2. RSA 공개키 암호 시스템의 구현

응용수학과 김 금 철
지도교수 배 재 국

인터넷으로 대표되는 정보화 사회에서 최근 정보의 보안에 관련한 문제는 무엇보다 중요하게 대두되고 있다. 약 4000 년 전 암호라는 개념이 처음 사용된 이래 제2차 세계대전을 거치면서 암호학은 급속도로 발전하기 시작하였는데 최근에는 보다 높은 안전성을 위하여 그 근거로 수학적인 개념을 도입한 시스템이 주류를 이루고 있는 실정이다. 현재 가장 많이 쓰이는 암호 시스템으로는 대칭키(symmetric-key) 암호 시스템과 공개키(public-key) 암호 시스템이 있다. 본 논문에서는 전송하고자 하는 메시지 M을 대칭키 암호 기법을 이용해 M'로 암호화하는 방법을 사용하였다. 그러나 대칭키 암호 시스템은 수행속도는 빠른 반변 대규모의 네트워크상에서 키 관리의 어려움과 공개키에 비해 안전성이 떨어진다는 단점이 있다. 이에 비해 공개키 암호 시스템은 키 관리가 효율적이고 안전성이 높은 편이지만 그 키의 사이즈가 너무 커서 수행속도가 현저하게 떨어진다. 이를 극복하기 위해 메시지를 암호화하는데 필요한 비밀키는 공개키 암호 기법을 이용해서 암호화시키고 암호화 된 메시지와 함께 전송하는 방법을 구현하였다.

본 논문에서 구현한 암호 알고리즘을 살펴보면 우선 대칭키 암호 시스템의 일종인 호환암호가 있는데 이는

$$e=\{1,2,3,\cdots,k\}\rightarrow\{1,2,3,\cdots,k\}$$

인 random permutation을 생성하고 이를 이용하여 메시지 M의 각 문자들의 위치를 바꾸는 방법이다. 여기서는 $k=128$로 잡았기 때문에 permutation e를 생성할 수 있는 방법의 가지수는 $128!$이다. 다라서 공격자가 e를 알아낼 수 있는 확률은 $\frac{1}{128!}$이다.

다음은 위에서 생성된 random permutation e를 공개키 암호 알고리즘을 이용해 암호화 시켜야 하는데 여기서 사용된 알고리즘은 RSA 공개키 암호 알고리즘이다. RSA는 1978년 개발된 이래 현재 가장 많이 쓰이고 있는 암호 알고리즘인데 장시간의 안전성을 위해서는 변수의 사이즈가 1024비트 이상은 되어야 한다. 즉, 1024비트의 random 소수 p와 q를 생생하고 $n=pq$를 계산한 다음 이를 이용해 개인키 d를 구하여야 하는데 큰 사이즈의 변수를 사용하기 위해 ntl이라는 헤더파일을 사용하였다. 또한 random 소수를 생성하는 방법은 임의의 random 정수를 생성하여 이것이 소수인지를 검증하는 방법을 사용하였는데 다음의 두 가지 방법을 사용하였다.

먼저 확률적 소수 검증인 Miller-Rabin의 소수 검증을 t번 통과한 수를 후보소수로 명명하였다. Miller-Rabin 검증을 t번 통과한 임의의 합성수 n에 대하여 n이 소수라고 판정할 확률은 $\left(\frac{1}{4^t}\right)$ 보다 작다는 것이 알려져 있으므로 t를 충분히 크게 한다면 소수의 성질에 가까운 수를 생성할 수가 있다. 그러나 이를 확실한 소수라고는 말할 수 없으므로 다시 True primality test를 이용해 정확한 소수를 생성할 수 있다. 이와 같은 과정을 통해 생성된 두 소수 p와 q의 곱인

$$n=pq\text{와}\quad \varnothing=(p-1)(q-1)$$

을 구하고

$$\gcd(e, \varnothing) = 1$$

을 만족하는 $1 < e < \varnothing$에서의 random 정수를 계산한다. 마지막으로

$$ed \equiv 1 \pmod{\varnothing}$$

를 만족하는 $1 < d < \varnothing$에서의 유일한 정수 d를 구해서 (n, e)는 공개키로 하고 d는 개인키로 사용한다.

다음은 암호화 과정인데 먼저 공개키 (n, e)를 획득하고 대칭키에서의 비밀키인 permutation e를 구간 $[0, n-1]$에서의 정수 m으로 표현하고

$$c = m^e \pmod{n}$$

이 암호화된 메시지가 된다. 따라서 entity A가 암호화한 (M', c)를 entity B에게 보내게 되고 B는 자신의 개인키 d를 이용하여

$$m = c^d \pmod{n}$$

을 계산함으로써 c에 대응되는 m을 구하고 m^{-1}에 의해 M'에 대응하는 M을 구할 수 있다.

RSA 암호 시스템의 안전성은 큰 정수의 소인수분해가 어렵다는 것에 그 근거를 두고 있다. 공격자의 목적은 공개된 정보 (n, e)를 이용해서 개인키 d를 구하는 것이다. 이 문제를 RSA 문제라고 하는데 공격자가 RSA 문제를 해결할 수 있는 방법은 n을 소인수분해 해서 $\varnothing$와 d를 구하는 것이다. 일단 d가 구해지면 공격자는 암호문 c를 복호화 할 수 있다. 따라서 공개키 (n, e)로부터 비밀키 d를 구하는 문제는 n을 소인수분해 하는 문제와 계산적으로 같다는 것을 알 수 있다.

다른 방법으로 공격자가 $n = pq$와 $\varnothing$를 알고 있다면 다음의 두 방정식에 의해 쉽게 n을 소인수분해 할 수 있다. 미지수 p, q에 대해

$$n = pq, \quad \varnothing = (p-1)(q-1)$$

두 번째 식에 $q = \frac{n}{p}$을 대입함으로써 다음과 같은 미지수 p에 대한 이차방정식을 얻는다.

$$p^2 - (n - \varnothing + 1)p + n = 0$$

이 방정식의 근은 p와 q일 것이다. 따라서 공격자는 $\varnothing$를 알 수 있게 되고 그 경우 이 암호계는 깨지게 된다. 하지만 $\varnothing$를 안다는 것은 n을 소인수분해 하는 문제와 같으므로 이 작업 또한 쉽지가 않다.

3. 지수분포하에서의 베이즈 추정치

응용수학과 김 지 환
지도교수 박 춘 일

This thesis is to compare and analyze the error among the Bayes estimators, GMLE of the