크립토 크리피를 이용한 정보의 보호 및 전달방법
-A method for data protection in communication on using cryptography-

최 진 탁*
신 승 호*
이 병 수**

Abstract

Because of the rapid growth of communicating with data and information. The protection of data which we want nowadays. This paper describes the various data securiconcentrated on adding senders signature with key to csecrecy, authenticity and ease of use.

1. 서 론

컴퓨터의 발달로 실제적인 정보처리 뿐만 아니라 저장된 정보를 보호할 수 있는 방법이 필요하게 되었다. 일반적으로 정보를 보호하는 문제는 먼저 정보자체의 접근을 통제하는 방법으로 흐름제어(Access control)에 대한 방법이 있다. 흐름제어 방법에는 사용자의 신원 또는 시스템의 특성을 고려해서 통제하는 방법으로 사용 통제행렬을 사용하는 것과 시스템 자체에서 각각의 독특한 암호를 부여하여 암호를 제시하는 자만이 사용할 수 있도록 하는 것이다. 사용 통제행렬은 실제적으로 적용할 때 사용자수가 많아지면 행렬의 크기가 과대해지므로 다른 방법을 적용 해야한다. 이를위해 모든 자원에 대해서 ACL(Access Control List)를 둔다. 이 리스트에는 자원의 인가된 사용자와 사용 방법이 주어진다. 사용통제 행렬이나 ACL은 보호될 자료가 직접 수록되어 있기 때문에 사용자의 암호나 시스템의 특성만 알고 있다면 누구든지 쉽게 내용의 진의를 파악할 수 있다는 단점이 있다. 이런 문제에서 탈피할 수 있는 방법은 자원자체의 사용은 통제하지않으나 내용자체를 암호화하여 사용자만이 그 내용의 진의를 파악할 수 있도록 보관하는 것이다.

이를 크립토 그라피(cryptography)라 한다. 본 연구에서는 비밀을 요하는 사항의 정보를 전송하거나 보관하는데 있어서 발송자가 key를 활용하여 자신의 싸인을 포함하여 암호화 해서 전송하고 이를 수신자가 받아 해독하는 크립토 그라피 알고리즘에 대하여 연구하였다.

2. 크립토 그라픽 시스템

(1) 크립토 그라피 과정

크립토그라피는 비밀사항의 내용을 작성하고 보관하는데 사용된다. 평문을 암호문으로 변명하는 과정을 암호화(encipherment 혹은 encryption)라 하고 반대로 암호문을 평문으로 변형하는 과정을 해독화(deciperment 혹은 decryption)라고 한다. 이 두 과정 모두가 다음 그림 1과 같이 어떤 특정한 키(key)값들에 의하여 결정이된다.

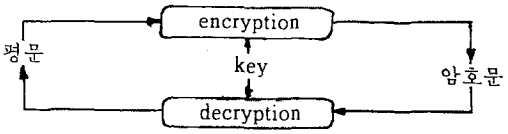

그림 1. 비밀문서

암호문의 작성에는 전위(transposition)과 치환(substitution)의 두가지 형태가 주워진다. 전위는 데이타 안에서 문자나 비트를 지정된 위치로 재배열하는 것이고 치환은 비트 문자 혹은 문자블럭을 임의 위치만큼 이동 시키거나 코드 형태로 대치하는 것이다. 또한 정보전달은 그림 2와 같이 메시지의 내용은 개방된 정보채널을 통하여 전송하고 키 값은 직접 인편으로

*인천대학교 전자계산학과 조교수
**인천대학교 전자계산학과 부교수
본논문은 1988년도 문교부 학술연구 조성비에 의하여 연구되었음.
접수 : 1989. 4. 15.

전하거나 개방되지 않은 다른 비밀 정보채널을 통하여 전송되어야 한다.

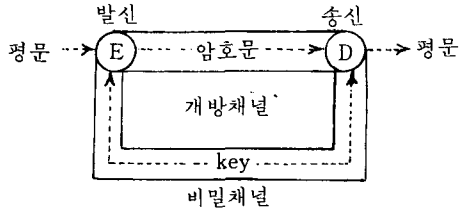

그림 2. 정보 전달채널

(2) 구성요소

크립토 그라픽 시스템은 그림 3과 같이 5개 성분으로 구성된다.

평문의 영역;M

암호문의 영역;C

Key 영역;K

암호문으로 변환(M−−>C);E_K

평문으로 변환(C−−>M);D_K

암호문으로의 변환 E_K는 모든 변환에 일반적인 암호와 알고리즘 (E)와 키(k) 값에 의해 정의되며 평문으로 D_K는 E_K의 역으로 정의된다.

$E_K(M)=C$

$D_K(C)=M$

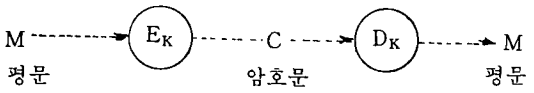

그림 3. 크립토 그라픽 시스템의 구성

크립토 시스템은 다음과 같이 3가지 조건을 만족해야 한다.

• 평문 <−> 암호문의 변환에 모든 키 들은 효율적 이어야 한다.

• 시스템을 사용하기가 쉬워야 한다.

• Key들은 비밀이 유지되고 알고리즘은 공개되어야 한다.

(3) 비밀유지

비밀유지(secrecy)는 암호해독가가 암호문의 정보를 입수 하더라도 평문으로 변환할 수 없는 것을 말하며 구성은 그림 4와 같다.

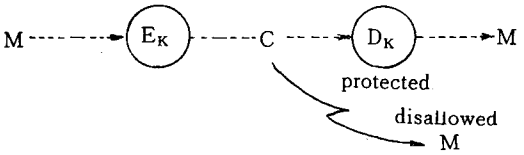

그림 4. 비밀유지의 구성

(4) 확실성

확실성(authenticity)은 메시지를 알고 있더라도 암호 변환방법을 모르면 암호해독가는 평문을 암호문으로 바꿀수가 없다. 그러므로 다른 메시지 M'을 C'로 변환하여 넣었을 때 D_K로 변환이 불가능한 것을 말하며 구성은 그림 5와 같다.

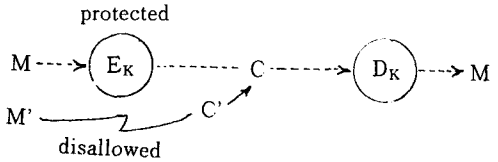

그림 5. 확실성의 구성

따라서 사용자들의 개인 화일을 단일 키를 사용하여 보호할 수 있다. 예를 들어 그림 6과 같이 사용자 A가 E_A, D_A를 호출할 수 없으면 사용자 A의 데이타 화일은 비밀이 보장되고 신뢰성이 있게 된다.

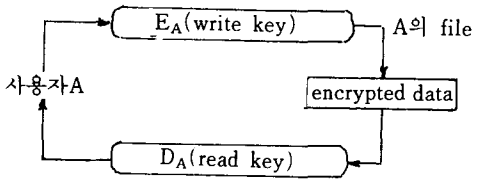

그림 6. 단일 키를 이용한 개인화일의 보호

3. 공동키 시스템

크립토 시스템에서 두개의 키 개념은 1976년 Diffie와 Hellman에 의해 소개되었으며 암호화의 새로 제안된 방법을 공통키 암호화 (public-key encryption) 라고 한다. 각 사용자는 공통의 키와 개인의 키 두개를 가지고 있으며 정보전달은 서로 공통의 키만을 가지고 사용할 수 있다. 공통키 시스템에서 사용자 A는 공통의 디렉토리에서 암호변환과정 E_A가 공통키이고 해독화 변환과정 D_A가 개인 키이다. 공통의 키 시스템에서 사용자 A가 사용자 B에게 메시지를 전달하면 A는 B의 공통키 E를 알고 있어야 한다. 그래서 사용자 A는 메시지 M을 암호화($E_B(M)$)해서 암호문 C로 사용자 B에게 보내는 것을 그림 7과 같이 비밀유지라한다.

$D_B(E_B(M))=D_B(C)=M$

또는 메시지 M이 사용자 A의 개인키를 가지고 변환되면 A는 B에게 암호문 $C=D_A(M)$을 보내므로서 B는 A의 공통키 E를 가지고 사용할 수 있게 된다. 이를 그림 8과 같이 확실성이라 한다.

$E_A(D_A(M))=E_A(C)=M$

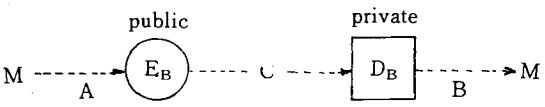

그림 7. 공동키 시스템에서의 비밀유지

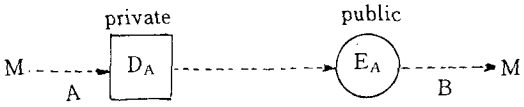

그림 8. 공동키 시스템에서의 확실성

위에서는 한 사람의 키를 사용하여 메시지를 전달하였지만 다음은 두 사람의 키를 이용하여 사용자 A가 메시지 M을 B에게 보내기를 원한다면 사용자 A는 메시지를 암호화하여 $E_B(D_A(M))=C$를 사용자 B에게 보낸다. 사용자 B는 받아서 해독하면 그림 9와 같이 $E_A(D_B(C))=E_A(D_B(D_A(M))))=M$이 된다.

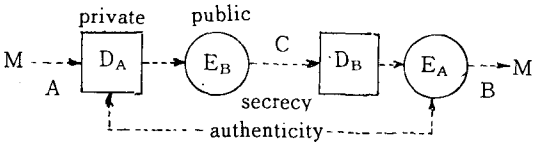

그림 9. 공동키 시스템에서의 비밀유지와 확실성

4. 암호화 알고리즘

(1) 전위 암호방호방법

이는 구조에 따라서 문자를 재정렬하는 것으로서 이는 기하학적인 도표로 만든 다음 다시 정리하여 표시하는 방법이다.

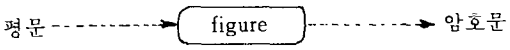

그림 10. 전위 암호과정

예를 들면 행렬의 열의 이용한 방법으로 평문 RENAISSANCE를 3행 4열로 만들면

1	2	3	4
R	E	N	A
I	S	S	A
N	C	E	

열의 순서 2−4−1−3으로 하면

평문 M=RENAISSANCE

암호문 C=ESCAARINNSE가 된다.

(2) 치환 암호방법

치환암호는 평문의 각 문자를 다른 문자로 대치하여 암호문으로 표기하는 것으로 이는 각 문자가 다음과 같이 1대 1 대응이 된다. 영문자 A−Z는 다음과 같이 대응된다.

M : ABCDEFGHIJKLMNOPQRSTUVWXYZ

C : QWERTYUIOPASDFGHJKLZXCVBNM

예를 들면 메시지

M=RENAISSANCE

이면 암호문은

C=KTFQOLLQFET

가 된다.

(3) 시저 암호(Caesar ciphers) 방법

어떤 문자의 코드의 값이 있다면 거기에 일정한 키 값을 더하여 만드는 것으로 영문자에서 key값이 3이면 A는 3번째 다음인 D가 된다. 즉

M =RENAISSANCE

$E_K(M)$=UHQDLVVDQFH

와 같이 된다.

(4) 동음자(Homophone) 치환방법

간단한 치환 암호법을 각문자가 1대 1 대응이지만 동음자 치환은 1대 다수 대응으로 어떠한 문자에 대하여 몇개의 대응되는 값이 있어 그중에서 하나를 선택하면 된다. 이 대응되는 수를 동음이라고도 한다. 예를들면

문자	대응숫자
A	17 19 34 41 56 60 67 83
⋮	⋮
L	03 44 76
M	08 22 53 65 88 90
N	02 09 15 27 32 40 59
O	01 11 23 28 42 54 70 80
P	33 91
⋮	⋮
T	05 10 20 29 45 58 64 78 99
⋮	⋮

M= P I L O T

C =33 08 76 28 78

(5) Vigenere and Beaufort 암호방법

시저 암호방법과 유사하지만 키 값이 고정되지 않고 한 단어를 키 값으로 하면서 메시지 값에 더하여준다. 예를들면

M = R E N A I S S A N C E

Key= B A N D B A N D B A N Key값은 BAND

1 0 13 3 1 0 13 3 1 0 13

$E_K(M)$= S E A D J S F D O C R

(6) polyalphabetic 암호치환방법

1대 1 대응이면서 각 문자에 대하여 고정적이지 않고 유동적이다. 그림 11과 같이 암호 디스크를 만들어 바깥원은 평문 안에 원이 대응되는 값이면서 회전이 가능하다.

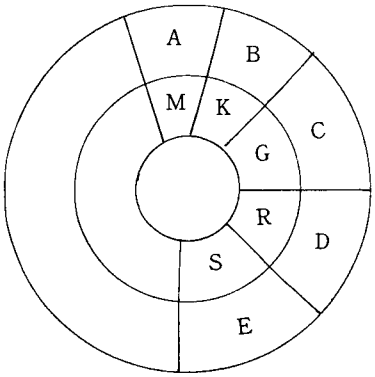

그림 11. 암호디스크

5. 효과적인 크립토 그라피 알고리즘 설계

(1) 지수를 이용한 암호

Pohling과 Hellman이 1978년 지수계산을 기초로한 암호 작성법을 발표하였고 같은 시기에 Rivest, shamir와 Adleman이 비슷한 알고리즘을 발표하였다. 위 두 가지 모두가 지수계산에 의하여 암호문을 작성한다.

$C=M^e \bmod n$

(e와 n은 암호화하는 key이다.)

M은 다시 C에다 평문화 하는 다른 key d를 지수연산에 사용하여 만든다.

$M=C^d \bmod n$

위의 지수계산을 빠른방법으로 하기 위하여 fastexp 라는 알고리즘을 사용한다.

C=fastexp(M, e, n)

M=fastexp(C, d, n)

n은 p와 q의 곱이고, p, q는 솟수이다.

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

$M^e \bmod n)^d \bmod n=M$

$M^{de} \bmod n \quad =M$

이러한 대칭 때문에 RSA scheme는 공통키 조직에서 비밀을 보장하고 확실하게 믿을 수 있는 것이다. 여기서 $\phi(n)$이 주어지면 (e, d)쌍을 구하기 쉽다.

Euclid s 알고리즘에 의하면

$e=inv(d, \phi(n))$

e, d는 대칭이므로 $d=inv(e, \phi(n))$,

$\phi(n)$과 e가 주어지면 d를 계산하기 쉽다.

(2) 디지탈 싸인을 첨가한 크립토 그라피 알고리즘 설계

1) 공통키 이용한 방법

메시지 M이 RENAISSANCE 일때 공통키를 이용하여 서로 변형하여 보자. p=53, q=61이고, d값을 791로 하면 $n=p*q=53*61=3233$, $\phi(n)=(p-1)(q-1)=52*60=3120$이 된다. 따라서 여기서 $\phi(n)$, d를 이용하여 $e=inv(d, \phi(n))=inv(791, 3120)=71$을 얻을 수 있다. A=00, B=01, C=02,……,Z=25, b=26이라고 가정하면

M=R E N A I S S A N C E B

17 04 13 00 08 18 18 00 13 02 04 26

두 문자씩 묶어서 C값을 구할 때 첫번째 RE 값을 계산해보면 M=1704이므로 $C=M \bmod n=1704 \bmod 3233=3106$ 이런 방법으로 전체를 계산하면 C=3106, 0100, 0931, 2691, 1984, 2927이 된다.

2) 한사람의 키만 이용한 방법

A와 B의 공동키 : E_A, nA, E_B, nB

A의 개인비밀 키 : dA

B의 개인비밀 키 : dB

일때, B가 비밀 사항의 내용을 보낼 경우를 생각하여 보자. B는 A의 공동키를 이용하여 $E_A(M)=M^{eA} \bmod nA=C$

A는 위의 암호 C를 받아서 A의 개인 키 dA를 이용하면

$D_A(C)=D_A(E_A(M))=M^{eAdA} \bmod nA=M$이 되고,

반대로 A가 자기의 키만 이용하여 B에게 보낼 경우

$D_A(M)=M^{dA} \bmod nA=C$

$E_A(C)=E_A(D_A(M))=M^{dAeA} \bmod nA=M$이 된다.

3) 디지탈 싸인을 첨가한 방법

상대방 한사람의 키를 사용하여 만든 암호문에 자기 개인 키를 추가하여 보낼 경우는 공통키만 이용할 경우 보다 더 복잡하지만 break 하는 데는 더욱 어렵다.

왜냐하면 여기서는 두사람 각자 개인 비밀의 키를 모두 사용하기 때문이다. A가 B에게 메시지 M을 보낼경우 $E_B(M)$ 보다 $E_B(D_A(M))$해서 보내는 경우가 A의 개인 디지탈 싸인인 dA가 포함되는 경우가 된다. 이 경우 만약 $C=E_B(D_A(M)$이고 $nA>nB$이면 C를 계산할 수 없다. 그러므로 nA, nB의 크기에 따라 달라지므로 $D_A(E_B(M))=C$로 바꾸어서 계산해야 한다. 또한 암호문 C에 추가로 key 값을 공통키를 이용하여 Ck로 변환하여 C와 Ck를 보내면 수신자 B는 암호문을 받아서 서로 약속에 의하여 C와 Ck의 값을 구분하여 평문으로 변환한다. 이때 수시로 키 값을 변경시킬 수 있는 장점이 있다.

(가) $nA<nB$일 경우

a. A가 B에게 메시지 M을 보낼때

$C=E_B(D_A(M))$

$=M^{eBdA} \bmod nA$

$M=E_A(D_B(C))=E_A(D_B(E_B(D_A(M))))$

$=C^{eAdB} \bmod nB$

b. B가 A에게 메시지 M을 보낼때

$C = E_A(D_B(M))$

$= M^{eAdB} \bmod nB$

$M = E_B(D_A(C)) = E_B(D_A(E_A(D_B(M))))$

$= C^{eBdA} \bmod nA$

c. 키값 전송

$Ck = Ek(Key)$

$Key = Dk(Ck)$

$C' = C + Ck$

$M' = M + Key$

(나) $nA > nB$일 경우

a. A가 B에게 메시지 M을 보낼때

$C = D_B(E_A(M))$

$= M_d^{AeB} \bmod nB$

$M = D_B(E_A(C))$

$= D^B(E_A(D_A(E_B(M))))$

$= C^{dBeA} \bmod nA$

b. B가 A에게 메시지 M을 보낼때

$C = D_B(E_A(M))$

$= M^{dBeA} \bmod nA$

```
FILENAME TO SAVE NORMAL SENTENCE
A
FILENAME TO SAVE NORMAL CODED SENTENCE
B
C=        172.0000000
C=        949.0000000
C=        914.0000000
C=         46.0000000
C=        286.0000000
C=        112.0000000
C=        210.0000000
C=        949.0000000
C=        837.0000000
C=         46.0000000
C=        667.0000000
C=        914.0000000
FILENAME TO SAVE CRYPTED SENTENCE
C
FILENAME TO SAVE CRYPTO PARAMETERS
D
Stop - Program terminated.
```

$M = D_A(E_B(C)) = D_A(E_B(D_B(E_A(M))))$

$= C^{dAeB} \bmod nB$

• 프로그램의 실예를 들면 다음과 같이 된다.

프로그램 실행의 예

```
  프로그램  실행의 예
==========================

     2      3      5      7     11
    13     17     19     23     29
    31     37     41     43     47
    53     59     61     67     71
    73     79     83     89     97
CHOOSE 2 NUMBERS (P,Q)
BUT  (P<Q)
TYPE P!
13
TYPE Q!
79


N=          1027
TYPE (N OR n), IF NOT SATISFIED !

LCM=          156
     5      7     11     17     19
    23     25     29     31     35
    37     41     43     47     49
    53     55     59     61     67
    71     73     77     79     83
    85     89     95     97    101
   103    107    109    113    115
   119    121    125    127    131
   133    137    139    145    149
   151    155      0      0      0
CHOOSE e!
TYPE e
29

 1 LINE  1 CHARACTER
TYPE  ~ ---> END
C
R
Y
P
T
O
G
R
A
P
H
Y
```

```
    TYPE  A
CRYPTOGRAPHY

    TYPE  B
     67      82      89      80      84      79      71      82      65      80      72      89

     P= 13   Q= 79


    TYPE C
     172     949     914      46     286     112     210     949     837      46     667     914

     P= 13   Q= 79


    TYPE  D

     I=   12     E=   29     N= 1027     LCM=  156


     P=   13     Q=   79
```

6. 결 론

정보화 시대에 각 정보의 보호가 점차 요구됨에 따라서 컴퓨터의 디스크 장치에 보관하고 있는 파일이나 상호간에 정보전달과정에 있어서 정보의 복사나 도청의 문제등이 있기 때문에 정보의 보호는 필연적이라고 할수 있다. 일반적으로 현재 정보의 보호는 ACL을 사용하여 사용자의 접근을 제한하는 방법이다. 이는 정보자체를 그대로 보관하고 있다는 문제점이 있다. 이를 교묘하게 dump나 copy에 의하여 침해될 수 있다.

본 논문에서는 정보를 얻더라도 사용할 수 없게 정보자체를 암호화하거나 전달하는 방법인 크립토그라피에 있어서 종래의 알고리즘을 알아보고 특히 공통키를 사용하는 문제에 있어 주로 한사람의 키를 사용하였지만 이보다 두사람의 키를 사용하므로서 외부 침입자로부터 해독을 더욱 방지할 수 있을 뿐만 아니라 정보의 전달과정때 디지탈 싸인을 해서 상대방에 전달하는 것과 똑같은 효과를 얻을 뿐만 아니라 매번 사용되는 키를 사용때마다 매번 바꿀 수가 있다. 이는 앞으로 두사람의 각자 개인 키로 정보의 보호가 요구되는 사항이나 군대에서 비밀취급에 있어 비밀 문서 전달과정에서 긴요하게 쓰일 수 있다고 볼 수 있다.

참 고 문 헌

1. Dorothy E. Denning, Cryptography and Data Security, Adison wesley publishing company (1982).
2. Dorothy E. Denning and Peter J. denning "Data Security" Computing Surveys Vol. 11, No. 3, Sep. 1979.
3. Robert Morris and Ken Thompson, "Password security", commu. ACNM, Vol. 22, No. 11, Nov. 1979.
4. R. L. Rivest, A. Shamir, and L. Adleman, "a method for obtaining digital signatures and public key cryptosystems", commu. ACM, Vol. 21, No. 2, Feb. 1978.
5. Dorothy e. Denning, "Secure personal computing in an insecure network", commu. ACM, Vol. 22, No. 8, Aug. 1979.
6. Leslie Lamport, "Password authentication with insecure communication", commu. ACM, Vol. 24, No. 11, Nov. 1981.
7. Gio Wiederhold, Database desion, Mcgraw-Hill, 1985.
8. Hamming, R. W., Coing and information theory, Prentice-hall, Englewood Cliffs, N.J.(1980).
9. Konheim, A. G., Cryptography, John Wiley and Song, N.Y.(1981).