論 文

RSA 公開키이 暗號方式의 擴張에 關한 硏究

正會員 李 智 永* 正會員 安 永 和** 正會員 尹 錫 昌***
正會員 元 東 豪**** 正會員 金 炳 贊*****

A Study on the Expansion of RSA Public Key Cryptosystem

Ji Yeong LEE*, Yeong Ha AN**, Suck Chang YUN***,
Dong Ho WON****, Byung Chan KIM***** *Regular Members*

要 約 本 硏究에서는 從來의 RSA 公開키이 暗號方式을 擴張한 새로운 RSA 公開키이暗號方式을 提案한다. 暗號化의 根本이 되는 法 파라메터 p, q를 擴張하여 乘算回數를 增加시켰다. 그 結果 暗號解讀에 要求되는 計算量이 增加되었으며, 整數論에 基礎를 둔 證明을 通하여 RSA公開키이 暗號의 強度를 改善할 수 있었다.

ABSTRACT In this paper a new RSA public-key cryptosystem which expands conventional RSA public-key cryptosystem is suggested. The number of multiplication times is increased by expanding the modulus parameters p, q which are the foundation of ciphering. As a result the amount of calculation which required in cryptoanalysis is increased, and we could improve strength of RSA public-key cryptography through a proof based on integral number theory.

I. 序 論

從來 秘密情報를 非保護 채널을 通하여 傳達할 때에 暗號化技法(Cryptography)을 使用하여 왔다[1]~[11]. 特히 外交文書의 傳達, 古代文書 解讀 등에 使用하던 暗號化技法은 最近 電子郵便, 데이타베이스및 綜合情報通信網 등에서 使用되고 있는 高價의 데이타를 不法使用하는 등 問題가 되고 있어 이를 防止하기 爲한 手段으로 注目을 받고 있다[1][2]. 서로 秘密리에情報를 交換할 수있는 權利를 最大한 保障하기 爲해 美國 商務省標準局은 暗號를 定量的으로 表示할 수 있는 方法을 公開募集하여 1977年 7月 15日 IBM에서 提案한 DES(Data Encryption Standard)를 秘密通信方法으로 採擇하였다[3]. 1978年에는 인텔 8094가 칩으로 生産됨에 따라 DES를 實際로 使用할 수 있게 되었다.

公開키이 暗號系는 RSA暗號系[4], Rabin 의 暗號系[5], Knapsack問題를 利用한 Merkle-Hellman 暗號系[6]와 Graham-Shamir 暗號系[7], 또한 線形誤差修正符號를 一般的으로 復號化하는데 問

*, **海軍士官學校 電子工學科
Dept. of Electronic Engineering R.O.K. Naval academic
***安養工業專門大學 電子計算學科
Dept. of Computer Science AN-YANG Jr. Technical College
****成均館大學校 工科大學 情報工學科
Dept. of information Engineering, Sung Kyun Kwan University Seoul 110, Korea.
*****成均館大學校 工科大學 電子工學科
Dept. of Electronic Engineering, Sung Kyun University Seoul 110, Korea.
論文番號 : 87-57(接受 1987. 7. 11)

題의 어려움이 있는 것을 利用한 McEliece 暗號系[8] 등이 提案되고 있다. 特히 Merkle-Hellman과 Rivest-Shamir-Adleman에 依해 提案된 RSA 暗號系는 가장 效率的인 公開키이 暗號系의 하나이다[4][6] 이 方法은 디지탈 署名이 可能하고 計量的인 安全度가 뛰어나 最近에도 有望한 公開키이 暗號方式으로 脚光을 받고 있다.

公開키이 暗號方式은 慣用暗號方式(conventional cryptography)과는 달리 暗號化키이를 公開하므로 키이 配送이 不必要한 方式이다. 이 方式은 각자가 暗號化키이에 對應하는 復號化키이를 求하고 復號化키이는 秘密리에 保管하도록 하며 각자의 暗號化키이는 公開한다. 第3者는 公開된 暗號化키이로부터 復號化키이를 求하는 것이 不可能하지만 暗號化키이 作成者는 暗號化키이로부터 復號化키이를 求할 수 있다.

本 論文에서는 從來의 RSA 公開키이 暗號方式을 擴張한 새로운 暗號方式을 提案하였다. RSA의 實際 應用面에서 $n=pq$이므로 制限된 素數로 n을 求할 때에 暗號加入者가 選擇해야 할 素數의 數가 制限되고 있으므로 n을 여러 개의 素數로 選擇한 경우 加入者가 얻을 수 있는 n값이 많아진다. 그러므로 暗號化의 根本이 되는 파라메터 p, q (但 p와 q는 素數)를 擴張하고 크기 調整이 可能한 n을 滿足할만하게 選擇한 後 그 證明을 通해 파라메터 抽出이 더욱 不可能하도록 試圖하였다. 結局 乘算回數가 늘어남에 따라 暗號解讀에 要求되는 計算量이 增大되었으며 이 計算量의 增大로 말미암아 RSA 公開키이 暗號의 強度를 改善할 수 있었다.

Ⅱ. 公開키이 暗號方式

DES를 包含한 從來의 慣用暗號方式에는 "키이 配送問題"의 어려움이 있다.

送信者 X는 暗號文을 傳送하기 前에 亂數列로부터 얻은 키이 e를 秘密通信을 願하는 特定受信者 Y에게 미리 傳達한 後 그 다음 그 키이를 使用하여 平文을 暗號文 C로 變換하여 受信者 Y에게 傳達한다. 受信者 Y는 送信者로부터 받은 키이를 使用하여 暗號文 C를 復號化하여 平文을 얻는다. 이와같이 慣用暗號方式은 키이를 미리 傳達해야 하는 不便함이 있다. 이것에 比해 公開키이 暗號方式은 키이配送이 不必要한 方法이다.

公開키이 暗號方式의 槪念을 說明하기 爲해 平文 M과 暗號文 C를 同一한 有限集合 T에 속한다고 하자. T^*를 T상의 全單射 全体로 하고 S와 K_E, K_D를 같은 크기의 有限集合으로 할 때 構造條件, 造作成條件 및 安全性條件을 滿足한다면 公開키이 暗號方式이 成立한다.

이때 全單射 $\psi: S \to K_E$
全單射 $\varphi: S \to K_D$
單 射 $E: K_E \to T^*$
單 射 $D: K_D \to T^*$

이 위 세가지 條件을 滿足하면 暗號系 $C=\langle T, S, K_E, K_D, \psi, \varphi, E, D\rangle$는 디지탈 署名도 可能한 公開키이 暗號系가 된다. 또한 위의 各 條件을 보면 다음과 같다.

Ⅱ-1. 構造條件

任意의 $k \in S$에 對해서 $D_{\varphi(k)} \cdot E_{\varphi(k)} = E_{\varphi(k)} \cdot D_{\varphi(k)} = I$ (項等事象)이 成立한다. 여기서 元 $e \in K_E$에 對해 E의 像을 E_e라고 表現한다. 이때 E_e는 T^*의 元이다. 또한 元 $d \in K_D$에 對해 D의 像을 D_d라고 表現한다. 이때 D_d는 T^*의 元이다.

Ⅱ-2. 造作性條件

暗號化 측면에서 보면 亂數列로부터 얻은 各 $e \in K_E$에 對해서 알고리즘 A_E를 通해서 暗號化 알고리즘 A_e를 만들면 暗號化 알고리즘 A_e는 E_e의 實際的인 알고리즘이다.

復號化 측면에서 보면 $d \in K_D$에 對해서 알고리즘 A_D를 通해서 復號化 알고리즘 A_d를 만들면 復號化 알고리즘 A_d는 D_d의 實際的인 알고리즘이다. 또한 任意의 $k \in S$에서 A_φ는 復號化키이 $d=\varphi(k)$를 만드는 過程의 알고리즘이며 A_ψ는 暗號化키이 $e=\psi(k)$를 만드는 過程의 알고리즘이다.

Ⅱ-3. 安全性條件

各 $e \in K_E$에 對해서 D_d $(d=\varphi\psi^{-1}(e))$의 알고

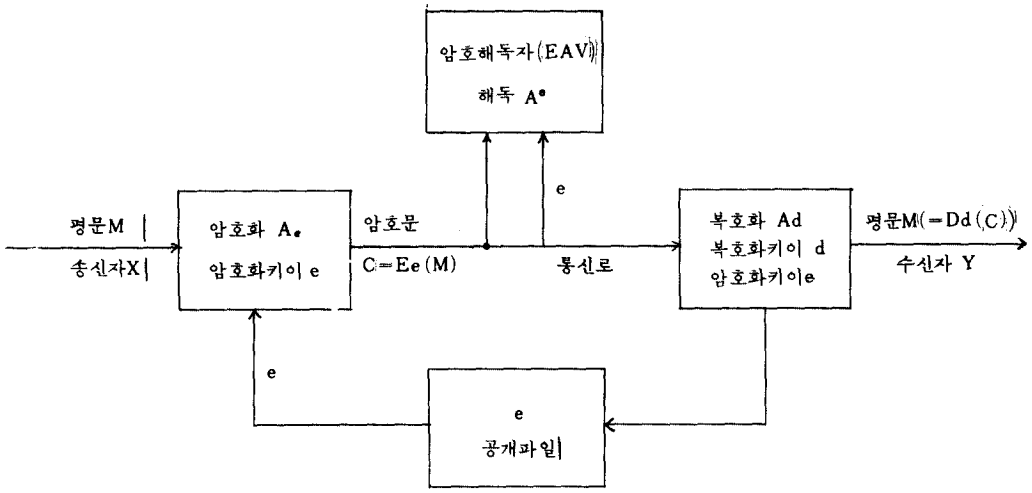


그림 1 공개키이 암호방식
Public key Cryptosystem.

리즘 A^e가 存在한다면 d를 使用하지 않고 A^e를 만들어내는 實際的인 알고리즘은 存在하지 않는다라고 말할 수 있다.

위의 세가지 條件中에서 (2)와 (3)에서의 "實際的"이라는 意味는 各 入力에 對해 出力을 計算하기 爲한 計算量이 充分히 작다는 것을 말한다 또한 條件(2), (3)에 對해서 計算量의 大小를 다루기 爲한 確認手段이 現在로는 없다. 그렇기 때문에 經驗的으로 (2)와 (3)을 滿足하는 暗號系를 생각할 수 있다. 暗號系와 그 暗號系의알고리즘은 다음의 그림 1에 圖示되어 있으며 이것이 公開키이 暗號方式이다.

正規受信者 Y는 자신에게 割當된 $k \in S$에서復號化키이 $d=\varphi(k)$와 暗號化키이 $e=\psi(k)$를 만들어 e는 公開파일에 登錄하고 d는 秘密리에 保管한다. 送信者 X가 受信者 Y에게 秘密通信을 하려고 할 때에, 公開파일에서 受信者 Y의 暗號化키이 e를 찾아 暗號化알고리즘 A_e에 依해 平文 $M \in T$을 暗號文 $C=E_e(M)$로 만들어서 通信路를 通해 傳送한다. 受信者 Y는 受信한暗號文 C를 A_d에 依한 平文 $M=D_d(D)$로 復號할 수 있다. M이 復元되는 것은 條件(1)에서 알 수 있다.

한편 暗號解讀者(EAV)는 中間에서 暗號文 C를 入手할 수 있고 또한 公開파일內에 있는 暗號化키이 e를 알 수 있지만 條件 (3)인 安全性條件에 依해서 平文 M은 事實상 復元이 不可能하다.

또한 送信者 X는 디지탈 署名이 可能하다. k′가 送信者 X用의 S의 元일때, 送信者 X는 平文 M을 復號化키이 $\varphi(k')$를 使用하여 $D_{\varphi(k')}(M)$을 만들 수 있다. 이 造作은 단지 送信者 X만이 可能하며 이것을 暗號化하여 보내면 受信者 Y는 자신의 復號化키이 $d=\varphi(k)$ (即 $D_{\varphi(k)}$를 使用)로 暗號文을 復號化한 後 다시 送信者의 公開키이로 暗號化하면 平文을 求할 수 있다. 그래서 이것이 送信者 X로 부터 온 것임을 알 수 있고 條件 (1)인 構造條件에서 保證되는 디지탈 署名原理이다. 即 安全한 暗號條件은 平文 M이 第三者에게 알려지지 않도록 通信하는 것이지만, 受信한 暗號文 C가 正當한 発信者로부터 送信된 것인가를 確認하는 過程이 디지탈 署名이다.

Ⅲ. RSA 公開키이 暗號方式

Ⅲ－1. RSA 暗號方式의 基本原理

i, K를 정의 정수로 하였을 때 i를 k로 나눈 나머지를 i mod k로 表現하자. RSA暗號方式 은 平文 $M(0 \leq M \leq n-1)$에 對해서 暗號文 C=

M^e mod n을 對應시킨 暗號法이다. 키이를 만들기 爲하여 우선 任意의 서로 다른 10^{100} 程度크기의 큰 素数를 選擇하고 그 두 素数의 곱을 法 파라메터 n이라 하자. 即,

$$n=p\times q \tag{1}$$

다음에 (p−1)과 (q−1)의 LCM L과 서로 素로서 이것보다 작은 任意의 정수를 暗號化키이 e라고 하자.

$$LCM\{(p-1),\ (q-1)\}=L \tag{2}$$

$$GCM(e,\ L)=1 \tag{3}$$

任意로 選擇한 e를 利用하여 다음 計算을 한다.

$$e\times d\equiv 1\ (\mathrm{mod}\ L) \tag{4}$$

即 mod L의 逆数인 $e\equiv d^{-1}\ (\mathrm{mod}\ L)$을 計算한다.

위의 過程에서 얻어진 暗號化키이는 (e, n)이고 復號化키이는 (n, d)이며 d는 秘密리에 保管한다. 여기서 d를 秘密리에 保管하였을 때 그 安全性이 威脅을 받지 않는 것은 e와 n으로부터 d를 求하는 節次가 거의 不可能하기 때문이다. 만일 d가 알려지면 第三者에 依해 RSA暗號는 쉽게 解讀된다. 이때 p, q가 알려지면 d를 求하는 것이 容易하다.

한편, n과 e自体만으로 RSA暗號文을 解讀하는 것은 一般的으로 n을 素因数分解하는 것과같은 程度의 時間이 必要한 것으로 알려져 있다. 即 RSA暗號方式은 이러한 因数分解의 어려움을 利用하여 trap door function을 實現, 暗號化하는 方式이다.

이상에서 說明한 바와 같이 公開키이暗號方式構成에서는 公開키이 暗號方式알고리즘 f, 暗號化키이 e, 復號化키이 d사이에는 다음과 같은 條件을 滿足해야한다.

a) 暗號化 計算 C=f(M, e)가 簡單해야 한다.

b) d가 미지인 경우 C, f, e로 부터 M을 얻을 수 없어야 한다.

c) f와 e로부터 d를 求할 수 없어야 한다.

d) 復號化 計算 $M=f^{-1}(c, d)$가 簡單해야 한다.

이때 a)−c)를 滿足하는 f를 一方向函数(one-way function)이라 하며 特히 d)를 滿足할 때 trap door function이라 한다.

暗號化 對象平文을 M, 暗號文을 C, 暗號키이를 e, d, n ($e\neq d$)라고 했을 때에 $0\leqq M\leqq n-1$을 滿足하는 平文 M의 暗號化, 復號化 過程은 다음과 같다.

$$C\equiv M^e\ (\mathrm{mod}\ n)\quad (暗號化) \tag{5}$$

$$M\equiv C^d\ (\mathrm{mod}\ n)\quad (復號化) \tag{6}$$

Ⅲ−2. RSA暗號方式의 擴張

이 節에서는 RSA 暗號方式의 擴張에 關하여 論述한다. RSA暗暗號方式의 擴張은 從來의RSA暗號方式과 같이 極秘의 데이타를 더욱 安全하게 傳送하는 데에 그 目的이 있다. 即 暗號通信에서 使用하는 키이 配送의 安全性을 考慮하여 여러개의 素数를 使用하는 方法이다. 여러가지 큰 素数의 곱에 起因한 法 파라메터 n은 커질수록 좋지만 큰 数의 素数는 量이 制限되어 있기 때문에 素数의 갯수가 늘어남에 따라 어려움도 增加하게 된다. 擴張 RSA暗號方式은 結局 여러개의 素数를 使用하여 暗號化키이 e의 값을 求하기가 더욱 어렵게 만든다. 即 素因数 分解의 어려움을 利用한 方式으로 이러한 暗號通信 方式은 어느 것이나 RSA 알고리즘에 따라서 행해진다. 結局 暗號計算은 더욱 複雜하여 지고 時間도 增加하게 된다. 물론 RSA暗號方式에서 처럼 서로 素인 두개의 큰 数의 곱과 크기가 비슷한 法 파라메터 n을 가지고도 充分히 計算을 複雜하게 만드는 效果를 가져온다.

우선 法 파라메터 n을 5個의 素数 p, q, r, s, t의 곱이라 하자. 그러면 擴張 RSA 알고리즘의 方法및 證明은 다음과 같다.

Ⅲ－2－1. 方　法

法 파라메터 $n = p \cdot q \cdot r \cdot s \cdot t$ (但 p, q, r, s, t는 서로 素) (7)

$$LCM(p-1, q-1, r-1, s-1, t-1) = L \quad (8)$$

$$GCD(e, L) = 1$$

$$e \times d \mod L = 1$$

Ⅲ－2－2. 提案된 알고리즘의 證明

여기서 $e \times d = aL + 1$

$$= ab(p-1) + 1 \quad (9)$$

$$= ac(q-1) + 1 \quad (10)$$

$$= ad(r-1) + 1 \quad (11)$$

$$= ae(s-1) + 1 \quad (12)$$

$$= af(t-1) + 1 \quad (13)$$

으로 쓸 수 있다.

따라서 式 (5)와 (6)에서 다음 式이 成立한다.

$$C^d = (M^e)^d = M^{e \cdot d}$$

$$C^d = (M^e)^d = M^{e \cdot d} \quad (14)$$

이 式 (14)에 式 (9)~(13)을 代入한다.

$$M^{ab(p-1)+1} \mod p = M$$

$$M^{ac(q-1)+1} \mod q = M$$

$$M^{ad(r-1)+1} \mod r = M$$

$$M^{ae(s-1)+1} \mod s = M$$

$$M^{af(t-1)+1} \mod t = M \text{ (Fermat 定理利用)}$$

이므로 $M^{e \cdot d} \equiv M \mod n (n = p \cdot q \cdot r \cdot s \cdot t)$ 임을 알 수 있다. (證明完了)

Ⅳ. 擴張 RSA의 計算量

Ⅳ－1. 復號手順

從來 RSA方法에서 $M \equiv C^d \pmod n$을 直接計算하지 않고 그 대신 改善된 擴張 RSA 方法은 中國人의 剩餘定理(Chinese remainder theorem)를 利用한다. 双마다 서로 素인 p, q, r, s, t에 對해 聯立合同式

$$M_1 \equiv C^d \pmod p$$

$$M_2 \equiv C^d \pmod q$$

$$\vdots$$

$$M_5 \equiv C^d \pmod t \text{ 는}$$

中國人의 剩餘定理에 依해 平文 $M (0 \leqq M < n)$이 一意的으로 求해진다.

簡單한 구체적인 例를 들어보자.

$p = 2$, $q = 3$, $r = 5$, $s = 7$, $t = 11$, $n = 2310$, $e = 7$, $M = 5$일 경우 暗號文 C는

$$C \equiv 5^7 = 1895 \pmod{2310}$$

가 된다. 다음 $L = LCM(1, 2, 4, 6, 10) = 60$으로부터 e의 역수, 復號化키이 $d = 43$을 얻을 수 있다. 이것을 C에 d 승하면 平文을 얻을 수있다.

$$M = C^{43} = (1895)^{43} \equiv 5 \pmod{2310}$$

위의 證明에서 알 수 있는 바와 같이 各各의 法 파라메터를 使用하였을 때도 마찬가지의 結果를 나타낸다.

Ⅳ－2. 從來의 RSA方式과 擴張 RSA 方式과의 計算量 比較

從來의 RSA方式을 使用하면 우선 M_1, M_2를 求한다. 서로 素인 p, q를 共通으로 2進 m비트라 하고 이것을 法으로 하는 乘算을 $2\log_2 d_i$ 回 ($d_i \equiv d \pmod{(p \text{ 또는 } q-1)}$) 행하면 된다. d_i도 약 m비트와 견주어 보면 乘算回數는 p, q에 對해 各各 2m回 된다. 同時에 4m回의 p, q를 法으로 하는 乘算이 必要하다. 다음 M을 求한다. 中國人 剩餘定理에 依해 式 (15)를 求할 수 있다.

$$M = M_1P + M_2Q \pmod{pq} \quad (15)$$

但, p, q는

$P \equiv 1 \pmod{p}$, $P \equiv 0 \pmod{q}$

$Q \equiv 1 \pmod{q}$, $Q \equiv 0 \pmod{p}$

을 滿足한다.

위의 p, q에서

$P = Q^{p-1}$

$Q = P^{q-1}$ 이다. (Fermat 定理)

이렇게 P, Q를 求해 놓고 任意의 M_1, M_2 (m비트)에 P, Q (2m비트)를 各各 곱해서 平文 M을 求한다. 이때 乘算回數는 2回이다.

擴張된 RSA 方法을 보면 우선 M_1, M_2, M_3, M_4, M_5를 求한다. 素數 p, q, r, s, t를 2進m′비트라 하면 이 素數를 法으로 하는 乘算은 10m′回 必要하다. 다음 M을 求한다. 이것 역시 從來의 RSA方法과 같이 平文 M이 求해지기 때문에 乘算回數는 5回면 된다. (中國人 剩餘定理使用)

$$M \equiv M_1P + M_2Q + M_3R + M_4S + M_5T \pmod{p \cdot q \cdot r \cdot s \cdot t}$$

即,

$P \equiv 1 \pmod{p}$,
$P \equiv 0 \pmod{q, r, s, t}$

$Q \equiv 1 \pmod{q}$,
$Q \equiv 0 \pmod{p, r, s, t}$

$R \equiv 1 \pmod{r}$,
$R \equiv 0 \pmod{p, q, s, t}$

$S \equiv 1 \pmod{s}$,
$S \equiv 0 \pmod{p, q, r, t}$

$T \equiv 1 \pmod{t}$,
$T \equiv 0 \pmod{p, q, r, s}$

표 1은 從來의 RSA 方式과 擴張된 RSA方式과의 乘算回數를 比較한 것이다.

표 1 RSA方式과 擴張된 RSA方式과의 乘算回數 比較
A comparison of the number of multiplication times between RSA and expanded RSA.

방식 \ 계산	Mi 계산	M계산
RSA	4m회 (p, q를 m비트로 가정)	2회
확장된RSA	10m′회 (p, q, r, s, t를 m′비트로가정)	5회

위의 過程에서 從來의 RSA暗號方式보다 本論文에서 提案한 擴張된 RSA暗號方式의 計算量이 훨씬 複雜하고 增大된 것을 알 수 있다.

V. 檢 討

從來의 RSA方法과 擴張 RSA方法의 計算量을 比較할 때, 從來의 RSA方式에서 法 파라메터 p, q를 各各 2進 300비트 程度(약 10^{100})로 한다. 또한 擴張RSA 方法에서 法 파라메터p, q, r, s, t를 各各 2進 120비트 程度로 取한다. 그러면 n비트數를 共히 600비트로 해서 比較한다. 그 結果 m : m′ = 300 : 120으로 하면 擴張 RSA의 計算量은 從來 RSA의 計算量의 $\frac{2}{5}$이면 족하다. 하지만 n이 두 소수의 곱인 경우와 여러 개의 素數의 곱일 경우 n의 비트數가 同一 하다고 假定할 경우에는 因數分解가 容易해지나 各各의 素數의 크기가 같다고 假定할 경우에는 여러개의 素數의 곱인 n이 計算量이 훨씬 많아진다. 이 두 方式에서 各 法 파라메터의 비트數를 同一하게한 計算量은 RSA가 600비트이고 擴張 RSA는1500비트가 되어 計算量은 擴張 RSA가 2.5倍 많다. 또한 n비트×n비트에서 n비트의 素數를 法으로 하는 乘算時間은 0 (n)로 한다. 이것은 n비트의 정수 乘·除算이 0 (n)로 行해지는 것에 依한다.

實際 暗號解讀을 爲한 計算에 있어서 平文의 길이를 n비트라 하면 平文의 種類는 2^n으로 有限個의 数가 되기 때문에 平文의 数가 적을 때 全部 平文으로 變換한 對應表를 만들면 簡單히 解讀讀할 수 있다. 그러나 平文의 길이가 100비트 정

도면 平文의 種類는 10^{33} 程度가 되므로 1秒에 10^{8}回 計算 可能한 高速 컴퓨터로 變換表를 만들려고해도 10^{14}年이 소요됨으로 事實상 實行 不可能하다. 그러나 複雜한 問題도 復號化키이를 알고 있는 受信者는 簡單히 暗號文 C로부터 平文 M을 求할 수 있다.

Ⅵ. 結 論

이 硏究에서는 서로 다른 5個의 큰 素數를 使用하여 暗號化키이를 求하는데 더욱 複雜한 過程을 거쳐야 함을 알 수 있었다. 結局 暗號解讀을 爲한 計算量의 增加로 말미암아 暗號의 強度를 改善할 수 있음을 알았다. 한편 n과 e 自体만으로 擴張 RSA 暗號文을 解讀하는 것은 n을素因数分解하는 것과 같은 程度로 難解하며 n의 行数가 아주 클 때 n을 素因数分解하는 것은 現在 알려져 있는 것중 가장 優秀한 알고리즘을 使用하여 풀어도 計算量이 多大하다. 또한 이 擴張된 RSA方法은 法파라메터 n이 몇 개의 素数의 곱인가를 알 수 없다. 따라서 n이 10^{200} 程度의 数라면 n과 e만으로 擴張된 RSA暗號文을 解讀하려면 새로운 高速의 因数分解 알고리즘이 開発되어야 할 것이다.

參 考 文 獻

(1) 一松信, "暗號の数理" pp. 126－144, 講談社.

(2) 廣瀬健, "暗號學と数學" セミナー, vol. 19, no. 8, pp. 6－14, Aug. 1982.

(3) Data Encryption Standard, Federal Information Processing Standard(FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC. Jan. 1977

(4) R.V. Rivest, A. Shamir and L. Adleman: "A Method for Obtaining Digital signatures and Public key Cryptosystem," Comm. ACM, 21, 2, pp. 120－126 1978.

(5) M. O. Rabin, "Probabilistic algorithms", In J. F. Tranb, Ed., Algorithms and Complexity, Academic Press, New York, pp. 21－40. 1976

(6) R.C. Merkle and M.E. Hellman, "Hiding information and signatures in trapdoor knapsacks," IEEE Trans Inform. Theory, vol. IT-24, pp. 524－530, Sept. 1978.

(7) A. Lempel, "Cryptology in transition", ACM Comput. surv. vol. 11. pp. 285－304 1979.

(8) R.J. McEliece, "A Public-key Crypto-system Based on Algebraic Coding Theory", Jet Propulsion Laboratory, California Institute of Technology, Pasadena, (A, DSN Progress Report, pp. 42－44, pp. 114－116, Jan－Feb. 1978.

(9) W. Diffie and M. Hellman, "New directions in cryptography", IEEE Trans. Inform. Theory, vol. IT－22, pp. 644－656. 1976.

(10) H.C. Williams, "A Modification of the RSA Public-key Encryption Procedure," IEEE Trans. Inform. Theory, vol. IT－26, no. 6, Nov. 1980.

(11) C. H. Meyer and S.M. Matyas, "Cryptography: A new dimension in computer data security", John Wiley & Sons, 1982.

(12) 高木貞治, "初等整数論講義第2版." 共立出版, 昭和60年.

李 智 永(Jie Young LEE) 正會員

1953年11月13日生

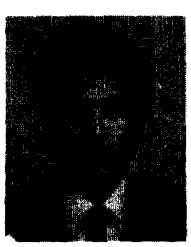
1983年 2月 : 成均館大學院 電子 工學科 卒業

1986月 2月 : 成均館大學院電子工學科博士課程 修了

1980年～1984年 2月 : Tandy Radio Shack 근무

1984年10月～現在 : 海軍士官學校 電子工學科 助教授

1988年成均館大學校 電子工學科 博士



安 永 和(Yeong Ha AN) 正會員

1952年 9月24日生

1971年 3月～1975年 2月 : 成均館大學校 電子工學科 卒業

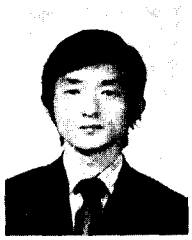
1975年 3月～1977年 2月 : 成均館大學校 大學院電氣工學科 (電子工學 專攻) 卒業

1985年 3月～現在 : 成均館大學校大學院 電子工學科(電子工學專攻) 博士課程

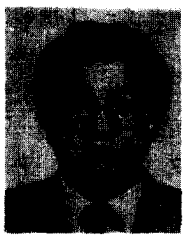
1975年 3月～1976年 2月 : 成均館大學校 電子工學科 教育助教

1977年11月～1981年 7月 : 空軍教育史令部 通信電子學校 教官

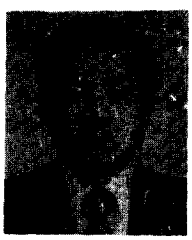
1983年 5月～現在 : 海軍士官學校 電子工學科 助教授



尹 錫 昌(Suck Chang YUN) 正會員
1953年 8月10日生
1971年：漢陽大學校 電子工科學 卒業
1976年：成均館大學校 電氣工學科(電子專攻) 碩士學位
1986年：成均館大學校 電子工學科 博士課程 修了
現在：安養工業專門大學電子計算學科助教授로 在職



元 東 豪(Dong Ho WON) 正會員
1949年 9月23日生
1976年 2月：成均館大學校 工科大學 電子工學科 卒業(工學士)
1978年 2月：成均館大學校 大學院 電子工學科 卒業(工學碩士)
1980年 3月：成均館大學校 大學院 電子工學科 博士課程 入學
1978年 3月～1980年 4月：韓國通信技術研究所 專任研究員
1985年 9月～1986年 8月：日本 東京工大 客員研究員
1982年 3月～現在：成均館大學校 副教授
1988年：成均館大學校電子工學科 博士



金 炳 贊(Byung Chan KIM) 正會員
1923年10月23日生
1947. 8：國立서울大學校 工學大學 電氣工學科 卒業
1955. 9～1966. 7：國立 慶北大學校 教授
1960 ～ 1962. 12：Denmark 原子力研究所 電子工學研究室에서 研究
1968. 7～1969. 6：Manchester理工大學(UMIST) 大學院에서 電子工學 研究
1966. 7～現在：成均館大學校 教授.
1983. 2～1987. 2：成均館大學校 副總長歷任