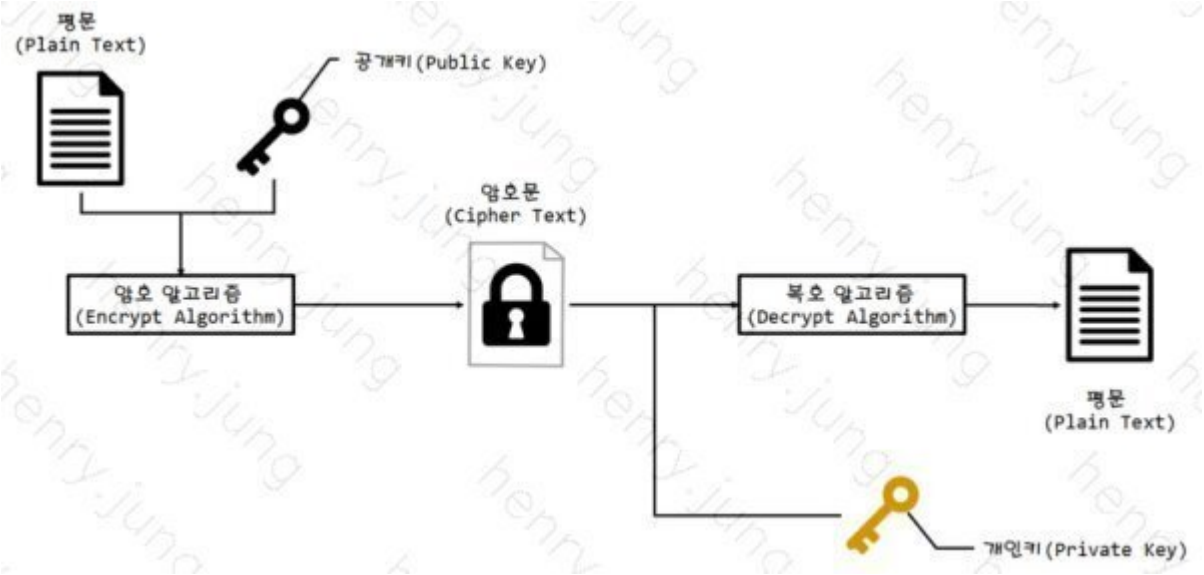
RSA 암호 체계는 미국 MIT에서 개발한 공개키 암호 시스템이다.

이 암호 알고리즘의 핵심은 큰 정수의 소인수 분해가 어렵다는 점을 이용하여 암호화를 시킨다.

이러한 RSA 암호 알고리즘은 전자상거래에서 가장 흔히 쓰고있는 공개키 알고리즘이다.

(3. RSA 암호 알고리즘 방식

1. A가 B에게 정보를 안전하게 보내고 싶어한다. 이때 RSA 알고리즘을 이용하고자 한다.
2. B가 공개키와 개인키를 만들어 A에게 공개키를 보낸다. (개인키는 B만 가지고 있다.)
3. A가 B로부터 받은 공개키를 이용하여 보낼 정보를 암호화한다.
4. A가 암호화된 정보를 B에게 보낸다. 5. B가 암호화된 정보를 받고 개인키를 이용하여 암호를 해독한다.



(4. RSA 암호 알고리즘 원리

1. 개인키와 공개키 만들기

RSA 암호 알고리즘 첫 단계는 공개키와 개인키를 만드는 것이다. 공개키는 n,e라는 두 정수로 이루어져있고 개인기는 n,d라는 두 정수를 이루어져있다.

n 구하기: 임의의 두 소수 p와 q를 정하고 n=p*q를 해주면 n을 구할 수 있다.

e 구하기: Φ(n) = (p - 1) * (q - 1)식을 이용하여 Φ(n)을 구한다. e는 1 < e < Φ(n)로써 1과 Φ(n) 사이에 있고 Φ(n)와 서로소인 e를 정해주면 된다. 이러한 e는 공개키에 이용이 될 것이다. 서로소란 1 이외에 공약수를 가지지 않는 수를 의미한다.

Φ이란? 그리스어 문자이다.

용도는 자속(물리학), 전속 (자기장 선속, 물리학), 상대습도에 대한 기호 (기상), 누적 정규 분포 함수(통계학)으로 사용한다.

모듈로 연산이란? 어떠 한 숫자를 다른 숫자로 나눈 나머지를 구하는 연산이므로, 나머지 연산(mod)이라고 한다

d 구하기: (e * d) mod Φ(n) = 1 즉, e*d를 Φ(n)으로 나누었을 때 나머지가 1인 d를 구하면 된다. 이때 d는 개인키에 사용될 숫자이다. 이제 공개키에 이용될 (n, e)와 개인키에 이용될 (n, d)를 모두 구하였다. 즉, 개인키와 공개키가 생성되었다.

2. 암호화하기

위에서 구한 공개키를 이용해 정보를 암호화 한다.

원래 정보를 M이라 하고 암호화된 정보를 C라 하자

$$C = M^e \mod n$$

위의 식을 이용하여 M을 C로 암호화 하면 된다. 이때 암호화를 할 때 e와 n의 값을 알아야 하므로 공개키(n, e)가 있어야 암호화 할 수 있다는 것은 자명하다.

3. 복호화하기(해독하기)

이제 암호화되어 온 정도 C를 복호화(해독)할 순서이다.

1) $C = M^e \mod n$

2) $M = C^d \mod n$

페르마의 소정리에 의해 1번식이 성립하면 2번식도 성립하게 된다.

$$M = C^d \mod n$$

암호화 할때는 1번식을 사용했으므로 복호화 할때는 위의 식 즉, 2번식을 이용하여 복호화를 한다. 이때 암호화된 정보 C를 M으로 복호화(해독)할 때는 n과 d값을 알아야 한다. 이때 이 값을 아는 사람은 개인키(n, d)를 가진 사람 B 뿐이다.

암호화 방법(식을 대입해서 설명)

1. 임의의 두 소수 p=31 q=47 n=pq=1457

2. e(공개키)구하기 : Φ(n) =(31-1)(47-1)=1380 이다

3. e는 1<e< Φ(n)=(1380) : 1과 Φ(n)사이에 있고 Φ(n)와 서로소인 e는 19

4. d(개인키)구하기: (19*d)나누기 Φ(n)=1 d=73

여기서 n=1457과 e=19은 공개키가 되고, d=73는 비밀키가 된다

만약, m=100를 암호화하기 위해서는 다음과 같이 계산한다.

c=(100^19)=280 (mod 1457)

이렇게 하여 암호화 된 c=280는 비밀키인 d=73을 통해 해독할 수 있다.

m=280^72=100 (mod 1457)

복호화 해독 방법(식을 대입해서 설명)

1. c(280) = m(100)^e(19) mod (1457)
2. m(100) = c(280)^d(72) mod (1457)

페르마의 소정리에 의해 1번식이 성립하면 2번식도 성립하게 된다.

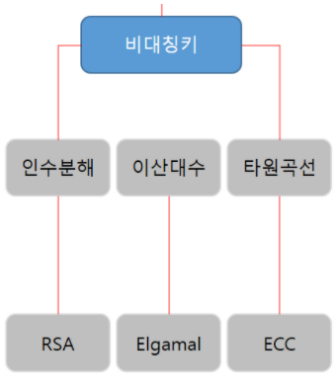
m(100) = c(280)^d(72) mod (1457)

암호화 할때는 1번식을 사용했으므로 복호화 할때는 위의 식 즉, 2번식을 이용하여 복호화를 한다. 이때 암호화된 정보 C를 M으로 복호화(해독)할 때는 n과 d값을 알아야 한다. 이때 이 값을 아는 사람은 개인키(n, d)를 가진 사람 B 뿐이다.

페르마의 소정리: 어떤 수가 소수일 간단한 필요 조건에 대한 정리이다.

비대칭키 암호화의 원리 (공개키 암호화) : 암호화/복호화 키가 서로 다른 암호화 방식

- 대칭키 암호화의 키 교환 문제에 대한 해결책
- 공개키 : 누구나 가질 수 있는 키로, 암호화에 사용
- 개인키 : 개인만이 가지고 있고, 외부에 알려지지 않아 복호화에 사용



*RSA : 큰 소인수의 곱은 인수분해가 어렵다는 원리를 이용

- 주로 무선환경에서 적은 비트로 암호화 할 때 사용

* ECC : 타원 곡선 기반의 구조체 안정/효율의 원리를 이용

- 주로 무선환경에서 적은 비트로 암호화 할 때 사용