키 생성 알고리즘의 안전성 요구사항에 관한 연구

송기언*, 조은성*, 주미리**, 양형규***, 원동호*

*성균관대학교, 컴퓨터공학과

**국가보안기술연구소

***강남대학교 컴퓨터공학과

Study on Requirements of Key Generation Algorithms

Kieon Song*, Eunsung Cho*, Miri Ju**, Hyungkyu Yang***, Dongho Won*

*Department of Computer Engineering Sungkyunkwan Univ.

**National Security research Institute.

***School of Computer Media Engineering, Kangnam Univ.

요 약

암호 시스템의 안전성 및 신뢰성은 키의 안전성에 기반을 두기 때문에, 암호 시스템의 설계 및 구현 시 키를 안전하게 생성하는 것은 매우 중요한 일이다. 키 생성은 암호학적인 안전성을 만족하는 키를 생성하는 절차를 의미하며, 키를 생성하기 위해서는 지금까지 알려진 여러 가지 공격 방법들에 대한 안전성을 확보할 수 있는 파라미터를 사용해야 한다. 본 논문에서는 암호 시스템의 설계 및 구현 시 공개키 암호방식의 키 생성 단계에서 이산대수 문제와 소인수분해 문제를 푸는 알고리즘들을 이용한 공격으로부터 안전성을 갖기 위한 요구사항을 분석한다. 또한 이러한 결과를 바탕으로 키 생성 단계의 안전성 확보를 위한 요구사항 명세서를 작성한다.

I. 서론

인터넷이라는 개방형 네트워크 상에서 전송되는 디지털 정보들을 안전하게 보호하기 위해 암호기술의 중요성이 부각되고 있으며, 이에 따라 많은 암호 시스템이 개발되고 있다. 이러한 암호 시스템들의 안전성의 가장 중요한 요구사항으로 안전한 키 관리가 요구되고 있다. 키 관리는 인가된 객체들 사이에 공통의 키 정보를 유지하는 관계를 설정하고 지속시키는 모든 절차를 포함한다. 즉, 키 관리는 크게 키 생성, 키 분배, 키 저장, 키 폐기, 키 복구로 구성된다. 이중 키 생성은 암호 시스템의 안전성에 큰 영향을 미치는 키 관리 구성요소이기 때문에 암호 시스템의 설계 및 구현 시 선택한 키 생성 알고리즘의 안전성에 대한 분석이 이루어 져야 한다. 따라서 키 생성 알고리즘 선택을 위한 안전성 요구사항이 필요하다.

본 논문에서는 암호 시스템의 설계 및 구현 시 공개키 암호 방식의 키 생성 단계에서 사용하는 알고리즘들이 이산대수 문제와 소인수분해 문제를 푸는 알고리즘들을 이용한 공격으로부터 안전성을 갖기 위한 요구사항을 분석하고, 이를 바탕으로 요구사항 명세서를 작성한다. 본 논문의 구성은 다음과 같다. 2장에서는 이산대수 문제와 소인수분해 문제를 푸는 알고리즘에 대해 살펴보고, 3장에서 키 생성 알고리즘의 안전성 요구사항에 대해 분석하고 안전성 요구사항 명세서를 작성한다. 마지막으로 4장에서는 결론을 맺는다.

II. 관련연구

키 생성의 안전성 요구사항을 도출하기 위해서는 우선 공개키 암호 시스템의 기반이 되는 이산

대수 문제와 소인수분해 문제를 푸는 알고리즘을 대한 연구가 필요하다. 본 절에서는 이산대수 문제와 소인수분해 문제를 푸는 알고리즘을 이용한 공격 방법에 대하여 알아본다.

1. 이산대수 문제

다음 알고리즘들은 $\beta=g^x \pmod p$의 이산대수 x를 구하는 알고리즘이다.

1) Exhaustive search Algorithm

■ 공격방법 : 위수가 $p-1$인 순환그룹 G의 원시원소 g와 원소 β를 가지며, $\beta=g^x \pmod p$의 이산대수 x를 구하기 위해서 g^0, g^1, $g^2,\ldots$를 순차적으로 계산하여 만족하는 x값을 찾는 방식이다.[1]

2) Baby-step/giant-step Algorithm

■ 공격방법 : 위수가 $p-1$인 순환그룹 G의 원시원소 g와 원소 β을 가지고 $0\le j<|\sqrt{p-1}|$의 범위에서 $\alpha^j \bmod p\ (0\le j<m)$를 계산한 표를 만들고 α^{-m}을 계산한다. $\alpha^j=\beta$가 되는 j가 존재할 때까지 $\beta=\beta\cdot\alpha^{-m}$를 반복하고 $\alpha^j=\beta$를 만족할 때 $x=i\cdot m+j$로 이산대수 값 x를 구하는 공격방법이다.[2]

3) Pollard's lambda Algorithm

■ 공격방법 : x가 $b<x<b+w$ 범위 안에 있다는 것을 알고있다고 가정할 때 가능한 공격방법이다. $\beta_0'=g^{b+w}, \beta_0=\beta$인 순열 T : $\beta_0', \beta_1', \beta_2', \ldots, \beta_N'$와 $W: \beta_0, \beta_1, \ldots, \beta_M$, 를 만들어 다음 식을 만족하는 d_M, d_N에 대해 $d_M>w+d_N'$일 때까지 수열을 검사하여 $\beta_M=\beta_N'$일 때 x값 계산한다.[3]

$$\log_g(B_N')=\log_g(\beta_0')+d_N'$$

$$\log_g(B_M)=\log_g(\beta_0)+d_M$$

$$d_N'=\sum_{i=0}^{N-1} f(\beta_i') \bmod p-1$$

$$d_M=\sum_{i=0}^{M-1} f(\beta_i) \bmod p-1$$

4) Pohlig-Hellman Algorithm

■ 공격방법 : 위수가 $p-1$인 순환그룹 G의 원시원소 g와 원소 β에 대해, $p-1$의 소인수 $n: n=p_1^{e_1}, p_2^{e_2}, \ldots\ldots p_r^{e_r}$를 찾아 위수의 크기를 $(p-1)/q_i$로 낮추어 이산대수 값을 구한 후 중국인의 나머지 정리를 이용하여 전체 그룹에서의 이산대수를 계산하는 방법이다.[4]

5) Index-calculus Algorithm

■ 공격방법 : factor base S 선택(S의 원소들의 곱으로 G안의 모든 원소를 효율적으로 표현할 수 있는 성질을 갖는 G의 부분집합 $S=\{p_1,p_2,\cdots,p_t\}$를 선택)하여 S의 원소들의 이산대수를 포함하는 선형 관계식을 만들어 푼다. $0\le k\le p-1$에서 랜덤수 k를 선택하고 $\beta\cdot g^k$을 S의 원소들의 곱으로 표현하여 아래 식을 계산한다. $\log_g\beta\equiv(\sum_{i=1}^{t}d_i\cdot\log_g p_i-k) \bmod p-1$을 계산하여 이산대수 값을 구한다.[5]

2. 소인수분해 문제

다음 알고리즘들은 합성수 n을 소인수분해 하는 알고리즘이다.

1) Pollard's rho factoring algorithm

■ 공격방법 : $n=pq$일 때, $x_0=2, x_{i+1}=f(x_i)=x_i^2+1$로 정의된 x_o, x_1, x_2, ... x_i 중에서 $x_i=x_j \bmod \mathrm{p}$을 만족하면, $\gcd(x_i-x_j, n)=d$를 만족하는 d를 찾는다.[6]

2) Fermat algorithm

■ 공격방법 : 입력으로 양의 정수 n을 받아서 완전 제곱수이면 끝내고, 완전 제곱수가 아니라면 $t=[\sqrt{kn}]+1$를 계산하고 $z=t^2-kn$를 계산한다. z가 완전 제곱수이면 $n=t^2-s^2$이므로 끝내고 아니면 $t=t+1$로 놓고 다시 z값을 계산한다.[1]

3) Pollard's $p-1$ algorithm

■ 공격방법 : smoothness bound B를 선택하고 $0\le a\le n-1$인 a를 랜덤하게 선택한다. $a=a^j \bmod n$를 $j=2$부터 B까지 수행한 후, $d=\gcd(a-1, n)$와 $1<d<n$를 만족하는 d를 찾는다.[7]

III. 키 생성 알고리즘 안전성 요구사항

안전하지 못한 키의 사용으로 인해 암호 시스템의 안전성에 손상을 야기할 수 있다. 그러므로 키 생성은 암호 시스템의 안전성에 가장 큰 영향을 미치는 중요한 요소이다. 따라서 암호 시스템을 설계 및 구현 시 키 생성에서 수행될 알고리즘을

선택은 매우 중요한 일이다. 키 생성 알고리즘의 선택하기 전에 수행되어야 할 작업은 키 생성 과정에서 가능한 공격 방법들에 대한 연구와 이러한 공격방법들의 공격을 위한 조건들을 분석하여 대응 방안에 대한 분석이 필요하다. 본 절에서는 공개키 암호 방식의 공개키, 개인키 쌍 생성의 안전성 기반인 이산대수 문제와 소인수분해 문제를 푸는 알고리즘에 대한 분석을 통해 그 대응 방안에 대해 기술한다. 또한 이산대수 문제와 소인수분해 문제를 푸는 알고리즘에 대한 대응 방안을 바탕으로 공개키 암호 방식의 키 생성 알고리즘의 안전성 요구사항 명세서를 작성한다.

1. 유한체 상에서의 이산대수 문제

1) Exhaustive search Algorithm

■ 대응방안 : 원시원소 g의 위수가 $p-1$이므로 $O(p-1)$번의 알고리즘 수행이 필요하다. 따라서 $p-1$의 크기가 알고리즘 수행의 어려움에 영향을 미친다.

■ 대응방안 : Subgroup에서도 Field order의 경우와 마찬가지로 원시원소 g'의 위수가 $q-1$이므로 $O(q-1)$번의 알고리즘 수행이 필요하다. 따라서 Subgroup의 원시원소 g'의 위수 $q-1$의 크기가 알고리즘 수행의 어려움에 영향을 미친다.

2) Baby-step/giant-step Algorithm

■ 대응방안 : 원시원소 g의 위수가 $p-1$이므로 위 알고리즘을 수행하기 위해 테이블을 만드는 경우 $O(\sqrt{p-1})$의 연산 수행이 필요하고, 값의 정렬을 위해선 $O(\sqrt{p-1}\log p-1)$의 비교가 필요하다. 또한 $\beta=\beta\cdot\alpha^{-m}$연산과 비교 수행이 $O(\sqrt{p-1})$번 이루어지므로, $p-1$의 크기가 알고리즘 수행의 어려움에 영향을 미친다.

■ 대응방안 : Subgroup에서도 Field order의 경우와 마찬가지로 g의 위수가 $q-1$일 경우 $O(\sqrt{q-1})$번의 알고리즘 수행이 필요하고, 값의 정렬을 위해선 $O(\sqrt{q-1}\log q-1)$의 비교가 필요하므로 $q-1$의 크기가 큰 경우에는 비효율적인 알고리즘이므로 q의 크기가 알고리즘 수행의 어려움에 영향을 미친다.

3) Pollard's lambda Algorithm

■ 대응방안 : 위 알고리즘은 공격자가 가능한 이산대수 값의 범위를 알 경우 수행되는 알고리즘이므로 이산대수 값의 범위가 노출되지 않게 해야 한다.

4) Pohlig-Hellman Algorithm

■ 대응방안 : 위 알고리즘은 원시원소 g의 위수를 작은 소수 q_i로 낮추어 각각에 대해 이산대수 값 ($\bmod q_i$)을 구하는 것이다. 따라서 원시원소 g의 위수가 적당한 크기의 소수들로 이루어진 경우에는 소수 q_i를 찾기 어렵기 때문에 알고리즘의 수행 또한 어려워진다.

5) Index-calculus Algorithm

■ 대응방안 : 알고리즘은 이산대수 값을 계산하기 위해서 가장먼저 factor base S를 구성해야 하는데, 이러한 공격에 안전하기 위해선 factor base S 계산 차제가 어려워야 한다. 즉, 그룹의 원소들이 factor base를 이루는 것을 방지해야 한다. 또한 이 알고리즘의 수행시간은 $O(\exp((c=o(1)(\log p)^{1/2}(\log\log p)^{1/2})$이므로 p의 크기 또한 알고리즘 수행의 어려움에 영향을 미친다.

2. 유한체 상에서의 소인수분해 문제

1) Pollard's rho factoring Algorithm

■ 대응방안 : p, q의 크기가 충분히 큰 경우, d를 계산하기가 힘들다.

2) Fermat Algorithm

■ 대응방안 : Fermat 알고리즘은 $n=pq$일 때 p와 q가 일정 크기 이하의 비슷한 크기의 수일 경우에 사용되므로, p와 q를 일정 크기 이상으로 선택했을 때 위 알고리즘을 이용한 공격으로부터 안전하다.

3) Pollard's $p-1$ Algorithm

■ 대응방안 : Pollard's $p-1$ 알고리즘은 n의 인수 p에 대해 $p-1$의 모든 소수가 일정크기 이상일 때 위 알고리즘 사용한 공격에 안전하다.

3. 요구사항 명세서

표 1은 앞에서 분석한 이산대수와 소인수분해 문제를 푸는 알고리즘들에 대한 대응 방안을 바탕으로 작성한 키 생성 알고리즘의 요구사항 명세서를 정리한 것이다. 필수 항목은 암호 시스템의 안전성을 위해서 반듯이 고려해야 할 사항이며 선택 항목은 암호 시스템의 사용 환경이나 목적에 따라서 적용 가능한 사항이다. 표 1에 나타난 안전성 요구사항은 암호시스템의 안전성에 기반이 되는 사항으로 반드시 고려해야 하는 필수 사항이 된다. 요구사항 명세서의 안전성 요구사항에 따라

표 1: 키 생성을 위한 안전성 요구사항 명세서

공격 알고리즘		안전성 요구사항	필수	선택
이산대수 문제 기반	Exhaustive search Algorithm Baby-step/giant-step Algorithm	서브 그룹의 위수는 일정 크기 이상	√	
		그룹의 위수는 일정크기 이상	√	
	Pollard's lambda Algorithm	그룹의 위수가 노출되지 않아야 함	√	
		이산대수 값의 범위가 노출되지 않아야 함	√	
	Pohlig-Hellman Algorithm	그룹의 위수가 smooth 그룹이되지 않아야 함	√	
		그룹의 위수가 최소한 하나이상의 큰 소수를 인수로 포함해야 함	√	
	Index-calculus Algorithm	그룹의 원소들이 factor base를 이루는 것을 방지	√	
소인수분해 문제 기반	Fermat algorithm	n=pq일 때 p와 q가 일정 크기 이상	√	
	Pollard's rho algorithm	n의 인수 p에 대해 p-1의 모든 소인수가 일정 크기 이상	√	

생성 알고리즘을 선택하고 설계하여 암호 시스템의 안전성을 향상시킬 수 있다.

III. 결론

암호 시스템의 안전성 및 신뢰성은 키의 안전성에 기반을 두기 때문에, 암호 시스템의 설계 및 구현 시 키를 안전하게 생성하는 것은 매우 중요한 일이다. 따라서 키 생성 알고리즘의 선택과 구현 시 알고리즘에 대한 안전성 분석이 필요하다. 본 논문에서는 암호 시스템의 설계 및 구현에서 공개키 암호방식의 키 생성 단계가 이산대수 문제와 소인수분해 문제를 푸는 알고리즘들을 이용한 공격으로부터 안전성을 갖기 위한 요구사항을 분석하였다. 또한 이러한 결과를 토대로 키 생성 단계의 안전성 확보를 위한 요구사항 명세서를 작성하였다. 본 논문의 안전성 요구사항을 세부적인 환경에 적용하기 위해 실재로 다양한 시스템 환경에서의 구체적인 연구가 필요하다. 또한 암호 시스템에서 안전한 키 관리를 위해서는 암호 시스템을 설계하기 전에 각 키 관리 구성요소별 공격 알고리즘 및 방법들에 대한 분석과 그 대응 방안에 대한 연구가 필요하며 대응 방안을 토대로 설계 시 고려해야 할 사항을 명시한 안전성 요구사항 명세서가 필요하다. 따라서 추후 키 관리의 전체 구성요소에 관한 안전성 요구사항에 대한 연구가 이루어져야 할 것이다.

참고문헌

[1] Alfred J.Menezes, Paul C.van Oorschot, Scott A.Vanstone, " Handbook of Applied Cryptography", 1996.10

[2] R. Heiman, "A note on discrete logarithm with special structure", In Advances in Cryptology-EUROCRYPT'92, LNCS 658, pp.437-448, 1993.

[3] J.M. Pollard, "Monte Carlo method for index computation (mod p)", Mathematics of Computation, 32, pp.918-924, 1978.

[4] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", IEEE Trans. Inform. Theory, IT-24(1), 1978, pp.106-110

[5] McCurely, "The discrete logarithm problem", C. Pomerance, editor, Cryptology and Computational Number Thoery, volume 42 of Proceeding of Symposia in Applied Mathematics, pp.49-74, American Mathematical society, 1990.

[6] Pollard, J. M. "A Monte Carlo Method for Factorization.". BIT, 15, pp.331-334, 1975.

[7] J.M.Pollard, "Theorems on factorization and primality testing", Proceedings of the Cambridge Philosophical Society, 76, pp.521-528, 1974