論文 83-20-5-2

컴퓨터 네트워크에서 多數 利用者를 위한 CP-暗號 시스템
(The CP-Cryptosystem for Multiuser in Computer Network)

李 尙 烈*, 朴 容 震**
(Sang Ryul Lee and Yong Jin Park)

要 約

컴퓨터 네트워크에 C-또는 P-暗號法을 導入함으로써 도청되기 쉬운 通信線上의 情報를 보호할 수 있다. 本 論文에서는 利用者가 많은 컴퓨터 네트워크에 이 두 暗號法을 同時에 導入하여 시스템 安全性이 높은 CP-暗號시스템을 提案하고 提示된 프로토콜에 의해 이 CP-暗號 시스템의 모든 利用者가 秘密通信 뿐 아니라 署名도 할 수 있음을 보여 준다.

Abstract

The use of conventional encryption algorithm or public-key encryption algorithm in existing computer networks can protect information on communication links which are subject to wiretapping. This paper presents the CP-cryptosystem of high system security by using both of these two algorithms in multiuser computer networks. It is proved by the protocols proposed in this paper that all of users in the CP-cryptosystem can not only communicate with others secretly but also affix their digital signature.

I. 序 論

데이타 通信의 발전으로 점차 컴퓨터 네트워크의 利用者가 增加함으로 인하여 現在의 "paper mail" 시스템은 "electronic mail" 시스템으로 轉換될 것이다. 이것이 実現化되기 위해서는 컴퓨터 네트워크의 利用者들의 通信內容을 保護할 수 있어야 하고 나아가 그 通信 內容에 署名을 할 수도 있어야 한다. 그 解決方法의 하나가 컴퓨터 네트워크에 暗號法을 導入하여 다음과 같은 두 가지 特性을 갖는 暗號 시스템을 構成하는 것이다.

①特定한 送信者가 보낸 情報를 特定한 受信者만이 받아 볼 수 있어야 한다.

②送信者가 作成한 變形된 情報 즉, 暗號文을 送信者外의 사람이 削除 또는 添加의 方法으로 捏造할 수 없어야 한다.

여기서의 暗號法에는 C-暗號法(conventional encryption algorithm)과 1976년 Diffe[2]에 의해 提示된 P-暗號法(public-key encryption algorithm)이 있는데, 送信者는 이를 利用하여 전달할 情報를 特定한 受信者外에는 알 수 없는 形態로 바꾸게 된다. 現在까지는 C-暗號法만을 導入한 C-暗號시스템(conventional cryptosystem)[1,5,9]과 P-暗號法만을 導入한 P-暗號시스템(public-key cryptosystem)[1,5,9]이 주로 提示되었고, 이 둘을 同時에 導入한 複合暗號시스템 즉, CP-暗號시스템(conventional and public-key cryptosystem)은 참고문헌[7]에서 약간 提示되었을 뿐이다.

從來의 C-暗號 시스템에서는 通信이 開設될 때마다 利用者들間에 새로운 키를 네트워크上의 어느 한 노드 또는 몇몇 노드에서 隱密히 分配해 주어야 하므로 그 特定 노드의 負擔이 컸었다. 그리고 P-暗號 시스템에서는 거기에 적용 가능한 P-暗號法을 發見하기

*準會員, 三星電子(株)
(Samsung Electronics Co., Ltd.)
**正會員, 漢陽大學校 工科大學 電子工學科
(Dept. of Elec. Eng., Han Yang Univ.)
接受日字 : 1983年 3月 24日

가 어려울 뿐더러 본질적으로 暗號化 時間이 많이 걸린다. 따라서 本 論文에서는 이러한 문제를 解決할 수 있는 새로운 CP-暗號 시스템을 構成하여 위의 두 가지 特性을 滿足시킬 수 있는 프로토콜을 提示하고 暗號 시스템의 安全性에 대해 考察하고자 한다.

Ⅱ. 두 가지 暗號法

暗號法이란 暗號文을 作成하고 解讀하는 方法을 말한다. 平文은 키와 함께 어떤 固定된 節次를 거쳐 暗號文으로 바뀌고(暗號文 作成), 暗號文 역시 키와 함께 어떤 固定된 節次를 거쳐 平文으로 바뀐다(暗號文 解讀). 여기서 어떤 固定된 節次는 代置方法, 位置交換方法, 代數的인 方法[9]으로 이루어 질 수 있다. 일반적으로 暗號 시스템의 모든 利用者가 이 節次를 알고 있다고 假定하기 때문에 暗號文의 作成과 解讀 여부는 키에 依存한다. 따라서 暗號文이 安全하려면 키 없이는 그 暗號文을 解讀할 수 없어야 한다.

C-暗號法의 特徵은 暗號文을 作成할 때 使用하는 키와 解讀할 때 使用하는 키가 같다. 그림1에서의 固定된 節次가 2진수로 表記된 두 入力 즉, 平文(또는 暗號文)과 키에 대해 順次的으로 exclusive-OR 演算을 거쳐 出力을 發生시킨다고 할 때, 만약 키가 無限한 길이의 랜덤數라면 키없이 暗號文으로부터 平文을 구해 내는 것은 거의 不可能하다.

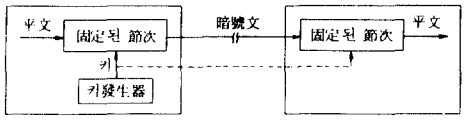

그림 1. C-暗號法의 情報 흐름

Fig. 1. Flow of information in conventional cryptosystem.

이러한 C-暗號法에서의 送信者는 暗號文을 作成할 때 使用한 키를 受信者에게 隱密한 方法으로 전달하여야 하는데, 키를 反復的으로 使用하지 않을 경우에 平文의 길이와 키의 길이가 같으므로 이러한 키를 受信者에게 隱密히 전달한다는 것은 經濟的으로나 時間的으로 낭비일 뿐이다. 따라서 이런 키를 直接 전달하는 대신 이 키를 發生시킬 수 있는 有限한 길이의 키(KS : key seed)를 전달한다. 有限 키로부터 無限 랜덤 키를 發生시키는 장치는 1977년 NBS에서 發表된 DES (data encryption standard)[3]를 使用하여 構成할 수 있다.[8] DES를 使用할 경우에 KS의 길이는 64 bits이므로 어떤 暗號文을 올바르게 解讀하기 위해서는 最大 2^{64}번까지 일일이 조사해 보는 도리밖에 없다. 따라서 키없이 어떤 暗號文을 올바르게 解讀하기란 現實的으로 不可能하다고 볼 수 있다. 平文(P) 이 키(KS)에 의해 暗號文(C)으로 바뀔 때 앞으로 $C=1\{P\}^{ks}$와 같은 式으로 表記한다.

P-暗號法의 特徵은 暗號文을 作成할 때 使用하는 키와 解讀할 때 使用하는 키가 다르다. 前者의 키는 모든 사람이 알고 있는 公開키로서 PK(public key)라 하고, 後者의 키는 自身만이 알고 있는 秘密키로써 SK(secret key)라 한다.

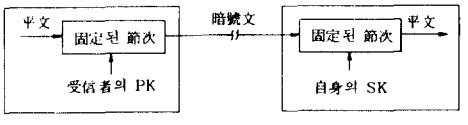

그림 2. P-暗號法의 情報흐름

Fig. 2. Flow of information in public-key cryptosystem.

그림 2에서 보는 바와 같이 P-暗號法에서는 隱密한 키 전달이 必要없다.

이를 위해 모든 利用者들은 PK와 SK가 1對1 對應關係에 있는 서로 다른 키쌍(PK, SK)을 미리 할당받아, SK는 自身이 隱密히 간직하고 PK는 모든 사람이 알 수 있도록 公開한다.

그렇게 하여 送信者는 受信者의 PK로써 전달하고자 하는 平文을 暗號化하여 보내고, 이를 받은 受信者는 自身의 SK로써 暗號文을 解讀하게 된다.

利用者가 많은 컴퓨터 네트워크에 이러한 P-暗號法을 導入하여 理想的인 P-暗號시스템을 実現시키기 위해서는 다음과 같은 네 가지 조건을 滿足시키는 키쌍(PK, SK)이 存在하여야 한다.

① $\{\{P\}^{PK}\}^{SK} = P$

② 쉽게 많이 發生시킬 수 있어야 한다.

③ PK로부터 SK를 演繹해 낼 수 없어야 한다.

④ $\{\{P\}^{SK}\}^{PK} = P$

일반적으로 P-暗號法은 C-暗號法보다 固定된 節次가 복잡하기 때문에 暗號化 速度가 느리다. 그러나 署名을 함에 있어서는 C-暗號法보다 P-暗號法을 利用하는 것이 有利하다.[5] P-暗號法의 네번째 키 조건은 署名을 容易하게 하기 위해서이다. 지금까지 알

려진 P-暗號法의 좋은 例로는 RSA 알고리즘[4] 이 있다.

Ⅲ. CP-暗號시스템 構成

C-暗號法 또는 P-暗號法을 컴퓨터 네트워크에 導入하여 暗號 시스템을 構成함으로써 모든 利用者들은 自身이 원하는 사람과 隱密히 情報를 交換할 수 있게 된다. 이 컴퓨터 네트워크에 C-暗號法만을 導入한 暗號시스템을 C-暗號시스템, P-暗號法만을 導入한 것을 P-暗號시스템, 그리고 C-暗號法과 P-暗號法을 同時에 導入한 것을 CP-暗號 시스템이라 한다.

從來의 可能한 세 가지 C-暗號시스템과 P-暗號시스템은 아래와 같다.[1,6]

C1-暗號시스템 : 모든 利用者들間에 固有의 키를 지정해 준다.

C2-暗號시스템 : 네트워크上의 隣接 노드間에 適用되는 키가 모두 다르다.

C3-暗號시스템 : 네트워크上의 어느 한 特定 노드가 키의 發生과 分配를 맡고 있고 모든 利用者들과 그 노드間에는 각기 다른 키를 지정해 준다.

P-暗號시스템 : 네트워크上의 어느 한 特定 노드가 모든 利用者들의 PK를 管理하고, 모든 利用者들은 그 노드의 PK를 알고 있다.

本 論文에서 새로이 提案하고자 하는 CP-暗號 시스템에서는 각 노드들은 다른 모든 노드들의 PK와 自身의 SK 그리고 隣接한 利用者들과의 C-暗號法을 위한 키(CK)를, 각 利用者들은 隣接한 노드와의 CK 그리고 그 노드의 PK를 갖고 있다. 그러한 狀況下에서 노드와 노드間은 P-暗號法을, 利用者와 利用者間은 C-暗號法을, 노드와 利用者間은 C-暗號法과 P-暗號法을 適用할 수 있게 된다. 그 適用方法은 Ⅳ章에, 適用理由는 Ⅴ章에 자세히 나타나 있다. 여기서 한 가지 注目할 사실은 CP-暗號시스템에 適用할 수 있는 P-暗號法의 범위가 P-暗號시스템에서 보다 넓다는 點이다. 왜냐하면 실제 네트워크에서는 노드 數가 利用者 數에 비하여 무척 적어 Ⅱ章에서 提示된 理想的인 P-暗號시스템이 実現되기 위한 키 조건 ①~④ 중에서 조건②가 緩和된 P-暗號法을 適用할 수 있기 때문이다.

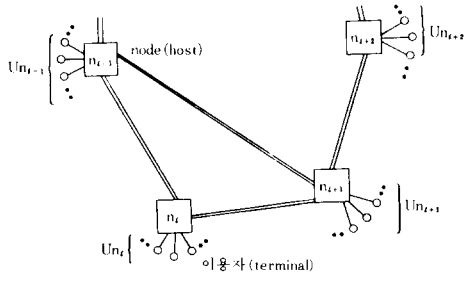

그림 3. 컴퓨터 네트워크의 例

Fig. 3. An example of computer networks.

그림 3과 같은 컴퓨터 네트워크上의 i번째 노드(host)가 n_i, 노드 n_i에 소속된 利用者(terminal) 數가 Un_i, 總 利用者數가 U, 總 노드數가 N일 때 표 1은 각 暗號시스템에서 노드와 利用者가 갖고 있는 키의 종류와 數를 나타낸다. 아직까지는 한 노드에 소속된 터미날 數가 많지 않으므로 네트워크上의 總 노드內에 간직되는 總 키數는 CP-暗號 시스템이 다른 暗號 시스템에 비하여 다소 많은 편이나 앞으로 이 터미날 數가 增加할 경우에 간직되는 總 키數는 C1-暗號 시스템을 除外하고는 각 暗號 시스템에서 대략 總 利用者數(U)가 되므로 키 保管을 위한 메모리 容量이 모두 비슷해진다. C1-暗號 시스템은 다른 暗號 시스템에 비하여 이러한 面에 있어서는 큰 長點을 갖고 있으나 다른 더 큰 短點을 갖고 있다. 이 短點에 대해서는 Ⅴ章에서 다룬다. 따라서 문제는 그 暗號 시스템이 Ⅰ章 ①, ②의 暗號 시스템이 갖추어야 할 特性을 갖고 있는가 또 어떤 偶發的인 事故에 대해 그 시스템이 얼마나 安全한가 이다. 이런 面에 대해서도 Ⅴ章에서 다룬다.

표 1. 노드와 利用者가 갖고 있는 키의 종류와 수

Table 1. The kinds and numbers of the key that are stored by the node and the user.

暗號시스템 \ 장소 \ 키종류			各(特定) node, 總 node			各利用者		
			PK	SK	CK	PK	SK	CK
CP		各	N-1	1	Un_i	1	0	1
		總	$U+N^2$					
P		特	U	1	0	1	1	0
		總	$U+1$					
C	1	各	0	0	0	0	0	U-1
		總	0					
	2	各	0	0	$Un_i+\alpha_{n_i}$	0	0	1
		總	$U+2\beta$					
	3	特	0	0	U	0	0	1
		總	U					

α_{n_i} : 노드 n_i에 隣接한 노드數

β : 隣接한 노드間 經路數 總合

Ⅳ. CP-暗號 시스템 프로토콜스

앞 章에서 構成한 CP-暗號시스템을 利用함으로써 願하는 사람들間의 秘密通信이 可能함과 同時에 그 通信 內容이 署名과 같은 效力을 낼 수 있음을 다음 프로토콜을 通하여 證明한다.

1. 秘密通信을 위한 프로토콜

秘密通信이라함은 이를테면 甲이 乙에게 "내일 만나자"란 말을 했을 때 甲과 乙 外에는 그 內容을 알 수 없는 경우를 말한다. 暗號 시스템에 使用되는 暗號法이 아무리 強力하다 하더라도 使用되는 키를 願치 않는 사람이 알고 있을 경우 秘密通信은 결코 이루어 질 수 없다. 따라서 秘密通信이 이루어지기 위한 必須的인 要件으로, 送信者는 키를 알고 있는 受信者의 身分을 確認할 수 있어야 하고 受信者 역시 키를 알고 있는 送信者의 身分을 確認할 수 있어야 한다.

CP-暗號 시스템에서는 送信者가 受信者에게 앞으로 双方間에 使用되어질 有限한 길이의 키(KS)를 決定하여 다음 프로토콜에 따라 전달하게 되는데, 그 전달되는 文이 다음과 같은 特性을 갖고 있다면 送受信者間의 身分確認이 이루어지게 되어 秘密通信이 可能해 진다.

①受信者만이 그 文을 理解할 수 있어야 한다.
(送信者가 受信者 身分 確認)

②送信者만이 그 文을 發生시킬 수 있어야 한다.
(受信者가 送信者 身分 確認)

通信 狀況에는 現在의 電話 시스템과 같이 送受信者가 서로 어떤 情報를 주고 받음으로써 이루어지는 双方通信과 郵便시스템과 같이 送信者가 一方的으로 受信者에게 어떤 情報를 보냄으로써 이루어지는 一方通信이 있다. 이 각각에 대한 프로토콜은 다음과 같다. 단, 프로토콜內에 전달되는 文은 秘密通信을 위해 꼭 必要한 최소한의 情報임을 알려 둔다.

1) 利用者 U_i가 利用者 U_j와 双方通信을 할 때 두 利用者間에 秘密通信이 이루어지기 위한 프로토콜

가) U_i가 노드 X 소속이고 U_j가 노드 Y 소속일 때

U_i는 노드 X의 固有번호(N_x)가 包含된 U_i 自身의 이름 또는 固有번호(N_i)를 平文으로 그리고 U_j의 N_j와 現在 時刻(T)을 노드 X와 U_i에게 할당된 키(CK_i)로써 暗號化하여 노드 X에게 보냄으로써, U_i는 노드 X에게 U_j가 소속된 노드의 PK 즉, PKY를 要請한다.

$$U_i \rightarrow X : N_i, \{T, N_j\}^{CK_i} \qquad (1)$$

여기서 N_i를 平文으로 보내는 理由는 노드 X가 CK_i를 찾아 내어 暗號文을 解讀할 수 있게 하기 위해서이다. 그리고 N_i를 숨기는 理由는 U_i가 U_j의 身分을 他人에게 알리지 않기 위해서 이다. 그리고 T를 包含시키는 理由는 此後의 응답들이 T時刻에 要請한 것에 대한 응답인지를 確認하기 위해서 이다.

正確性을 기하기 위해 모든 利用者들은 동기된 T를 使用한다. (1)의 文을 받은 노드 X는 U_i에게 PKY를 알려 주기 위하여 다음과 같은 文을 보낸다.

$$X \rightarrow U_i : \{T, N_j, \{PKY\}^{SKX}\}^{CK_i} \qquad (2)$$

이를 받은 U_i는 CK_i로써 暗號文을 解讀하여 T와 N_j를 보고서 나머지 暗號文의 內容이 T時刻에 U_j가 소속된 노드의 PK임을 알 수 있다. 따라서 U_i는 PKX로써 그 暗號文을 解讀하여 PKY를 알아 내게 된다. 여기서 각 노드들은 다른 노드들의 PK를 저장해 둘 때 自身의 SK로써 暗號化시켜 저장해 두면 (2)의 文을 發生시키는데 時間이 단축될 것이다. 따라서 그만큼 노드의 부담을 줄일 수 있다.

다음에 U_i는 앞으로 U_j와 通信할 때 使用하게 될 키(KS)를 自身이 任意로 決定하여 U_j에게 전달하는 過程에서 KS를 node Y만이 解讀할 수 있도록 PKY로써 KS를 暗號化한 後, 이 暗號文($\{KS\}^{PKY}$)을 노드 Y로 安全하게 전달하기 위하여 다음과 같은 文을 노드 X에게 보낸다.

$$U_i \rightarrow X : N_i, \{T, N_i, N_j, \{KS\}^{PKY}\}^{CK_i} \qquad (3)$$

(2)의 文에서 PKY를 구태여 SKX로 暗號化시켜 보내는 理由를 지금 설명할 수 있다. 이는 만약 어떤 공격자가 CK_i를 알아 낸다하더라도 SKX를 알지 못하면 自身이 바라는 $\{PKY'\}^{SKX}$를 發生시킬 수 없기에 SKY를 알고 있는 노드 Y만이 (3)의 文의 $\{KS\}^{PKY}$를 解讀할 수 있어 비록 공격자가 CK_i를 알고 있다하더라도 送信者인 U_i에게 U_j인척하며 나타날 수 없다는 잇점이 생기기 때문이다. 한편 (3)의 文에서 KS를 PKY로 暗號化시키는 理由는 노드 X에서도 KS를 解讀해 낼 수 없도록 하여 KS를 解讀해 낼 수 있는 곳의 범위를 최대한으로 줄이기 위해서이다. 그러므로 인해 KS의 누설 위험성을 줄일 수 있다.

지금까지 (1)~(3)을 通하여 CK_i가 누설되지 않았다는 전제下에서 각 暗號文의 發生과 解讀은 U_i와 노드 X만이 할 수 있으므로 U_i와 노드 X間에 双方 身分確認이 이루어진다.

(3)의 文을 받은 노드 X는 이 文의 內容을 노드 Y로 安全하게 전달하기 위하여 다음과 같은 文을 作成하여 보낸다.

$$X \rightarrow Y : \{N_x, \{T, N_i, N_j, \{KS\}^{PKY}\}^{SKX}\}^{PKY} \qquad (4)$$

이때 SKX, SKY가 누설되지 않았다는 전제下에서 (4)의 文의 $\{T, N_i, N_j, \}\{KS\}^{PKY}\}^{SKX}$를 노드 X만이 發生시킬 수 있고 (4)의 文을 노드 Y만이 解讀할 수 있기 때문에 노드 X와 노드 Y 間에 双方 身分確認이 이루어진다.

(4)의 文을 받은 노드 Y는 SKY로써 解讀하여 N_x에 따라 PKX를 찾아 내어 暗號文의 內容을 解讀하게 된다. 暗號文의 內容이 뜻하는 바는 "T時刻에 U_i가 U_j에게 KS를 전달하고자 한다." 따라서 노드 Y는 SKY로써 KS를 알아내어 노드 Y와 U 間에 할당된 CK_i로써 이 內容을 다음과 같이 暗號化하여 U_j에게 전달한다.

$$Y \rightarrow U_j : \{T, N_i, N_j, KS\}^{CK_j} \quad (5)$$

이를 받아 解讀한 U_j는 T時刻에 U_i가 自己와의 秘密通信을 위한 키(KS)를 지정하였음을 알게 된다. 이때 CK_j가 누설되지 않았다는 전제下에서 (5)의 文을 노드 Y와 受信者 U_j만이 發生, 解讀할 수 있기 때문에 노드 Y와 受信者 U_j 間에 双方身分確認이 이루어진다. 여기서 만일 T를 使用하지 않는다면 어떤 공격자가 비록 CK_j를 모르더라도 지난 번에 U_i가 U_j에게 보낸 (5)의 文에서 어떻게 하여 KS를 알아내면 이 KS를 알아낸 (5)의 文을 나중 어느 때고 node Y를 거치지 않고 직접 U_j에게 전달함으로써 공격자는 u_j에게 u_i인척하며 나타날 수 있다.

(1)~(5)에 의하여 U_i는 自身이 發生시킨 KS를 U_j만이 알아 낼 수 있다고 確認할 수 있고 U_j 또한 (5)의 文의 內容을 U_i만이 發生시킬 수 있다고 確認할 수 있기 때문에 送受信者間의 身分 確認이 이루어지게 된다.

그리고 전송시의 잘못으로 KS등에 變化가 있을 수 있으므로 이를 確認하기 위하여 U_j는 다음과 같은 文을 U_i에게 보낸다.

$$U_j \rightarrow U_j : \{T, N_i, N_j, KS\}^{KS} \quad (6)$$

이를 받은 U_i는 이 文의 內容이 自身이 보낸 것과 一致할 경우, 앞으로 보내고자 하는 情報를 KS로써 暗號化하여 보내기 시작함으로써 此後의 U_i와 U_j 間의 모든 通信은 秘密이 보장된다. 단, 양쪽 利用者와 노드들이 隱密히 간직해야 할 키가 노출되지 않아야 한다. 참고로 受信者 U_j가 소속된 노드의 PK 즉, PKY를 送信者 U_i가 알아야 하는 理由는 (3)에서 說明이 되었으나 各 利用者들이 다른 利用者들이 소속된 노드의 PK를 알고 있다면 U_i가 PKY를 알기 위한 (1), (2) 節次는 必要없다. 그러나 利用者와 노드가 많을 경우에 이러한 假定은 利用者들에게 많은 不便을 줄 것이다. 따라서 本 論文에서는 利用者들 自身이 소속된 노드에게 相対方이 소속된 노드의 PK를 要請하는 方式을 擇했다.

나) U_i와 U_j가 같은 node X 소속일 때

U_i는 애초에 PKY를 알고 있기 때문에 (1), (2) 節次는 必要하지 않으며, 노드間 (4)의 文을 交換할 必要도 없게 된다. 다만 U_i가 노드 X를 통하여 U_j에게 KS를 隱密히 전달함으로써 双方間의 身分 確認이 이루어진다.

$$U_i \rightarrow X : N_i, \{T, N_i, N_j, \{KS\}^{PKX}\}^{CK_i} \quad (3-a)$$
$$X \rightarrow U_j : \{T, N_i, N_j, KS\}^{CK_j} \quad (5-a)$$
$$U_j \rightarrow U_i : \{T, N_i, N_j, KS\}^{KS} \quad (6-a)$$

다) U_i와 U_j가 빈번히 秘密通信을 해야 하는 立場일 때

U_i와 U_j가 T時刻에 사용한 키(KS)를 隱密히 간직하고 있다고 假定할 때 U_i와 U_j 間의 双方 身分 確認은 훨씬 간단해진다. 이는 U_i가 U_j에게 T, N_i를 보냄으로써 시작된다. 이를 받은 U_j는 T時刻에 U_i와 通信할 때 사용한 키에 대한 暗號文 즉, $\{T, N_i, N_j, KS\}^{KS}$를 U_i에게 전달함으로써 双方間의 身分 確認이 이루어진다. 이때 U_i와 U_j가 같은 노드 소속이든 다른 노드 소속이든 관계없이 어떠한 노드에서도 暗號文을 作成하거나 解讀하는 일이 없다.

2) U_i가 U_j에게 一方的으로 情報(M)를 보내는 一方通信에서 秘密通信이 이루어지기 위한 프로토콜

U_i가 情報(M)를 U_j에게 보낼 때, U_j가 不在中이더라도 M은 安全하게 전달될 수 있다. 이는 U_i가 U_j에게 双方通信에서와 같은 프로토콜 (단, (6)은 除外)에 의해 KS를 安全하게 전달함과 同時에 U_i가 U_j에게 直接 $T, N_i, \{M\}^{KS}$를 보냄으로써 可能하다. 만약 U_j가 不在中에 여러 利用者들로부터 여러 개의 情報가 도착하였다면 U_j는 여러 개의 $\{T, N_i, N_j, KS\}^{CK_j}$과 $T, N_i, \{M\}^{KS}$에서 T, N_i가 서로 一致하는 KS로써 $\{M\}^{KS}$를 解讀하게 된다. 만일 T를 使用하지 않는다면 U_j가 不在中에 U_i로부터 키(KS)가 다른 여러 개의 情報가 도착하였을 경우에 U_j는 여러 개의 $\{N_i, N_j, KS\}^{CK_j}$과 $N_i, \{M\}^{KS}$에서 各 $\{M\}^{KS}$를 解讀하기 위한 KS를 찾는데 不便이 있다.

2. 署名을 위한 프로토콜

어떤 通信狀況에서 秘密通信이 成功的이 되더라도 解決되지 않는 문제가 있다. 이를테면 甲이 乙에게 "甲은 乙에게 200萬원을 支拂할 것을 약속한다"란 약속文을 前 프로토콜에 의해 暗號文으로 作成하여 보낼 경우 甲과 乙만이 이 약속 內容을 알 수 있을 것이다. 그러나 이때 乙이 200萬원을 500萬원으로 고칠 수 있

으므로 此後에 乙이 甲에게 支拂要請을 할 경우, 甲은 乙의 支拂要請을 거절할 수 있을 것이다.

그런데 만약 甲만이 이 약속文에 대한 暗號文을 作成할 수 있고 乙은 이 暗號文을 解讀할 수 있으되 造作된 暗號文을 作成할 수 없다면, 甲은 乙의 支拂要請에 응하지 않을 수 없게 될 것이다. 왜냐하면 甲은 自身의 약속文에 署名을 한 것이나 다름없기 때문이다.

어떤 文이 일반적인 署名文으로서의 效力을 발휘할 수 있기 위해서는, 署名者만이 그 文을 作成할 수 있어야 하고 署名者外 어느 누구도 그 文을 變造 또는 捏造할 수 없어야 한다. CP-暗號 시스템에서 노드 X 소속의 U_i가 노드 Y 소속의 U_j에게 이와 같은 效力있는 署名文을 보낼 수 있기 위한 프로토콜은 우선 (1)~(6)에 의해 U_i는 U_j에게 KS를 분명히 전달함으로써 시작된다. 다음 U_i는 署名할 文(M)을 決定하고 그 文에 대한 MV(message value)[5]를 어떤 함수 f (아직까지 구체적인 例는 없음)에 의해 계산하여 노드 X에 전달하게 된다. 이를 式으로 表現하면 다음과 같다.

$$MV = f(M)$$

여기서 MV는 署名할 文(M)에 의해 決定되는 값으로서, 같은 MV를 갖는 文이 결코 두 가지 이상 存在하여서는 안된다. 그리고 모든 利用者는 MV를 계산해 낼 수 있는 能力이 있다고 假定한다.

$$U_i \rightarrow X : N_i, \{T, MV\}^{CK_i} \qquad (7)$$

이를 받은 노드 X에서는 다음과 같은 署名源을 作成하여 U_i에게 보낸다.

$$X \rightarrow U_i : \{N_i, T, MV\}^{SKX} \qquad (8)$$

U_i만이 이와같은 署名源을 노드 X로 부터 받을 수 있다. 왜냐하면 CK_i를 알고 있는 U_i만이 (7)의 文을 作成할 수 있기 때문이다. U_i는 PKX로써 署名源을 解讀하여 內容을 確認한 後 署名할 文(M)과 署名源을 이미 지정된 KS로써 暗號化시켜 다음과 같은 署名文을 作成하여 U_j에게 보낸다.

$$U_i \rightarrow U_j : \{M, \{N_i, T, MV\}^{SKX}\}^{KS} \qquad (9)$$

이를 받은 U_j는 KS로써 解讀하여 M을 알아낸다. 그리고 이 M에 대한 MV′를 U_j 自身이 直接 계산해 낸다. 그리고 U_j는 署名源을 解讀하기 위하여 (1), (2)와 類似한 다음과 같은 節次로 노드 Y로 부터 PKX를 알아낸다. 단, U_i와 U_j가 같은 노드 소속이면 이 節次는 생략된다.

$$U_j \rightarrow Y : N_j, \{T, N_i\}^{CK_j} \qquad (10)$$

$$Y \rightarrow U_j : \{T, N_i, \{PKX\}^{SKY}\}^{CK_j} \qquad (11)$$

이렇게 하여 PKX를 알아낸 U_j는 署名源을 解讀하여 MV를 찾아낸다. 이 MV가 自身이 直接 구한 MV′와 一致하면 이 署名文속의 M은 U_i가 文書에 署名한 것과 같은 效力을 지니게 된다. 왜냐하면 署名源을 作成할 수 있는 사람은 U_i뿐이고 署名源속의 MV를 노드 X 外에는 누구도 바꿀 수 없기 때문이다. 따라서 만약 U_j가 M과 M에 合當한 署名源을 함께 갖고 있다면 U_i는 M의 內容에 대해 否認할 수 없다.

지금까지의 프로토콜에서 送受信者間의 秘密通信이 開設될 때까지 노드에서의 暗·復號 횟수는 CP-暗號 시스템이 從來의 C-暗號 시스템이나 P-暗號 시스템보다 많다. 그러나 이로 인한 노드 負擔이 다른 暗號 시스템에 비하여 絶対的으로 크지만은 않다. 이를테면 C2-暗號시스템에서는 送受信者間의 秘密通信이 開設된 後에도 전달되는 모든 情報를 노드에서 暗·復號를 해야 하지만 CP-시스템에서는 送受信者間의 秘密通信이 開設될 때까지 키(KS)에 관련되는 情報만을 노드에서 暗·復號하기 때문에 C2-暗號시스템보다는 훨씬 노드 負擔이 적다. 그리고 P-暗號시스템보다는 送受信者間의 秘密通信이 開設될 때까지의 暗·復號 횟수는 많으나 실제 이때 오가는 情報는 아주 적은 양이므로 노드 負擔이 P-暗號 시스템보다 월등히 크지는 않을 것이다. 오히려 이러한 短點보다는 P-暗號法이 C-暗號法보다 根本的으로 暗號化 速度가 느리므로 많은 양의 情報를 전달할 경우에 P-暗號法을 使用하는 것보다 C-暗號法을 使用하는 것이 有利하다는 側面에서 送受信者間의 秘密通信이 開設된 後에도 계속적으로 P-暗號法을 使用하는 P-暗號시스템보다 送受信者間의 秘密通信이 開設된 後에는 C-暗號法을 使用하는 CP-暗號 시스템이 暗號化 時間이 적게 걸리는 長點과 앞으로 V章에서 論議될 시스템 安全性面에서도 CP-暗號시스템이 높다는 長點이 더 많다.

V. CP-暗號시스템 安全性

시스템內에 隱密히 간직되어야 할 키가 고의로든 우발적으로든 노출되었을 때 시스템 전체의 安全性에 영향을 적게 미칠수록 暗號시스템 安全性이 높다. 우선 Ⅲ章에서 나타낸 從來의 세 가지 C-暗號시스템과 P-暗號시스템의 安全性을 考察한다. C1-暗號시스템은 그 어떤 暗號시스템보다 시스템 安全性이 높으나, 利用者가 U名일 때 各 利用者들이 隱密히 간직해야 할 키 数가 U-1개이므로, 利用者가 많을 경우 모든 利用者들은 多量의 키를 隱密히 저장할 장치를 갖

추어야 한다. 따라서 거기에 所要되는 費用은 엄청날 것이며 또 新規加入者는 既存 利用者들 모두에게 각기 다른 키를 隱密히 전달해야 하는 不便이 있어 사실상 C1-暗號시스템은 利用者가 많을 경우 実現不可能한 것이다. C2-暗號시스템은 C1-暗號시스템보다 키 分配는 쉬우나 通信經路上의 어느 한 부분이라도 파괴되면 그 通信은 安全性을 잃게 된다. C3-暗號시스템은 C1-暗號시스템과 C2-暗號 시스템을 改善한 것이나 키를 發生하고 分配하는 特定 노드의 파괴로 暗號시스템 전체의 安全性을 잃게 된다. P-暗號시스템 역시 PK를 管理하는 特定 노드의 파괴는 暗號시스템 전체의 安全性을 위태롭게 만든다.

그러면 지금부터 CP-暗號시스템內의 P-暗號法을 C-暗號法으로 代置시켰을 경우에 比較하면서 CP-暗號시스템 安全性을 考察한다. C-暗號法으로 代置시키기 위해 노드와 利用者間의 키는 그대로 두고 노드와 노드間에 C-暗號法을 위한 키(CK)를 지정해 준다. 실제 네트워크에서는 노드数가 利用者数에 비하여 아주 적으므로 실현 可能한 CK 지정方法은 다음과 같은 두 가지 경우가 있다.

① 隣接한 노드間에 모두 다른 키(CK)를 지정해 준다.

② 모든 可能한 노드双에 모두 다른 키(CK)를 지정해준다.

①의 경우를 CC1-暗號시스템, ②의 경우를 CC2-暗號시스템이라고 부르자.

만약 이러한 CC-暗號시스템에서 node間의 어느 한 키(CK)가 노출되거나 CP-暗號시스템에서 어느 한 노드의 SK가 노출될 경우의 시스템 安全性을 살펴보자. 단, 시스템 安全性을 考察함에 있어서 署名문제는 생각하지 않고 다만 秘密通信의 可能性만 타진한다. CC1-暗號 시스템에서는 노드間의 키가 노출된 經路를 지나는 通信은 安全性을 잃게 되기 때문에 결국 시스템 전체의 安全性은 없어진다. CC2-暗號시스템에서는 양쪽 노드에 소속된 利用者들間의 通信만 安全性을 잃게 된다. CP-暗號 시스템에서는 SK가 노출된 노드 소속의 利用者가 受信 立場이 될 경우의 通信은 (4)文의 발각으로 安全性을 잃게 되지만, 送信 立場이 될 경우의 通信은 노출된 SK를 直接的으로 利用하지 않기 때문에 安全하다.

그리고 만약 利用者와 노드間의 어느 한 키(CK)가 노출될 경우의 시스템 安全性을 살펴 보자. CC-暗號시스템에서는 그 利用者의 모든 通信은 安全性을 잃게 된다. 그러나 CP-暗號시스템에서는 그 利用者가 受信 立場이 될 경우의 通信은 (5)文의 발각으로 安全性을 잃게 되지만 送信 立場이 될 경우에는 (3)에서 自身이 發生시킨 KS는 결코 발각되지 않으므로 自身은 상대방을 確認하며 秘密通信을 할 수 있다. 그러나 (3)의 文에서 U_i가 아닌 者가 $\{KS'\}^{PK_Y}$를 造作하여 U_j에게 U_i인척하며 나타날 수 있기 때문에 受信者인 U_j는 送信者가 U임을 確信할 수 없다.

이상을 綜合해 보면 시스템內에 隱密히 간직되어야 할 키가 고의로든 우발적으로든 노출되었을 경우, 本論文에서 提案하는 CP-暗號시스템이 従來의 다른 暗號 시스템보다 시스템 安全性이 높음을 알 수 있다.

Ⅵ. 結 論

지금까지의 C-暗號시스템과 P-暗號시스템과는 달리 相互間 실제적인 情報 交換은 C-暗號法을 利用하고 키의 分配는 C-와 P-暗號法을 利用하는 CP-暗號시스템은 秘密通信이나 署名을 만족스럽게 할 수 있을 뿐 아니라, C-暗號法보다 暗號化 速度가 느린 P-暗號法을 利用하는 P-暗號 시스템보다 暗號化 時間이 적게 걸리고, 暗號 시스템의 부담(키의 發生과 分配 및 管理)을 모든 노드와 利用者들에게로 分散시킴으로써 特定 몇몇 노드에 集中된 C-또는 P-暗號시스템보다 시스템 安全性을 높일 수 있었다. 그리고 P-暗號法의 키 조건을 완화시킴으로써 P-暗號 시스템보다 多様한 CP-暗號시스템이 存在할 수 있음을 보였다.

參 考 文 献

[1] W. Diffe and M.E. Hellman, "Multiuser cryptographic techniques", *Proc. AFIPS 1976 NCC*, AFIPS Press, Montvale, N.J. pp. 109-112.

[2] W. Diffe and M.E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, IT-22, 6, pp. 644-654, Nov. 1976.

[3] Data Encryption Standard, *Federal Information Processing Standard (FIPS) Publication 46.*, National Bureau of Standard, U.S. Department of Commerce, Washington D.C. Jan. 1977.

[4] R. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signature and public-key cryptosystem," *Commun. ACM. 21*, 2, pp. 120-126, Feb. 1978.

[5] R.M. Needham and M.D. Schroeder, "Using encryption for authentication in large computer networks," *Commun. ACM, 21,* 12, pp. 993-999, Dec. 1978.

[6] C.S. Kline and G.J. Popek, "Public key vs. conventional key encryption," *Proc. AFIPS 1979 NCC*, vol. 48, AFIPS Press, Arlington, va., pp. 831-837.

[7] I. Ingemarsson and C.K. Wong, "Encryption and authentication in on-board processing sattellite communication systems," *IEEE Trans. Commun. COM-29,* 11, pp. 1684-1687, Nov. 1981.

[8] C.M. Campbell, "Design and specification of cryptographic capabilities," *IEEE Communications Society Magazine,* pp. 15-19, Nov. 1978.

[9] G.J. Simmons, "Symmetric and asymmetric encryption," *Comput. Surv. 11,* 4, pp. 305-330, Dec. 1979.