creative commons

COMMONS DEED

저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer

dCollection

[UCI]I804:24011-200000240203

2010년 6월
교육학석사(수학교육)학위논문

암호학에 관한 고찰

조선대학교 교육대학원

수학교육전공

김 경 아

암호학에 관한 고찰

A Study of Cryptology

2010년 6월

조선대학교 교육대학원

수학교육전공

김 경 아

암호학에 관한 고찰

지도교수 박 순 철

이 논문을 교육학석사(수학교육)학위 청구논문으로 제출함.

2010년 6월

조선대학교 교육대학원

수학교육전공

김 경 아

김경아의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 김 남 길 인

심사위원 조선대학교 교수 이 관 규 인

심사위원 조선대학교 교수 박 순 철 인

2010년 6월

조선대학교 교육대학원

목 차

ABSTRACT

Ⅰ. 서 론 ---------- 1

Ⅱ. 본 론 ---------- 3

1. 암호의 이해 ---------- 3

(1) 암호와 암호학 ---------- 3

(2) 암호용어 정리 ---------- 4

(3) 암호의 분류 ---------- 6

2. RSA암호 ---------- 8

(1) RSA암호가 나오게 된 배경 ---------- 8

(2) RSA암호 방식 ---------- 10

(3) RSA암호의 활용 ---------- 28

Ⅲ. 결 론 ---------- 31

◉ 참 고 문 헌 ---------- 32

ABSTRACT

A Study of Cryptology

Kim Kyoung-ah

Advisor : Prof. Park Soon-cheol Ph.D.
Major in Mathematics Education
Graduate School of Education, Chosun University

We purchase items at internet shopping mall, transfer money by using internet banking, and trade stocks at cyber stock exchange. Meanwhile, personal information come and go through the internet although it is very crucial and fatal when it is exposed. That is the reason why we need cryptograph which enable us to secure personal information from danger.

Therefore development of cryptographic ciphers is a very important in this internet-enabled society. But this is impossible without mathematics indeed. This paper reviews RSA cipher through concrete examples. RSA cipher, a representative public key cipher, is based on numbertheory.

Ⅰ. 서 론

암호는 더 이상 특정인들만 사용하는 특수문자가 아니다. 정보 노출이 두려운 현대사회에서 사람들은 일상에서 자신도 모르는 사이에 수십 개의 암호를 사용하고 있다.

“내가 암호를 사용하고 있다고?”라고 반문하는 사람들이 있을지도 모른다.

자신이 기억하고 있는 웹사이트의 비밀번호나 다른 사람들이 알아보지 못하도록 다이어리에 대충 흘겨 쓴 글씨나 기호들, 혹은 휴대폰 문지메세지의 이모티콘이나 줄여서 사용하는 신세대의 용어들, 연인들끼리 서로를 부르는 둘만의 비밀 호칭 등등. 다른 사람이 몰래 훔쳐봤지만, 암호의 규칙이나 기호들 간의 연관성을 모르면 절대 알아채지 못하는 것, 그 모든 것이 바로 ‘암호’다[2].

특히, 인터넷 쇼핑이나 사이버 증권거래소에서 주식을 거래하면서 우리의 정보는 인터넷 정보망에 돌아다니게 된다. 남들에게 노출되면 심각한 피해를 미칠 수 있는 정보도 인터넷에 돌아다니는 것이다. 그래서 자신의 중요한 정보를 보호할 수 있는 암호화가 필요하고 그것이 인터넷의 생활화와 함께 그 중요성이 점점 더 커지고 있다.

이처럼 암호는 우리의 생활과 밀접한 연관이 있다. 그런데 이 암호는 수학을 빼놓고는 얘기 할 수가 없다. 수학은 암호의 이론적 토양을 제공할 뿐만 아니라 다양한 암호체계를 만들고 이렇게 만들어진 암호체계의 효용성과 안전성을 분석하는 암호기술의 핵심적인 도구 역할을 담당하고 있다.

이처럼 수학의 실용성과 중요성은 실생활에 밀접한 암호를 통해서도 알 수 있다.

본 논문에서는 먼저 암호의 이해를 돕고자 암호와 암호학이 무엇인지 그리고 암호용어에 대해 간단히 정리를 하고 암호의 분류를 대략적으로 살펴볼 것이다. 그리고 RSA암호를 중심으로 RSA암호 방식, RSA 암호 해독과 공격, RSA안정성, RSA암호의 이론적 배경에 대해 살펴보고 간단한 암호화와 복호화를 하는 과정을

쉽게 이해 할 수 있도록 간단하고 쉬운 예들을 간단히 소개하고자 한다. 또한 RSA 암호의 활용의 예인 전자서명에 대해서도 알아보고자 한다.

이를 통해 암호의 실용성과 중요성을 강조함으로써 암호의 이론적 토양이요 암호 기술의 핵심적인 도구 역할을 감당하는 수학의 실용성과 중요성을 강조하고자 한다.

Ⅱ. 본　　론

1. 암호의 이해

(1) 암호와 암호학

암호(暗號, cryptograph, cipher)란 보통의 기호나 문자처럼 그 의미를 바로 알 수 없는 기호나 문자열들의 나열을 말한다. 한자에서도 알 수 있듯이 暗(암)은 “어둡게 한다”는 의미이다. 즉, 무언가를 어둡게 해서 감춘다는 의미이다. 그리고 cryptograph(암호)는 그리스어로 [숨은, 숨겨진, 비밀]이라는 뜻의 crypt와 [문자, 그림]이라는 뜻의 graph가 합쳐진 말이다. 한자와 영어 표현에서 알 수 있듯이 암호는 문자나 그림을 사용하여 비밀을 유지할 수 있도록 하기 위해서 발명되었다고 할 수 있다. 그리고 사이퍼(cipher)라는 단어는 원래 아라비아로 숫자 ″0″을 의미한다. 이것이 암호의 의미로 사용된 것은 ″0″은 무언가를 숨기고 있는 비밀의 부호로 생각해 암호의 어원으로 자리 잡았다. 이렇듯 기호나 문자로서 암호를 사용하게 되었기 때문에 암호는 문자가 생긴 뒤 바로 생겨났다고 할 수 있다[11].

암호학(cryptology)은 그리스어 cryptos(hidden)와 logos(science)의 합성어로 자신의 정보를 가로채려는 노력으로부터 자신의 정보를 보호하기 위해 암호작성을 하는 것과 상대의 정보를 가로채려는 암호해독(cryptanalysis)에 관한 연구를 말한다. 이와 같은 두 가지 관점 즉, 평범한 사람이 이해할 수 있는 내용을 특정한 사람을 제외하고는 이해할 수 없는 형태로의 변형과 특정한 사람을 제외하면 이해할 수 없는 내용을 평범한 사람이 이해할 수 있는 형태로 바꾸는 방법을 연구하는 원리, 기술 또는 과학을 암호학이라 한다. 암호학은 암호작성과 암호해독 양쪽을 연구하는 학문이다[3, 6, 9, 11].

(2) 암호용어 정리

이 절에서는 암호학에 자주 나오는 기본적이고 중요한 용어를 몇 가지 간추려 설명하고자 한다[3, 5, 7, 10].

ⓐ 평문과 암호문 : 평범한 사람이 이해할 수 있는 형태인 일반 문장을 평문(plaintext, P)이라 하고, 평문이 일반인이 이해할 수 없는 형태로 변형된 문장을 암호문(cryptogram 또는 ciphertext, C)이라 한다. 이들 평문과 암호문을 이루는 기본 단위를 문자 또는 알파벳이라고 한다.

ⓑ 암호화와 복호화 : 평문을 암호문으로 변환하는 과정을 암호화과정(encryption process)이라 한다. 암호문을 평문으로 변환하는 방법을 알고 평문으로 바꾸는 과정을 복호화과정(decryption process)이라 한다.

ⓒ 송신자와 수신자 : 암호화된 정보를 안전하게 보내기를 원하는 사람 또는 주체를 송신자(sender), 송신자로부터 합법적으로 정보를 받는 사람 또는 주체를 수신자(receiver)라 한다.

ⓓ 암호화열쇠와 복호화열쇠 : 평문을 암호문으로 바꾸는 데 필요한 기술 또는 원리를 암호화열쇠(encryption key, EK)라 하고 암호문을 평문으로 바꾸는 데 필요한 기술 또는 원리를 복호화열쇠(decryption key, DK)라 한다. 암호화열쇠와 복호화열쇠를 암호열쇠라 한다.

ⓔ 암호알고리즘 : 암호화열쇠와 복호화열쇠는 보통 함수로 표현된다. 이 때, 암호화열쇠를 암호화함수(encryption function, E) 또는 암호화 알고리즘(encryption algorithm)이라 하고 복호화열쇠를 복호화함수(decryption function, D) 또는 복호화

알고리즘(decryption algorithm)이라 한다. 또한 암호화 알고리즘과 복호화알고리즘을 포함한 알고리즘을 암호알고리즘(crypto algorithm)이라 한다.

ⓕ 해독과정과 도청자 : 변환하는 방법을 모르는 상태에서 평문을 얻는 과정을 해독과정(analysis process) 또는 공격과정(attack process)이라 한다. 송신자와 수신자 사이에 전송중인 정보 또는 저장된 정보를 가로채려는 사람 또는 주체를 도청자(eavesdropper)라 한다. 이 때, 단순히 정보를 가로채려는 사람을 수동적인 도청자라 하고, 정보의 변조 또는 차단 등으로 수신자를 혼돈 시키는 도청자를 능동적인 도청자라 한다.

ⓖ 인증과 전자서명 : 수신자가 받은 정보가 원래의 송신자로부터 온 것임을 확인하는 것으로 도청자가 송신자를 가장 할 수 없도록 하는 과정이 인증(authentication)이고 수신자가 정보를 보낸 송신자를 통신 중에 위조하지 못하도록 확인하는 체계가 전자서명(digital signature)이다.

ⓗ 부인봉쇄와 무결성 : 정보의 송수신 과정에서 필요한 개념으로 정보의 송신 또는 수신을 송신자와 수신자가 부인하지 못하도록 하는 성질을 부인봉쇄(non-repudiation)라 하며, 전송된 정보가 변조되지 않게 하는 성질을 무결성(integrity)이라 한다.

ⓘ 암호화프로토콜 : 신뢰할 수 없는 두 주체 또는 다 주체간에 암호계를 이용하여 안전한 통신을 하는 절차를 암호화프로토콜(encryption protocol)이라 한다.

(3) 암호의 분류

평문들의 집합과 암호문의 집합을 포함한 암호알고리즘을 암호계(crypto system 또는 cipher system)라 한다. 암호알고리즘과, 시대에 따라 암호계는 다음과 같이 분류된다[3, 10].

ⓐ 대칭암호와 비대칭암호 : 암호화열쇠와 복호화열쇠가 같거나 상호간에 쉽게 얻어지는 암호를 대칭암호(symmetric cipher)라 하고, 그렇지 않은 암호를 비대칭암호(asymmetric cipher)라 한다. 즉, 암호화함수가 주어졌을 때, 암호화함수의 역함수인 복호화함수가 쉽게 얻어지는 암호는 대칭암호이고 그렇지 않은 암호는 비대칭암호이다. 따라서 대칭암호계에서 암호화함수가 알려지면 암호화된 정보는 더 이상 보호될 수 없으므로 암호화함수(또는 암호열쇠)는 비밀이 유지되어야 한다. 이러한 관점에서 대칭암호를 비밀열쇠암호(secret key cipher)라 한다. 이와 달리 암호화함수로부터 복호화함수를 얻을 수 없는 비대칭암호계에서는 암호화함수와 암호문이 노출되어도 암호문으로부터 평문을 얻을 수 없으므로 안전하다. 이와 같은 암호계에서는 암호화함수 또는 암호화열쇠는 일반인에게 공개하고 복호화함수 또는 복호화열쇠는 비밀이 유지되어야 한다. 이러한 관점에서 암호화열쇠를 공개열쇠(public key)라 하고 이 암호를 공개열쇠암호(public key cipher)라 한다. 이때에 비밀을 유지해야 하는 복호화열쇠를 개인열쇠(private key)라 한다. 예를 들면, DES와 AES는 대표적인 대칭암호이고 RSA는 비대칭암호이다.

ⓑ 블록암호와 스트림암호 : 암호화하는 과정에서 변환되는 단위가 블록인 암호를 블록암호(block cipher)라 하고 무한 임의 이진 수열(또는 무한 난수)을 이용하여 이진 수열로 변환된 평문을 암호화하는 암호를 스트림암호(stream cipher)라 한다. 즉, 암호함수의 정의역에 속하는 단위가 유한인 암호는 블록암호이고 유한이 아닌 암호는 스트림암호이다. 여기에서 무한 난수는 평문 전체의 길이보다 작지 않

은 난수들의 열을 의미한다.

ⓒ 고전암호, 기계암호 및 현대암호 : 시대에 따라 암호계를 분류하는 방법으로, 시대에 따라 암호알고리즘에 사용되는 도구나 암호화하는 방법이 다르다. 제1차 세계대전 이전까지 사용된 암호로 전치, 대입, 치환의 원리를 이용하여 직접계산하거나 또는 표를 이용하여 변환하는 암호를 고전암호라 하며, 대표적인 암호로는 그리스시대의 Scytale 암호, 로마시대의 Caesar 암호 등이 있다. 이와 비교하여 제1차 세계대전 말부터 개발되어 제2차 세계대전까지 주로 사용된 암호로 기계(rotor machine이라 불리는)를 이용한 암호를 기계암호라 하며, 예로는 Hagelin(또는 M209), Enigma 등이 있다. 한편, 제2차 세계대전 이후 컴퓨터의 발달과 더불어, 암호화와 복호화에 과거의 암호들과는 달리 상당히 복잡한 계산량을 요구하는 컴퓨터를 이용한 암호를 현대암호라 한다. 현대암호의 대표적인 예로는 DES, AES, RSA 등이 있다.

2. RSA암호

(1) RSA암호가 나오게 된 배경

고전 암호 시스템, 스트림 암호 시스템 그리고 DES에서는 송신자와 수신자가 동일한 키를 이용하여 암호화하거나 복호화 했다. 송신자가 보유한 키와 수신자의 키가 동일한 암호시스템을 대칭형 암호시스템(symmetric cryptosystem)이라고 한다. 따라서 이런 대칭형 암호시스템에서는 송·수신자에게 사전에 키 분배가 있어야 한다. 특히 군대처럼 다소 폐쇄적인 단체나 기업에서는 이 암호체계 사용이 용이한 반면, 인터넷을 광범위하게 사용하는 현대의 개방형 체계에서 상대방을 전혀 알지 못하는 사용자들 간의 정보교환에서 대칭형 암호 체계는 적합하지 않다[1, 9].

예를 들어, n명의 사용자로 구성된 네트워크에 새로운 사용자가 한명 더 추가 될 때마다 n개의 대칭키가 추가로 요구된다. 일반적으로 n명으로 구성된 네트워크 사용자들 간에는 n·(n-1)/2개의 서로 다른 대칭키가 필요하다. 따라서 사용자의 수가 증가함에 따라 키를 생성하고 분배하는 작업은 시스템의 효율을 크게 저하시킬 뿐만 아니라 각 사용자가 많은 키를 유지, 관리하는 것은 매우 번거로운 일이다.

이러한 대칭형 암호시스템의 약점을 보완하기 위하여, 1976년에 미국 스탠퍼드 대학의 Diffie와 Hellmann이 공개키 암호시스템(publickey cryptosystem)이라는 새로운 개념을 발표하였다. 그 후 1978년 미국 MIT대학의 Rivest, Shamir와 Adleman이 처음 RSA라고 하는 유명한 공개키 암호 방식을 제안하였다[8].

이 RSA암호가 나오게 된 배경에는 다음과 같은 일화가 있다[12].

「 *Ron Rivest는 한 대학생의 논문을 읽고 전율을 느끼고 암호학의 새로운 방향에 강하게 끌렸고, 그의 인생을 바꾸는 계기가 되었다. 그 논문 저자가 바로 Diffie였다. Diffie가 일하는 인공지능 연구소는 Rivest가 일하는 컴퓨터 과학연구소 바로 위층 이었지만 Rivest는 Diffie나 Hellman의 이름조차 몰랐고*

암호에 대해서도 거의 아는 것이 없었다. 하지만 충분히 강한 일방향함수를 찾는다면 완전히 새로운 종류의 전자상거래가 탄생할 것이라 확신했기 때문에 동료들에게도 과제를 전파하기 시작했고 그 중 Leonard Adleman이란 젊은 수학자가 있었다. 하지만 Aldeman은 Rivest와는 달리 순수이론분야에는 관심이 많았지만 응용분야에는 큰 관심이 없었기 때문에 Rivest가 제시한 과제에 대해서도 큰 관심을 갖지 않았다. 그래서 처음에는 친분 때문에 일에 참여하게 된다. Adi Shamir도 Rivest와 같이 일방향함수를 찾는 것이 중요하다는 것에 동조했고 이 셋은 한 팀이 되어 연구를 시작한다. Rivest와 Shamir가 어떤 체제를 만들어오면 Adleman은 그 체제의 결함을 제시하는 방식이었다. Rivest는 만들어 온 체제마다 번번히 체제가 공격당하자 연구방향을 반대로 하여 강력한 일방향함수가 존재하지 않음을 증명하려고 시도하였으나 그 쪽도 진전이 없었다.

1977년 4월 3일 Rivest는 유월절 축제를 지내고 집에 돌아와 골똘히 생각하던 중에 새로운 체계에 대한 아이디어를 생각해내고 다음날 아침 Shamir와 Adleman에게 발표 가능한 형식으로 쓴 원고를 보여주었는데 세 사람의 이름이 모두 적혀 있었다. Adleman은 처음에는 논문에서 자신의 이름이 올라가는 것을 올바르지 않다고 주장했지만 나중에 이름은 올리되 맨 마지막에 올려달라고 주문하고, Shamir는 Rivest의 이름이 제일 먼저 기재되기를 원하며 이 세 사람의 이름순서대로 RSA라는 이름이 탄생했다. Ron Rivest, Adi Shamir, Leonard Adleman이 만든 RSA 방식은 암호화하는 열쇠와 복호화하는 열쇠를 달리 함으로써 기밀성 이외에도 인증 기술까지도 제공할 수 있어 공개열쇠 암호방식의 기초가 된다. Shamir는 오히려 암호에 대해 잘 알지 못했던 것이 값진 자산이었다고 말한다. 암호학을 어느 정도라도 알고 있었다면 기존의 틀에서 연구하려고 했을 텐데 암호학에 대해 아는 것이 부족했기 때문에 대학에서 배운 개념들을 시험해보며 연구했다고 말한다. ┘

(2) RSA암호 방식

1) RSA암호 방식

1976년 Diffie와 Hellman이 공개키 암호 방식의 개념을 발표한 후, 1978년 미국 MIT대학의 Rivest, Shamir와 Adleman이 처음 RSA라고 하는 유명한 공개키 암호 방식을 제안하였다[9, 14].

이들은 합성수의 소인수 분해의 어려움을 이용하여 RSA 암호 방식을 실현하였다[4].

암호화 과정과 복호화 과정을 설명하기 위하여 필요한 몇 가지 기호를 나열하면 아래와 같다[3, 8].

n : 암호화 과정과 복호화 과정에 이용되는 공개된 법(modulus)으로 공개되지 않은 두 소수 p, q의 곱 즉 $n=p \cdot q$
e : 공개된 지수
d : $d \equiv 1(\bmod (p-1)(q-1))$을 만족하는 공개되지 않은 양의 정수
P : 암호화하기 전의 평문(양의 정수)
C : 암호화된 암호문(양의 정수)

가입자는 백 자리 크기 이상의 두 개의 소수 p, q를 선택하여 $n=p \cdot q$를 계산한다. 이 때 p와 q를 알고 있는 사람은 n을 계산하기 쉽지만 n만 알고 있는 사람은 n으로부터 p와 q를 찾는 소인수 분해는 어렵다.

p와 q를 선택하여 n을 계산한 다음 Euler 함수 값 $\phi(n)=(p-1)(q-1)$과 서로소인 e를 선택한다. 다시 유클리드 호제법을 이용하여 다음 식을 만족하는 d를 계산한다.

$$ed \equiv 1(\bmod \phi(n))$$

e와 n은 공개목록에 등록하여 공개하고 d는 비밀리에 보관한다. 즉, e는 공개키가 되고 d는 비밀키가 된다[4].

RSA 공개열쇠 암호의 암호화변환함수 E와 복호화변환함수 D는 각각

$$C = E(P) \equiv P^e \pmod{n}, \qquad P = D(C) \equiv C^d \pmod{n}$$

으로 정의된다. 이때 공개된 수 e와 n을 이 암호계의 공개열쇠(public key)라 하고 d를 개인이 보안을 유지해야 하는 개인열쇠(private key)라 한다[3, 8].

[예 1] 소수 $p = 47$, $q = 59$로 RSA공개키 암호를 구성해 보자.

☞) $n = pq = 2773 \qquad \phi(n) = (p-1)(q-1) = 2668$

$\gcd(e, 2668) = 1$인 e를 157로 선정하자. $ed \equiv 1 \pmod{2668}$인 d를 구하자.

$\Rightarrow$ d를 구하는 방법 : $(d = 17)$

$2668 = 16 \times 157 + 156$

$157 = 156 \times 1 + 1$

$157 = (2668 - 16 \times 157) \times 1 + 1$

$$157 \times 17 = 2668 \times 1 + 1 \equiv 1 \pmod{2668}$$

평문 알파벳을 두 자리 수로 표시하자.

blank = 00	f = 06	l = 12	r = 18	x = 24
a = 01	g = 07	m = 13	s = 19	y = 25
b = 02	h = 08	n = 14	t = 20	z = 26
c = 03	i = 09	o = 15	u = 21	
d = 04	j = 10	p = 16	v = 22	
e = 05	k = 11	q = 17	w = 23	

다음 평문을 암호화 해보자.

public key cryptography

우선 평문을 암호화하기 위해 두 문자 당 하나의 숫자로 대응 시킨다.

1621, 0212, 0903, 0011, 0525, 0003, 1825, 1620, 1507, 1801, 1608, 2500

위 숫자를 암호화 해보자.

$$1621^{157} \equiv 2616 \pmod{2773} \quad 0212^{157} \equiv 0251 \pmod{2773}$$
$$0903^{157} \equiv 1581 \pmod{2773} \quad 0011^{157} \equiv 1690 \pmod{2773}$$
$$0525^{157} \equiv 2706 \pmod{2773} \quad 0003^{157} \equiv 0441 \pmod{2773}$$
$$1825^{157} \equiv 1853 \pmod{2773} \quad 1620^{157} \equiv 0417 \pmod{2773}$$
$$1507^{157} \equiv 2415 \pmod{2773} \quad 1801^{157} \equiv 0039 \pmod{2773}$$
$$1608^{157} \equiv 0735 \pmod{2773} \quad 2500^{157} \equiv 0230 \pmod{2773}$$

위 숫자를 암호문을 복호화 해보자.

$$2646^{17} \equiv 1621 \pmod{2773} \quad 0251^{17} \equiv 0212 \pmod{2773}$$
$$1581^{17} \equiv 0903 \pmod{2773} \quad 1690^{17} \equiv 0011 \pmod{2773}$$
$$2706^{17} \equiv 0525 \pmod{2773} \quad 0441^{17} \equiv 0003 \pmod{2773}$$
$$1853^{17} \equiv 1825 \pmod{2773} \quad 0417^{17} \equiv 1620 \pmod{2773}$$
$$2415^{17} \equiv 1507 \pmod{2773} \quad 0039^{17} \equiv 1801 \pmod{2773}$$
$$0735^{17} \equiv 1608 \pmod{2773} \quad 0230^{17} \equiv 2500 \pmod{2773}$$

[예 2] 소수 $p=11$, $q=17$로 RSA 공개키 암호를 구성해보자.

☞) $n = pq = 11 \cdot 17 = 187$

$\phi(n) = (p-1)(q-1) = (11-1)(17-1) = 10 \cdot 16 = 160$

$\gcd(e, 160) = 1$, $e = 7$으로 선정

$ed = 7d \equiv 1 \pmod{160}$ $\qquad \therefore d = 23$

즉 공개키 $(7,187)$이고 비밀키는 $d = 23$이다.

[예 3] 위**[예 2]**의 암호키($e=7$) 이용하여 $M=3$일 때 암호 하여라.

☞) $C \equiv M^e \pmod{n}$이므로 $C \equiv 3^7 \pmod{187}$이다.

$3^2 = 9 \pmod{187}$

$3^3 = 27 \pmod{187}$

$3^4 = 81 \pmod{187}$

$3^5 = 243 \equiv 56 \pmod{187}$

$3^6 = 168 \pmod{187}$

$3^7 = 504 \equiv 130 \pmod{187}$ $\qquad \therefore C = 130$

[예 4] 공개키(3, 22)를 이용하여 다음 평문 M=apple을 암호화 해보자.

blank = 00	f = 06	l = 12	r = 18	x = 24
a = 01	g = 07	m = 13	s = 19	y = 25
b = 02	h = 08	n = 14	t = 20	z = 26
c = 03	i = 09	o = 15	u = 21	
d = 04	j = 10	p = 16	v = 22	
e = 05	k = 11	q = 17	w = 23	

☞) 우선 평문을 암호화하기 위해 문자를 하나의 숫자로 대응시킨다.

($a=01 \quad p=16 \quad p=16 \quad l=12 \quad e=05$) 이제 암호화 해보자.

$1^3 \equiv 1 \pmod{22}$

$16^3 \equiv 4 \pmod{22}$

$16^3 \equiv 4 \pmod{22}$

$12^3 \equiv 12 \pmod{22}$

$5^3 \equiv 15 \pmod{22}$

$\therefore addlo$

2) RSA암호 해독

① RSA암호 방식의 해독

암호 해독자가 RSA암호 방식의 $\phi(n)$을 우연히 알 수 있었다면 n이 p, q의 곱이기 때문에 다음의 두 방정식을 이용하여 n을 소인수 분해할 수 있다.

$$n = pq$$

$$\phi(n) = (p-1)(q-1)$$

$q = n/p$를 두 번째 식에 대입하면 미지수 p에 관한 2차 방정식을 얻을 수 있다.

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

이 방정식의 두 개의 근 p와 q가 n의 인수가 된다. 따라서 암호 해독자가 $\phi(n)$

값을 알면 n을 소인수분해해서 RSA암호 방식을 해독할 수 있다. 물론 n으로부터 $\phi(n)$의 계산은 n을 소인수분해 하는 것보다 간단하지 않다[4, 8].

[예 5] 암호 해독자가 $n=2419$와 $\phi(n)=2320$을 알고 있을 때, 이 정보로부터 $n=pq$의 p, q를 다음과 같이 계산할 수 있다.

$p^2-(2419-2320+1)p+2419=0$

$p^2-100p+2419=0$

이 2차 방정식의 근은 41과 59로 $n=pq=41\times 59=2419$를 간단히 계산할 수 있다.

② RSA암호 방식의 반복법에 의한 해독

RSA암호 방식의 해독 방법으로 $n=pq$의 소인수 분해를 통하여 p와 q를 찾아 공개 암호화 키 e와 비밀 복호화 키 d를 찾는 방법을 생각해 왔다.

유사한 방법으로 평문 M이 인수로 p또는 q가 포함되어 있는 경우 p혹은 q를 찾을 수 있다. 평문 M 이 인수로 p또는 q를 갖고 있으면 법 n도 인수로 p또는 q를 갖고 있으므로 암호문 C로도 인수로 p또는 q를 찾을 수 있다.

실제로 이 해독 방법은 해독할 성공률이 낮다. 왜냐하면, p와 q를 인수로 갖는 평문 M이 상당히 적기 때문이다.

RAS암호 방식의 더욱 잠재적인 약점으로 지적되는 것은 n의 소인수분해나, 비밀 복호화 키 d를 찾는 것이 아니라 공개 암호화 키 e와 암호문 C만을 갖고 평문을 찾는 방법이다. 이 공격법은 C와 n, 공개 암호화 키 e만 갖고, 평문을 찾는 방법이다. 이 공격법은 C와 n, 공개 암호화 키 e만 갖고, 소인수분해를 통하여 p, q를 찾는 것보다 훨씬 짧은 시간 내에 평문 M을 구할 수 있다. 이 공격법은 암호문 C를 공개 암호화 키 e로 반복 암호화하는 방법이다. 암호문 C를 공개 암호화 키 e로 반복 암호화하면 다시 암호문 C가 나타난다. 그러면 다시 암호문 C가 나타나기 전에 값이 평문 M이 된다[4, 8].

[예 6] $p=11$, $q=3$으로 구성되는 작은 n값의 RSA암호 방식에서 반복 암호화 해독을 해보자.

☞) RSA암호 방식을 구성하자.

$$n=pq=33,\ \phi(n)=20$$

e를 3으로 선택하자.

$$ed \equiv 1 \pmod{\phi(n)}$$

$$d=7$$

공개 암호화 키 $e=3$, 비밀 복호화 키 $d=7$

평문 $M=3$을 암호화한 후 반복 암호화 해독을 해보면 다음과 같다.

$$\begin{aligned} C &\equiv 3^3 \pmod{33} \\ &\equiv 27 \pmod{33} \end{aligned}$$

$$27^3 \equiv 15 \pmod{33} \quad 15^3 \equiv 9 \pmod{33} \quad 9^3 \equiv 3 \pmod{33} \quad 3^3 \equiv 27 \pmod{33}$$

암호문 $C=27$을 반복 암호화하면 4번 만에 다시 동일 암호문 27이 나타나므로 그 전단계의 암호화 과정의 3이 평문임을 알 수 있다.

다시 평문 $M=5$에 대한 암호문 $C=5^3 \equiv 26 \pmod{33}$을 반복 암호화 공격을 해보자.

$$26^3 \equiv 20 \pmod{33} \quad 20^3 \equiv 14 \pmod{33} \quad 14^3 \equiv 5 \pmod{33} \quad 5^3 \equiv 26 \pmod{33}$$

[예 7] 위의 **[예 3]**의 암호문($C=130$)을 비밀키 $d=23$을 이용하여 해독하여라.

☞) $M \equiv C^d \pmod{n}$이므로

$$M \equiv 130^{23} \pmod{187}$$

$$130^2 = 16900 \equiv 70 \pmod{187}$$

$$\vdots$$

$$130^{23} \equiv 3 \pmod{187}$$

$$\therefore M=3$$

[예 8] 이제 비밀키 $d=7$을 이용하여 위의 **[예 4]**의 암호문을 복호화 해보자.

☞) $1^7 \equiv 1 \pmod{22}$

$4^7 \equiv 16 \pmod{22}$

$4^7 \equiv 16 \pmod{22}$

$12^7 \equiv 12 \pmod{22}$

$15^7 \equiv 15 \pmod{22}$

$\therefore apple$

마찬가지로 반복 암호화 해독으로 RSA암호 방식이 해독을 당할 수 있음을 알 수 있다. Rivest는 이 반복 암호화 해독법으로 RSA암호 방식을 해독하는 경우 다시 암호문이 나타날 때까지의 반복 암호화 주기를 분석하고 소수 p, q의 선택에 따라 RSA암호 방식이 안전할 수 있는 조건이 존재하는 것을 확인하였다.

즉, $n=pq$에서 대수 계산에 강한 암호 방식을 만들기 위해서는 $p-1$과 $q-1$의 인수 p'과 q'도 큰 인수를 갖고 있어야만 반복 암호화 해독에 견딜 수 있음을 확인하였다[4, 8].

3) RSA암호 안전성

RSA암호 방식의 안전성은 소수 p와 q에 달려 있다. 공개키 e와 n을 가지고 비밀키 d를 구할 수 있다면 RSA암호시스템은 쉽게 해독이 된다. 또한 n으로부터 소수 p와 q를 찾을 수 있다면 즉, n의 소인수분해가 가능하면 Euler 함수 $\phi(n)$을 찾게 되어 유클리드 알고리즘을 사용하여 공개키 e로부터 비밀키 d를 쉽게 계산할 수 있다. 그러므로 RSA암호시스템의 전체 안전성은 $\phi(n)$을 구할 수 있다면 유클리드 알고리즘으로 d를 쉽게 계산할 수 있다. 따라서 RSA암호 시스템의 전체 안전성은 $\phi(n)$의 계산에 달려 있다고 할 수 있다. $\phi(n)$은 n을 소인수분해 할 수 있다면 자동적으로 계산되기에 n의 소인수분해는 곧 RSA암호 시스템의 해독을 의미

하게 된다. 그러므로 n의 소인수를 모르고 Euler 함수 $\phi(n)$의 값을 결정하는 방법은 아직까지 알려져 있지 않다[4].

RSA암호 방식의 안전성을 보장받기 위한 소수 p와 q의 선택조건과 공개키 e와 비밀키 d의 조건들이 부가적으로 필요하다.

RSA암호 시스템을 안전하게 구성하기 위하여 소수 p, q는

ⓐ p, q는 거의 같은 크기의 수이다.

ⓑ $p-1$, $q-1$은 큰 소인수를 갖는다.

ⓒ $\gcd(p-1, q-1)$은 작은 수이다.

ⓓ $p+1$, $q+1$이 큰 소인수를 갖는다.

ⓔ $|p-q|$는 충분히 커야한다.

는 조건을 만족해야 한다[10, 14].

위와 같은 조건은 $n=pq$의 소인수분해를 어렵게 만들므로 이를 이용한 RSA암호 방식의 해독을 어렵게 만든다.

현재까지 알려진 인수분해 알고리즘 중 가장 우수하다고 할 수 있는 것의 복잡도는 $\exp((O(1)+1)\log n \log\log n)^{1/2}$이다. 소수 p와 q의 크기가 100자리이고 n이 200자리인 합성수라면 현재의 소인수분해 알고리즘과 정보공학 기술로는 이러한 n을 소인수분해하는 것은 거의 불가능한 것으로 알려져 있다[1, 4, 11].

공개키 n의 소인수분해가 어렵다고 해서 RSA암호가 해독이 어렵다고 믿는다. 그러나 공개키 n의 소인수분해가 가능하지 않다고 해서 RSA암호가 해독 불가능하다는 것은 아니다. 즉 소인수분해 이외의 방법으로도 RSA암호 시스템은 해독될 수 있다. 따라서 RSA암호 시스템의 안전성의 상한치는 소인수분해라고 말할 수 있다.

4) RSA암호 이론적 배경

RSA암호의 수학적 원리는 크게 유클리드 호제법과 Euler정리에 근거한다.

[정리 1] 두 정수 a, b에 대하여 $(a,b)=d$일 때, 적당한 정수 x, y가 존재하여

$$d=ax+by$$

이다[11].

증명) 먼저 정수 s, t에 관한 $as+bt$를 a, b의 일차결합이라 한다.

a, b의 일차결합 전체집합을 S라 하면 $S=\{as+bt|as+bt>0, s\in Z, t\in Z\}$ 이다.

여기서 임의의 $s,t\in Z$에 대하여 $as=as+b\cdot 0\in S$, $bt=a\cdot 0+bt\in S$ 이므로 $S\neq\varnothing$이다.

또한 임의의 $s,t,u,v\in Z$에 대하여 $(as+bt)\pm(au+bv)=a(s\pm u)+b(t\pm v)$ 이므로 S는 덧셈과 뺄셈에 관하여 닫혀 있다. 따라서 정수의 정렬성에 의하여 최소 양의 정수가 존재하며 이를 d라 하자. $d\in S$이므로 적당한 정수 x, y이 존재하여 $d=ax+by$이다.

이제 $d=(a,b)$임을 보이자. $a\neq 0$이고 $d>0$이므로 정수의 나눗셈 알고리즘에 의하여 $a=qd+r$, $0\le r<d$인 정수 q, r이 존재한다. 이것을 r에 대하여 나타내면 $r=a-qd=a-q(ax+by)=a(1-qx)+b(-qy)$이다. 만약 $r>0$이면 $r\in S$이 되어 d의 선택에 모순이다. 그러므로 $r=0$이다. 따라서 $a=dq$ 즉, $d|a$이다.

또한 $b\neq 0$ 일 때는 적당한 $q'\in Z$가 존재하여 $b=dq'$ 즉, $d|a$이다.

이것으로 d는 a, b의 공약수임이 증명되었다.

이제 최대공약수임을 보이기 위해 정수 c가 a, b의 공약수이면 $c|a$, $c|b$ 이므로$c|(ax+by)$이다. 따라서 $c|d$이다. 그러므로 d는 a, b의 최대공약수이다.

[정리 2] 유클리드 호제법 (Euclidean algorithm) [9, 11]

두 정수의 최대공약수를 계산할 때는 유클리드의 호제법을 이용한다.

두 양의 정수 a, b에 대하여 다음이 성립한다고 하자.

$$
\begin{aligned}
b &= q_1 a + r_1 & 0 &< r_1 < a \\
a &= q_2 r_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &< r_3 < r_2 \\
&\vdots & &\vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} & 0 &< r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n
\end{aligned}
$$

이때, $(a, b) = r_n$이다.

또한 앞의 등식들을 반대로 차례차례 이용하면 **[정리 1]**에 의하여 $(a, b) = r_n = as + bt$인 정수 s, t를 구할 수 있다.

$$
\begin{aligned}
r_n &= r_{n-2} - q_n r_{n-1} \\
&= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\
&= r_{n-2}(1 + q_{n-1} q_n) + r_{n-3}(-q_n) \\
&\quad \vdots \\
&= as + bt
\end{aligned}
$$

[정리 3] 양의 정수 m과 정수 a에 대하여 $(a, m) = 1$이면, 일차합동식

$$ax \equiv b \pmod{m}$$

는 단 하나의 해를 갖는다[11].

증명) ㉠ 존재성 : $(a, m) = 1$이면 **[정리 1]**에 의해 $as + mt = 1$인 정수 s, t가 존재한다.

이때 $a(sb) + m(tb) = b$ 이므로 $a(sb) \equiv b \pmod{m}$이고

따라서 $x \equiv sb \pmod{m}$는 주어진 합동식의 해가 된다.

㉡ 유일성 : $x = x_1 \pmod{m}$, $x = x_2 \pmod{m}$를 이 합동식의 해라고 하자.

$ax_1 \equiv b \equiv ax_2 \pmod{m}$이고 $a(x_1 - x_2) \equiv 0 \pmod{m}$이다.

$(a, m) = 1$이므로 $x_1 \equiv x_2 \pmod{m}$이다. 따라서 합동식의 해는 한 개뿐이다.

$(a, m) = 1$일 때 일차합동식의 특수한 경우인 $ax \equiv 1 \pmod{m}$의 해 x를 법 m에 관한 a의 역원(inverse element)이라 한다. 해 x를 구할 때 법 m이 작은 자연수의 경우는 직접 대입하여 구하지만, 법 m이 큰 수인 경우에는 유클리드 호제법을 이용하여 구한다[11].

[정리 4] 집합 $R = \{r_1, r_2, \cdots, r_{\phi(m)}\}$가 법$m$에 관한 기약 잉여계일 때,

$(a, m) = 1$인 정수 a에 대하여 $T = \{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$

는 법 m에 관한 기약 잉여계이다[11].

증명) $ar_i \equiv ar_j \pmod{m}$이면, $(a, m) = 1$이므로 $r_i \equiv r_j \pmod{m}$이고 R이

기약잉여계 이므로 $r_i = r_j$이다. 즉, $r_i \neq r_j$이면 $ar_i \neq ar_j \pmod{m}$이다.

따라서 $ar_1, ar_2, \cdots, ar_{\phi(m)}$은 모두 다르므로 $|T| = \phi(m)$이다.

그리고 $(a, m) = 1$이고 각 $r_i \in R$에 대하여 $(r_i, m) = 1$이므로 $(ar_i, m) = 1$

이다.

따라서 T는 법 m에 관한 기약잉여계이다.

[정리 5] Euler의 정리

양의 정수 m과 $(a, m) = 1$인 정수 a에 대하여 다음이 성립한다.

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

특히, $m = p$가 소수일 때 $a^{\phi(p)} = a^{p-1} \equiv 1 \pmod{p}$이다[11].

증명) 집합 $R=\{r_1, r_2, \cdots, r_{\phi(m)}\}$을 법 m에 관한 기약잉여계라고 하면, **[정리 4]**에 의하여 $(a, m)=1$일 때 $T=\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$는 법 m에 관한 기약잉여계이다. 따라서 T의 각 원소는 R의 단 한 개의 원소와 법 m에 관하여 합동이므로 다음이 성립한다.

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod m$$

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod m$$

$r_i \in R$에 대해 $(r_i, m)=1$이다. 합동식으로부터 $a^{\phi(m)} \equiv 1 \pmod m$을 얻는다.

[정리 6] 정수 n은 서로 다른 홀수인 소수 p와 q의 곱이고, 즉 $\phi(n)=(p-1)(q-1)$이고 $ed \equiv 1 \pmod{\phi(n)}$이면, 임의의 P에 대하여

$$P^{ed} \equiv P \pmod n$$

이다[3, 8, 11].

증명) 가정에 의하여 적당한 정수 k가 존재하여 $ed-1=k\phi(n)$이다.

(ⅰ) $\gcd(P, n)=1$: Euler의 정리에 의하여 $P^{\phi(n)} \equiv 1 \pmod n$이므로 $P^{ed-1} \equiv P^{k\phi(n)} \equiv 1 \pmod n$이다. 따라서 $P^{ed} \equiv P \pmod n$이다.

(ⅱ) $\gcd(P, n) \neq 1$: $\gcd(P, n)=n$이면 양변 모두 0이 되어 분명하다. 이제 $\gcd(P, n)=p$인 경우만 증명하면 $\gcd(P, n)=q$인 경우는 같은 방법으로 증명되므로, $\gcd(P, n)=p$인 경우를 증명한다. 즉, $\gcd(P, q)=1$이므로 Euler의 정리에 의하여 $P^{q-1} \equiv 1 \pmod q$이므로

$$P^{ed-1} \equiv P^{k\phi(n)} \equiv 1 \pmod q$$

이다. 따라서 $P^{ed} \equiv P \pmod q$이므로 적당한 정수 r이 존재하여

$$P^{ed} - P = rq$$

이다. 한편, P는 p의 배수이므로 적당한 정수 t가 존재하여

$$P^{ed} - P = tpq = tn$$

이다. 따라서 $P^{ed} \equiv P \pmod n$이다.

따라서 RSA 공개열쇠 암호의 복호화과정이 **[정리 6]**에 의존되는 것을 쉽게 알 수 있다.

P =======> $P^e \pmod n$ =======> $(P^e)^d \pmod n$ 암호화 복호화

이 공개열쇠 암호의 해독은 공개열쇠 e와 n을 이용하여 d를 구하는 문제와 같다. 한편, 임의의 자연수 e와 k가 서로소이면, $ed \equiv 1 \pmod k$인 d가 존재하며, 이 d를 구하기 위하여 Lamé의 정리와 Euclid 호제법을 이용한다. 실제로 Lamé의 정리에 의하면 $\gcd(e, \phi(n)) = 1$일 때, $ed \equiv 1 \pmod{\phi(n)}$을 만족하는 d를 얻기 위하여 기껏해야 $-2 + [\log_R \phi(n)]$단계의 나눗셈을 시행하여 얻을 수 있다(단 $R = \frac{(1+\sqrt{5})}{2}$). 따라서 RSA암호가 해독되지 않으려면 $\phi(n)$을 얻기 어려워야 한다.

[정리 7]은 n을 소인수분해하는 것과 $\phi(n)$을 아는 것이 동치임을 보여준다[3, 8].

[정리 7] 정수 n이 소수 p와 q의 곱일 때, p와 q가 주어지는 것은 $\phi(n)$이 주어지는 것과 동치이다[3, 8, 11].

증명) $n = pq$이면 $\phi(n) = (p-1)(q-1) = n+1-(p+q)$이다. 따라서 p와 q가 주어지면 $\phi(n)$이 쉽게 구하여 진다.

역으로, $\phi(n)$이 주어지면

$$p+q = n+1-\phi(n)\text{이고 } pq = n$$

이므로 p와 q는 이차방정식

$$t^2 - [n+1-\phi(n)]t + n = 0$$

의 근이다. 따라서 p와 q를 쉽게 구할 수 있다.

실제, $n = 3233$이고 $\phi(n) = 3120$이면 $pq = 3233$이고 $(p-1)(q-1) = 3120$이므로 $p+q = pq+1-3120 = 144$이다. 소수 p와 q는 이차방정식 $t^2 - 114t + 3233 = 0$의 근이므로 p와 q는 53또는 61이다[3, 8].

앞에서, $n=pq$의 소인수를 아는 것과 $\phi(n)$을 아는 것은 동치이며, 이들을 알고 e를 알면, 유클리드 호제법을 이용하여 $ed \equiv 1 \pmod{\phi(n)}$을 만족하는 d를 구할 수 있었다. 이제, 역으로 n, e와 d가 주어지면 LasVegas알고리즘을 이용하여 n을 소인수분해 할 수 있음을 증명한다. 즉, n의 소인수분해와 개인열쇠 d를 구하는 것이 동치이다[3, 8].

개인열쇠 d가 알려졌을 때, 인수분해 알고리즘은 다음과 같다[3, 8].

[개인열쇠가 주어졌을 때, n의 소인수분해]

1단계 : 임의의 정수 $w(1 \le w \le n-1)$를 선택한다.
2단계 : $x = \gcd(w, n)$을 계산한다.
3단계 : $1 < x < n$이면 중지하고 $x=p$또는 $x=q$를 구한다. $x=1$이면, 4단계로 간다.
4단계 : $ed-1 = 2^s r$(r은 홀수)로 표현한다.
5단계 : $v \equiv w^r \pmod{n}$을 계산한다.
6단계 : $v \equiv 1 \pmod{n}$이면, 중단(실패이므로)하고 11단계로 가고, $v \not\equiv 1 \pmod{n}$이면, 7단계로 간다.
7단계 : $v \equiv -1 \pmod{n}$이면, 중단(실패이므로)하고 1단계로 가고, $v \not\equiv -1 \pmod{n}$이면, 8단계로 간다.
8단계 : $v_0 = v$로 놓고 $v \equiv v_0^2 \pmod{n}$을 계산하여 9단계로 간다.
9단계 : $v \equiv 1 \pmod{n}$이면, 10단계로 가고, $v \not\equiv 1 \pmod{n}$이면, 7단계로 간다.
10단계 : $x = \gcd(v_0+1, n)$을 계산하므로 $x=p$또는 $x=q$를 얻는다.

이제 $p-1 = 2^i p_1$, $q-1 = 2^j q_1$(p_1과 q_1은 홀수), $n=pq$라 하고 w는 n과 서로소라 할 때, 이 알고리즘을 이용하여 확률 $\frac{1}{2}$이상으로 n을 소인수분해 할 수 있음을 다음 몇 가지 보조정리를 이용하여 증명한다[3].

[보조정리 8] (1) $\phi(n) = (p-1)(q-1) = 2^{i+j} p_1 q_1$

(2) $ed \equiv 1 \pmod{\phi(n)}$이면 $ed-1 = 2^s r$이다. 단, r은 홀수이다.

(3) $w^{2^s r} \equiv 1 \pmod{n}$이다[3].

증명) $p-1=2^i p_1$, $q-1=2^j q_1$을 대입함으로써 쉽게 증명된다.

[보조정리 9] 합동식 $w^r \equiv 1 \pmod{n}$의 해의 개수는 $p_1 q_1$이다[3].

증명) g를 p를 법으로 한 원시근이라 하면, 적당한 u가 존재하여 $w \equiv g^u \pmod{p}$ 이다. 그러면 $w^r = g^{ur} \equiv 1 \pmod{p}$이고 $2^i p_1 | ur$이다. 한편, g^u이 $w^r \equiv 1 \pmod{p}$의 해일 필요충분조건은 $2^i | u$이다. 따라서, $w^r \equiv 1 \pmod{p}$의 해의 개수는 p_1이다.

같은 방법으로 $w^r \equiv 1 \pmod{p}$의 해의 개수는 q_1이므로 중국인의 나머지 정리에 의하여 $w^r \equiv 1 \pmod{n}$의 해의 개수는 $p_1 q_1$이다.

[보조정리 10] 합동식 $w^{2^t r} \equiv -1 \pmod{p}$의 해의 개수는

$$\frac{p-1}{2^{i-t-1}} \times \frac{1}{2} = 2^t p_1 \qquad [3,\ 8]$$

증명) g를 p를 법으로 한 원시근이라 하면, 적당한 u가 존재하여 $w \equiv g^u \pmod{p}$ 이다. 그러면 g는 p를 법으로 한 원시근이므로 $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$이다.

따라서, $w^{2^t r} = g^{u 2^t r} \equiv -1 \pmod{p}$이고 $u 2^t r \equiv \frac{p-1}{2} \pmod{(p-1)}$이다.

따라서

$$\begin{aligned} g^u \text{이 } w^{2^t r} \equiv -1 \pmod{p} \text{의 해} &\Leftrightarrow (p-1) | (u 2^t r - \frac{p-1}{2}) \\ &\Leftrightarrow 2(p-1) | (u 2^{t+1} r - (p-1)) \\ &\Leftrightarrow 2^{i+1} p_1 | (u 2^{t+1} r - 2^i p_1) \\ &\Leftrightarrow 2^{i+1} | (\frac{u 2^{t+1} r}{p_1} - 2^i) \end{aligned}$$

이다. 따라서 $t \geq i$이면 해가 없다.

한편, $t \le i-1$일 때, g^u가 $w^{2^t r} \equiv -1 \pmod p$의 해일 필요충분조건은 u는 2^{i-t-1}의 홀수 배수이다.

따라서 $w^{2^t r} \equiv -1 \pmod p$의 해의 개수는 $\frac{p-1}{2^{i-t-1}} \times \frac{1}{2} = 2^t p_1$이다.

[보조정리 11] $w^{2^t r} \equiv -1 \pmod n$의 해의 개수는

$$0 \quad : t \ge \min\{i, j\}$$

$$2^{2t} p_1 q_1 \ : t \le \min\{i, j\} - 1 \qquad [3,\ 8]$$

증명) 중국인의 나머지 정리에 의하여 $w^{2^t r} \equiv -1 \pmod n$의 해의 개수는 $w^{2^t r} \equiv -1 \pmod n$의 해의 개수와 $w^{2^t r} \equiv -1 \pmod n$의 해의 개수의 곱이므로 **[보조정리 10]**에 분명하다.

[정리 12] 개인열쇠 d가 알려졌을 때, 인수분해 알고리즘은 적어도 확률 $\frac{1}{2}$로 n을 인수분해한다[3, 8].

증명) $\phi(n) = (p-1)(q-1) = 2^{t+j} p_1 q_1 < n$이고 $i \le j$를 가정해도 좋으므로 6단계와 7단계를 만족하는 w의 개수는

$$\begin{aligned} p_1 q_1 + p_1 q_1 (1 + 2^2 + 2^4 + \cdots + 2^{2i-2}) &= p_1 q_1 \left(1 + \frac{2^{2i-1} - 1}{3}\right) \\ &= \frac{2}{3} p_1 q_1 + \frac{2^{2i-1}}{3} p_1 q_1 \\ &\le \frac{n}{6} + \frac{n}{3} \\ &= \frac{n}{2} \end{aligned}$$

이다. 따라서 인수분해 할 수 없는 확률은 $\frac{1}{2}$이하이다.

예를 들면, $n=89855713$, $d=34986517$이고 $e=82330933$일 때, 임의의 정수 $w=5$를 선택하면 $ed-1=2^3\times 36005907337895$이다.

5단계에서 $v=85877701$이고

7단계에서 $v=1$이므로

10단계에서 $\gcd(85877702, n)=9103$을 얻는다.

이제 RSA 공개열쇠 암호계에서 공개열쇠 e를 선택하는 방법에 관하여 알아보자.

예를 들어, 공개열쇠의 쌍 $(e,n)=(17,35)$이 주어졌다고 하면 평문 8에 대하여 암호문은 $8^{17}\equiv 8 \pmod{35}$으로 평문과 같아 좋은 암호가 될 수 없다. 다음 **[정리 13]**은 이 예의 일반화를 설명한다.

[정리 13] 공개열쇠의 쌍 (e,n)을 가지는 RSA 알고리즘을 이용하여 암호화하면,

$$\{1+\gcd(e-1,p-1)\}\{1+\gcd(e-1,q-1)\}$$

개는 평문과 같은 암호문을 가진다[3, 8].

증명) 평문 P가 암호화변환에 의하여 불변일 필요충분조건은

$$P^e\equiv P \pmod{n}$$

이므로

$$P^e\equiv P \pmod{p}\text{이고 } P^e\equiv P \pmod{q}$$

이다. 한편,

$$P^e\equiv P \pmod{p} \Leftrightarrow P^{e-1}\equiv 1 \pmod{p} \text{ 또는 } P\equiv 0 \pmod{p}$$

이고 $P^{e-1}\equiv 1 \pmod{p}$의 해는 $\gcd(e-1,p-1)$개이므로 $P^e\equiv P \pmod{p}$는 $1+\gcd(e-1,p-1)$개의 해를 갖는다.

같은 방법으로 $P^e\equiv P \pmod{q}$는 $1+\gcd(e-1,q-1)$개의 해를 가지므로 중국인의 나머지 정리에 의하여 정리가 성립한다.

[예 9] $n=35$라 할 때, $e=17$이면 평문과 암호문이 같은 개수는

$$\{1+\gcd(16,4)\}\{1+\gcd(16,6)\}=15$$

이다. 즉,

$$\{0,1,6,7,8,13,14,15,20,21,22,27,28,29,34\}$$

는 평문과 암호문이 같다.

암호화변환에 대하여 불변인 평문의 개수 m은 **[정리 13]**으로부터 p, q 및 e에 의존되며 특정한 m의 값에 대하여 다음 결과를 얻는다.

ⓐ $m=4$: $\gcd(e-1,p-1)=\gcd(e-1,q-1)=1$

ⓑ $m=9$: $\gcd(e-1,p-1)=\gcd(e-1,q-1)=2$

실제로, 선택된 두 소수 p와 q에 대하여 위 조건을 만족하는 e를 선택할 수 있으므로 원하는 적은 m값을 얻을 수 있다. 이와 같이 얻은 m은 두 소수 p와 q의 곱 n과 비교하면 무시될 정고로 극히 작은 수로 암호문과 평문이 같은 경우는 일어나지 않는 것으로 생각할 수 있다.

(3) RSA암호의 활용

【 RSA암호 방식을 이용한 전자서명 】

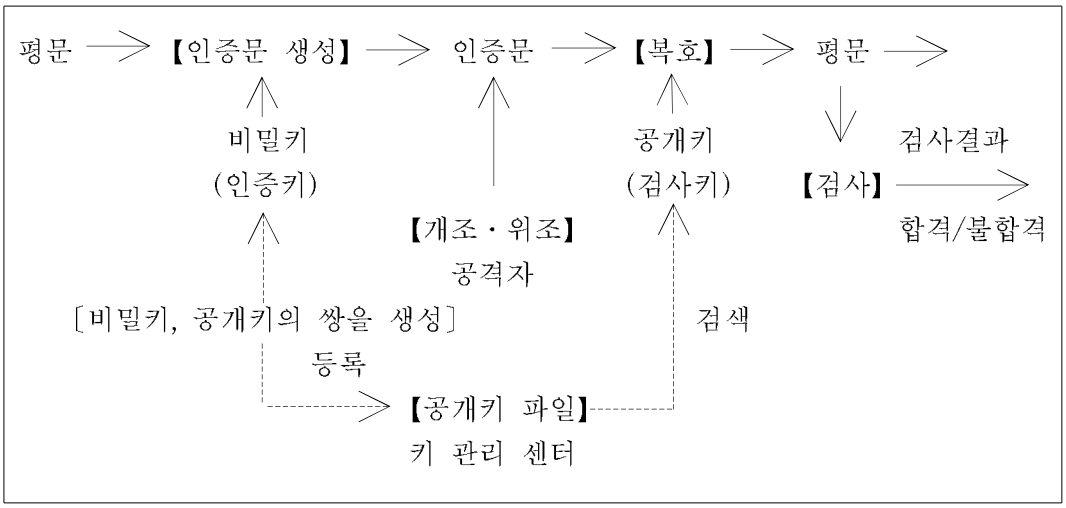
먼저 공개키 암호 방식을 이용한 전자 서명 방식을 살펴보도록 하겠다.

일반적으로 전자 서명이라 하면 공개키 암호 방식을 이용한 전자 서명 방식을 말한다. 관용 암호 방식을 이용한 중재 서명 방식은 서명자 A와 검증자 B사이에 서명할 때마다 중재자가 관여하여 서명의 당위성을 확인해야 하는 절차를 거쳐야 하므로 서명 방식 운영이 복잡하고 불편해질 수밖에 없다.

그러나 공개키 암호 방식을 이용한 서명 방식은 중재자를 필요로 하지 않는다. 공개키 암호 방식을 이용한 서명 방식은 가입자 전원이 비밀 서명 생성 정보(비밀키)와 공개 검증 정보(공개키)를 생성하여 비밀 서명 생성 정보는 비밀리에 보관하고, 공개 검증 정보는 공개목록에 등록한다.

서명자는 자신의 비밀 서명 생성 정보로 서명문 M의 서명 S를 생성하여 서명문 M과 함께 검증자에게 전송한다. 검증자는 서명자를 확인하고, 공개목록의 공개 검증 정보를 이용하여 서명자의 서명을 확인한다[4].

공개키 암호 시스템을 적용한 인증시스템을 살펴보면 다음과 같다[15].



여기서 전자 서명이 유효하기 위해서 갖추어야 할 기본적인 요구사항들은 다음과 같다[13].

- 위조불가(Unforgeable) : 합법적인 서명자만이 전자 서명을 생성할 수 있다.
- 서명자 인증(User authentication) : 전자 서명의 서명자를 누구나 검증할 수 있으며, 검증자는 서명자의 서명 행위를 확신 할 수 있다.
- 부인방지(Nonrepudiable) : 서명자는 서명행위 이후 서명한 사실을 부인 할 수 없다.
- 변경불가(Unalterable) : 서명 이후 그 내용을 수정, 변경할 수 없다.
- 재사용불가(Reusable) : 어떤 문서의 서명을 다른 문서의 서명으로 재사용 할 수 없다.

이제 공개키 암호 방식을 이용한 전자 서명 방식을 이용한 전자 서명 방식중 하나인 RSA암호 방식을 이용한 전자 서명을 살펴보도록 하자.

RSA 공개키 암호 방식은 정보보호 기능과 전자 서명 기능을 동시에 수행할 수 있는 암호 방식으로 전자 서명에 널리 이용되고 있다.

RSA암호 방식을 이용한 전자 서명 방식은 다음과 같다.

RSA암호 방식과 같이 서명자 A는 충분히 큰 소수 p, q를 선택하여 $n=pq$를 계산하고, $\phi(n)=(p-1)(q-1)$과 서로소인 e를 선택하여 $ed \equiv 1 \pmod{\phi(n)}$를 만족하는 d를 구한 다음 e와 n를 공개목록에 등록하고 d는 비밀리에 보관한다. 이 때, e, n는 서명 검증을 위한 공개 검증 정보이고 d는 비밀 서명 생성 정보이다.

서명 과정을 살펴보자. 공개 일방향 해쉬 함수(hash function)로 서명문 M을 서명할 수 있는 크기로 압축 $H=h(M)$한다. 압축된 서명문 H에 대한 서명 $S \equiv H^d \pmod{n}$를 계산하여 서명문 M과 함께 검증자 B에게 전송한다.

검증 과정을 알아보자. 검증자 B는 서명자 A의 서명문 M과 서명 S를 수신한 다음 공개목록의 서명자 A의 공개 검증 정보 e, n로 검증을 하게 된다. 수신한 서명문 M의 공개 일방향 해쉬 함수값 $H'=h(M)$을 계산하고 수신한 서명 S로부터 $H \equiv S^e \pmod{n}$를 계산한 다음 H와 H'를 비교하여 서로 같으면 서명문 M과 서명

S의 정당성을 확인할 수 있다. 만일, 서로 다르면 서명문 M이 전송 중에 병경되었거나 서명의 정당성에 이상이 있는 것으로 간주하고 이 서명 절차를 유효하지 않은 것으로 단정한다.

RSA암호 방식을 이용한 전자 서명의 안전도는 RSA암호 방식의 안전도와 일치한다. 즉 소수 p, q의 크기에 따른 $n=pq$의 소인수분해의 어려움을 기반으로 한 전자 서명 방식이다[4].

[예 10] $p=5$, $q=11$인 RSA암호 방식을 이용한 전자 서명 방식을 구성해보자.

서명문은 $M=5$로 해쉬 함수를 사용하지 않는다. 즉 $H=M=5$로 간주한다.

☞) $n=pq=55$

$\phi(n)=\phi(55)=40$

$\gcd(e,\phi(n))=1,\ e=7$

$ed\equiv 1 \pmod{\phi(n)}$

$7d\equiv 1 \pmod{40},\ d=23$

서명자 A의 비밀 서명 생성 정보는 $d=23$이고 공개 검증 정보는 $e=7$이다. 서명자 A가 서명문 $M=5$를 서명하여 검증자 B에게 전송한다.

서명문 $M=5$가 $n=55$보다 작아서 압축 해쉬 함수를 사용할 필요없이 서명 $S\equiv 5^{23} \pmod{55}\equiv 15$를 계산하여 서명문 $M=5$와 함께 검증자 B에게 전송한다.

검증자 B는 수신한 서명 $S=15$를 공개 검증 정보로 서명의 정당성을 확인한다. $M'\equiv S^e \pmod{n}\equiv 15^7 \pmod{55}$를 계산하여 M과 비교하여 서명을 확인한다[4].

전자서명의 대표적인 용도는 인터넷뱅킹 등의 금융거래, 인터넷 민원서비스, 인터넷쇼핑 등이 있으며, 앞으로 국제간 전자상거래, 전자투표 등으로 확대될 수 있다. 인터넷뱅킹이나 온라인 주식거래에 필요한 공인인증서는 국가가 지정한 공인인증기관에서 발행하고 공개키를 관리하는 대표적인 전자서명이다.

Ⅲ. 결　론

인터넷이 없이는 하루도 살 수 없는 이 시대에서 인터넷 쇼핑이나 사이버 증권 거래소에서 주식을 거래하면서 남들에게 노출되면 심각한 피해를 미칠 수 있는 정보가 인터넷망을 돌아다닌다. 그래서 정보의 중요성은 계속 논의 되고 있고 자신의 중요한 정보를 보호할 수 있는 암호화가 필요하다. 그것이 인터넷의 생활화와 함께 그 중요성이 점점 더 커지고 있다.

그런데 이 암호는 수학을 빼 놓고는 얘기 할 수가 없다.

고찰을 통해 암호의 실용성과 중요성을 살펴봄으로 수학의 실용성과 중요성을 확인 하였다.

본 논문에서는 먼저 암호의 이해를 돕고자 간단히 암호에 대해 설명한 후 RSA 암호를 중심으로 RSA암호 방식, RSA 암호 해독, RSA안정성과 RSA암호의 이론적 배경에 대해 살펴보았다. 그리고 이론적 배경을 이용한 간단한 암호화와 복호화를 하는 RSA암호의 예들을 살펴보았다. 특히 쉬운 예들을 살펴봄으로 암호에 대한 친근감을 높이고자 하였다. 그리고 RSA의 활용인 전자서명에 대해서도 살펴보았다.

RSA의 활용인 전자서명의 용도는 금융거래, 인터넷 민원서비스, 인터넷쇼핑, 그리고 인터넷뱅킹이나 온라인 주식거래에 필요한 공인인증서 등이 있다. 이러한 점을 미루어 보아 전자서명은 이제는 인터넷과 함께하는 우리들의 생활에 빠질 수 없는 부분이다. 인터넷의 생활화와 더불어 개인정보 보안의 중요성이 높아졌다. 이러한 것들을 생각했을 때에 인터넷 사용과 더불어 예측되는 어려움을 예방하기 위해 암호에 관한 연구가 더욱 활발히 이루어져야 할 것이다.

참 고 문 헌

[1] 박승안(2008) 암호학과 부호이론. 경문사.

[2] 박영수(2006) 암호 이야기. 북로드.

[3] 이민섭(2008) 현대암호학. 교우사.

[4] 원동호(2004) 현대암호학. 도서출판 그린.

[5] 김정헌(2002) 암호학 입문. 교우사.

[6] 이민섭(2007) 정수론과 암호학. 교우사.

[7] Masaaki Mitani, Shinichi Satou(2007) 만화로 쉽게 배우는 암호. 성안당.

[8] 김태호(2007) 이산수학을 통한 RSA 암호학. 경희대학교 교육대학원 석사학위논문.

[9] 정효정(2007) 정수에 관한 기본 개념과 정리를 활용한 암호체계. 동국대학교 교육대학원 석사학위논문.

[10] 김희원(2005) 암호학에 관한 연구. 신라대학교 교육대학원 석사학위논문.

[11] 류화정(2008) 정수론에 기초한 공개키 암호에 대한 연구. 신라대학교 교육대학원 석사학위논문.

[12] 이주행(2007) RSA공개암호 시스템과 제반 공격에 관한 연구. 인하대학교 교육대학원 석사학위논문.

[13] 김영설(2003) RSA기반 부인방지 대리서명. 서강대학교 대학원 석사학위논문.

[14] 조정제(2004) 공개키 암호에 대한 연구. 인제대학교 교육대학원 석사학위논문.

[15] 류춘열, 이경현, 박지환(2001) 암호 이야기. 동영출판사

저작물 이용 허락서

학 과	수학교육	학 번	20078205	과 정	석사
성 명	한글 : 김 경 아 한문 : 金 憬 兒 영문 : Kim Kyoung Ah				
주 소	서울특별시 은평구 대조동 205-2				
연락처	E-MAIL : ahsaja@naver.com				
논문제목	한글 : 암호학에관한 고찰 영어 : A Study of Cryptology				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의( ) 반대( )

2010년 6월 일

저작자: 김 경 아 (서명 또는 인)

조선대학교 총장 귀하