韓國通信情報保護學會誌
第1卷, 第1號, 1991. 4

暗號의 歷史的 考察

李 晩 榮*

1. 序 論

컴퓨터通信에 대한 要求와 需要가 擴大되어 감에 따라 近者에 이르기까지 軍事 및 外交分野에서만 利用되어 오던 暗號通信技法은 通信網을 통한 情報의 傳送과 데이타 貯藏裝置에서 情報의 收錄 및 貯藏시 第3者에 의해 盜聽당하거나 露出되는 것을 防止할 目的으로 商用通信(business communication), 個人間 通信(private communication) 또는 컴퓨터保安(computer security)分野에 까지 널리 適用되어 利用하고 있는 趨勢이다.

VLSI集積技術의 急速한 向上에 따른 컴퓨터 하드웨어 價格의 下落으로 컴퓨터 普及이 크게 늘어났으며, 通信網을 통한 數많은 컴퓨터와 端末器間의 相互連結로 綜合的 情報시스템構築이 實現되었다. 特히, 컴퓨터 데이타베이스(computer database)에 貯藏된 尨大한 情報를 分散處理함으로써 보다 效率的인 데이타의 利用이 實用化되었고, 이에 따른 컴퓨터間의 圓滑한 情報交換 및 流通을 達成하기 위한 要求가 急激히 擴散되고 있다.

이러한 컴퓨터通信 環境은 權限이 없는 他人(unauthorized person)이 通信中인 情報를 盜聽(eavesdropping or wiretapping)하여 데이타를 變造(modification), 挿入 혹은 添加(injection or addition), 또는 削除(deletion)하여 惡用하는 새로운 문제점을 惹起시키고 있다.

通信裝置, 通信線路 등으로 構成되는 通信網에서는 情報의 漏泄, 變造, 盜聽 등이 可能하며 이와 같은 不安全한 通信網을 통한 情報流通時 그 安全保護對策으로 唯一한 手段과 方法은 情報를 통한 暗號化(encryption)시키는 技法에 依存할 수 밖에 없다. 다시말해서 컴퓨터에 貯藏된 데이타 및 文書로 記錄된 情報나 地上通信回線, 마이크로波 施設 및 通信衛星을 통한 情報(音聲, 符號(data), 映像 등)를 盜聽 解讀으로부터 保護하고 變造를 防止하는 어떠한 措置가 切實히 要望되고 이에 對備한 가장 經濟的인 方法은 暗號通信에 依存하는 길밖에 없다는 것이다.

이와 같은 理由로 效率的인 暗號技法의 開發은 컴퓨터 通信網 또는 公衆電話通信網에서의 情報保護라는 側面에서 반드시 먼저 開發되어야 할 것이다.

軍事 및 行政電算網에서의 機密을 要하는 文書나 貯藏된 데이타를 通信하는 문제를 除外하더라도 機密維持를 위한 暗號應用分野를 列擧해 보면 다음과 같다. 文書認證(message authentication), 僞造할 수 없는 署名(digital signature), 巨額의 電子資金傳送(electronic funds transfer : EFT), 證券賣買情報, 自動金錢引出機(Automated Teller Machine : ATM)의 個人識別番號, 信用카드의 不當增額(credit card authorization), 個人의 人事카드 및 個人機密 情報의 惡用, 商去來 記錄의 僞造,

* 정회원, 漢陽大學校 名譽教授, 本 學會 會長

在庫量의 惡意的 變更, 醫療센터의 健康 및 患者 治療記錄, 法施行機關間의 逮捕令 및 前科記錄 등등 이와같은 數없이 많은 문제들을 保護한다는 側面에서 21世紀의 情報化 社會는 安全한 情報의 交換 및 處理가 무엇보다도 重要視 될 것이다. 따라서 活潑한 情報의 流通이 個人에 관한 情報의 露出로 인한 프라이버시 侵害문제, 國家 重要政策의 情報露出에 따른 安保上의 문제 그리고 情報變造와 破壞에 따른 우리社會의 混亂 및 經濟的 損失 등에 대해서도 對備策을 講究해야 할 時期가 왔다고 본다.

2. 歷史的 背景

一般的으로 暗號는 轉置暗號(transposition cipher), 換字暗號(substitution cipher) 및 合成暗號(product cipher) 등으로 分類된다. 最古의 暗號技法으로 알려져 있는 것이 紀元前 400年頃 希臘(Greeks)人들에 의해 使用된 Scytale暗號라 불리우는 轉置暗號인 것이다. 이 暗號는 通信文(message)의 文字를 再配置하는 技法으로 直徑이 一定한 棍棒에 papyrus(종이)를 감은 다음 message를 橫書한 後 종이를 풀면 通信文의 各 文字는 再 配置되어 完全히 秘化된다. 受信人은 같은 直徑의 棒에 이 通信文을 다시 감음으로써 message를 復元시키게 된다. 最初의 換字暗號는 Julius Caesar 暗號이다. 이것은 通信文(message) 또는 平文(plaintext)의 各 文字를 左側으로 3文字씩 移動시켜 그 位置에 對應하는 다른 文字로 置換함으로써 平文을 暗號文(ciphertext or cryptogram)으로 暗號化한다. 復號해서 平文을 얻기 위해서는 單純히 暗號文을 逆處理하면 된다. 合成暗號는 轉置暗號와 換字暗號法을 適當히 組合한 暗號로서 一例로 1914年 第1次 世界大戰中 獨逸陸軍에 의해 使用된 ADFGVX 暗號를 들 수 있다.

第2次 世界大戰 勃發로 强大國들은 暗號研究와 그 技法 알고리즘 開發에 의해 軍事通信을 위한 强力한 알고리즘 確保에 血眼이 되었다. 勿論 換字와 轉置를 交代로 處理하는 合成暗號(product cipher)를 使用했던 것이다. 그 後 1945年 終戰과 더불어 디지탈 컴퓨터 開發이 本格化되었고 1960年代末부터는 大規模 集積回路(LSI) 技術 開發에 힘입어 대단히 複雜한 暗號 알고리즘을 한個의 chip안에 收容可能케 함으로써 高速暗號處理能力이 實現化된 것이다.

우리가 經驗한 걸프 戰爭이 短期에 끝난 것은 美空軍의 猛爆으로 이라크 空軍과 軍施設은 勿論 作戰遂行上 中樞神經格인 C^3(command, control and communications)를 完全 破壞한 結果라 하겠다. 그러나 여기서 한가지 追加하고 싶은 것은 多國籍軍側의 暗號通信을 들을 수 있을 것이다. 歷史的으로 1914年 第1次 世界大戰時 獨蘇宣戰布告로 蘇軍은 레넨캄푸將軍揮下의 第1軍 10萬 兵力과 쌈스노프將軍이 이끄는 第2軍 10萬 都合 20萬大軍이 西下해 내려오고 獨逸軍은 힌덴부르크將軍指揮下에 15萬 大軍이 東北上하여 對峙狀態에 있었다. 그런데 蘇 1軍의 兵站補給 困難으로 더 以上 進軍이 困難해지자 蘇 2軍에 再補給이 實現될 때까지는 前進하지 말것을 暗號文으로 打電해 왔다. 그런데 獨逸軍 無線諜報部隊가 蘇軍의 交信을 解讀한 다음 蘇 2軍에게 蘇 1軍쪽으로 移動해 달라는 支援要請의 內容을 暗號文으로 變造하여 打電한 것이다. 그 結果 蘇 2軍을 단데베루히로 誘導, 8月 26日부터 30日까지 5日間의 戰鬪에서 蘇 2軍 10萬 兵力이 全滅당하였고 이는 獨逸軍의 通信情報의 偉大한 成果라 하겠다. 第2次 世界大戰時 日本聯合艦隊司令長官 山本 八十六 提督의 搭乘機가 太平洋 라 바울에서 擊墜 당한 것도 日本의 Purple 暗號가 美國의 Sigaba暗號보다 弱해 손쉽게 解讀당함으로써 빚어진 悲劇이다. 또 하나 興味있는 일은 1970年代 蘇聯의 無人人工衛星이 달에 着陸하여 搭載한 高速카메라로 찍은 寫眞을 映像處理해서 테레메트리(telemetry)로 地上地球局으로 傳送하는 것을 英國電子天文臺에서 榜受하고 再生하여 달 表面의 形態를 發表한 일이 있었다. 그러나 蘇聯의 祕密은 映像再生의 縱橫比인데 英國은 그 比를 任意로 取했기 때문에 發表한 것이 웃음거리가 되고 만 것이다. 이와 같이 暗號技術은 앞에서 記述한 軍事, 外交, 科學과 같은 國家運命을 左右하는 分野에서 뿐 만 아니라 이제는 金融, 企業, 社會,

個人 全般에 걸쳐 그 重要性이 크게 擴散되고 있다. 따라서 情報保護側面에서 暗號學 關聯分野의 硏究는 必然的이며 반드시 活性化되어야 할 것이다.

3. 暗號의 基礎槪念

暗號시스템은 컴퓨터 및 通信시스템에서 情報의 秘密保障과 認證(authentication)을 提供할 目的으로 使用된다. 이러한 暗號시스템에는 크게 對稱形과 非對稱形으로 나누어 진다. 暗號化 알고리즘이란 平文(plaintext)을 키(key)를 利用하여 暗號文으로 變換시키는 것을 말하고, 復號化 알고리즘이란 원래의 平文을 復元시키기 위한 技法이다. 暗號化 및 復號化 키는 使用되는 暗號시스템의 種類에 따라 同一할 수도 있고 그렇지 않을 수도 있다. 對稱暗號시스템은 單一키 暗號시스템, 또는 同期暗號시스템이라고 하는데 暗號化 키와 復號化 키가 原則的으로 同一하다. 勿論 이러한 키는 반드시 秘密이 維持되어야 한다. 對稱暗號시스템의 경우 使用되는 키의 가지수는 一般的으로 n名의 使用者(user)에 대해 $n(n-1)/2$個의 키가 必要하다. 例를 들어, DES(Data Encryption Standard)와 Rotor 暗號器가 對稱暗號시스템에 속한다. 非對稱暗號시스템에서는 두개의 다른 키가 使用되는데, 暗號化에 使用되는 키는 公開시키는 反面에 復號化에 使用하는 다른 키는 秘密로 한다. 모든 公開 키(public key) 暗號시스템(例, RSA方式)은 非對稱暗號시스템에 속한다.

盜聽(eavesdropping or wiretapping)이란 權限外의 個人 또는 集團에 의해 通信채널을 監聽함으로써 情報 데이타를 가로채는 것을 말한다. 만일 盜聽을 하려는 第3者(opponent)가 傳送되는 情報를 盜聽하거나 記錄하면 이를 消極的, 또는 單純攻擊(passive attack)이라 하고, 通信채널을 通해 傳送되는 情報 데이타를 變造(modify) 또는 挿入(inject)한다면 積極攻擊(active attack)이라 한다. 盜聽者가 키에 대한 知識없이 暗號文을 復號(즉, 暗號의 破壞)하려는 어떠한 試圖를 暗號解讀(cryptanalysis)이라 한다. 解讀可能한 暗號器는 平文 또는 키 決定이 可能하거나 限定된 計算資料를 利用하여 暗號文으로 부터 平文과 키 모두의 決定이 可能한 것을 말한다.

暗號化 및 復號化 演算은 一般的으로

$$Y = E_{K_E}(X) \qquad \text{(暗號化)}$$

$$X = D_{K_D}(Y) \qquad \text{(復號化)}$$

으로 表現되고, 여기서 X는 平文, Y는 暗號文, 그리고 K_E와 K_D는 各各 暗號化 키와 復號化 키를 表示한다. 그림 1은 暗號시스템에서의 情報흐름을 說明한 것이다.

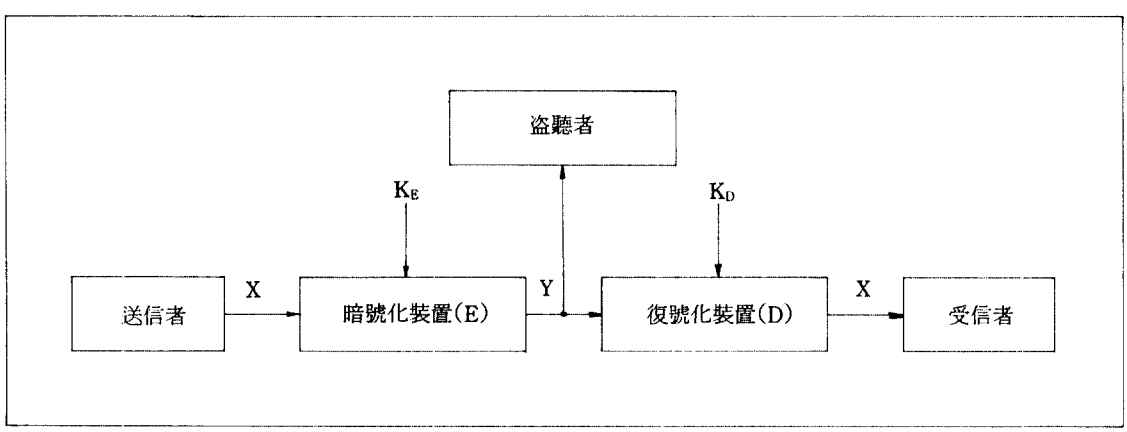


그림 1. 暗號시스템의 一般型

4. 暗號의 種類

暗號의 種類는 暗號化 方法에 따라 祕密키 暗號(private-key cryptosystems)와 公開키 暗號(public-key cryptosystems)로 大別된다. 여기서 祕密키 暗號는 平文(plaintext)의 暗號化 方法에 따라 다시 블럭暗號(block cipher)와 스트림暗號(stream cipher)로 細分된다. 祕密키 暗號方式은 暗號化 키(enciphering key)와 復號化 키(deciphering key)가 同一하며 이 두 키는 送信者와 受信者가 共用하는 祕密키(secret key)가 된다. 따라서 祕密키 暗號시스템을 때로는 對稱暗號시스템(symmetric cipher systems)이라고도 부른다. 한편, 公開키 暗號는 暗號化 키와 復號化 키가 서로 다르며 暗號化 키는 公開하나 復號化 키는 祕密로 保管하는 것이 普通이다. 이런 公開키 暗號시스템을 非對稱 暗號시스템(asymmetric cryptosystems)이라고도 부른다. 兩暗號方式을 比較해 보면 (1) 祕密키 暗號시스템은 祕密키의 配分이 必要하므로 이에 따른 保管問題가 어렵고 暗號化 速度가 高速이라는 長點을 가지나 完全한 認證(authentication)이 困難하다는 短點이 있다. 스트림暗號는 主로 外交 軍事用으로 使用되고 블럭 暗號는 商業用으로 汎用되고 있다. 한편, (2) 公開키 暗號는 祕密키의 分配가 不必要한 反面 暗號化 速度가 低速인 短點이 있으나 認證手順은 매우 容易하다. 따라서 公開키 暗號는 公衆通信網用에 適合하다.

블럭暗號는 平文을 一定 길이의 블럭(blocks)으로 分割해서 블럭마다 同一키(same key)를 使用하여 暗號化한다. 平文과 暗號文의 길이는 같으므로 暗號文이 平文보다 짧은 境遇에는 復號가 不可能하게 된다. 合成暗號를 構成하기 위한 블럭暗號는 換字(substitution), 互換(permutation) 및 加算(addition) 등의 演算을 施行하는 여러 單位暗號器를 連鎖結合시킴으로써 可能하다. 이러한 블럭 暗號시스템의 例로서는 Hill暗號와 DES(Data Encryption Standard) 등을 들 수 있다.

한편, 스트림(逐字)暗號는 같은 길이의 키 數列(key-bit sequence)과 平文을 비트單位(bit-by-bit)로 暗號化해서 똑같은 길이의 暗號文을 만든다. 그러나 同一한 平文일지라도 키 數列에 따라 判異한 暗號文이 生成된다. 週期性을 保有한 LFSR(linear feedback shift register)을 키 發生器로 使用하는 경우 週期 스트림 暗號시스템이라 부르는데 이러한 暗號시스템의 例로는 Hagelin 暗號器와 Rotor 暗號器를 들 수 있다. 反面에 非週期 스트림 暗號시스템에는 Vernam 暗號器와 其他 設定키(非週期키) 暗號器를 들 수 있다.

Poligram暗號는 여러개의 비트(bit) 또는 심볼(symbol)을 單一키로 一時에 暗號化하는 것으로 2-gram 換字暗號方式인 Playfair暗號, 그리고 N-gram 換字暗號方式인 Hill暗號 등을 들 수 있다. Caesar暗號는 固定키 單一文字換字暗號(monoalphabetical substitution cipher)이다. Caesar暗號는 使用이 簡便하기 때문에 專門家가 아닌 사람도 쉽게 取扱할 수 있으므로 密輸團이나 間諜 등이 愛用하며 간단한 외교용 암호로도 使用可能하다. 또한, 이 暗號는 日記, 戀愛便紙 등 個人의 프라이버시를 保全하는 데도 便利할 것이다. Homphonic cipher의 一種으로 Beale 暗號를 들 수 있다. Vigenere 或은 Beaufort 暗號는 週期性을 지닌 多文字換字暗號(polyalphabetic substitution ciphers)들이다. 그러나 Kasiski方法을 使用하면 解讀이 可能해서 쉽게 깨질 수 있다. 相當히 긴 週期를 갖는 키 數列이 生成하는 多文字暗號器에는 Hagelin暗號器(M-209)가 있으며, 또 第2次 世界大戰時 使用했던 Rotor暗號器를 들 수 있다. 이 Rotor暗號器에는 英國의 Typex, 美國의 Sigaba(M-134), 獨逸의 Enigma, 日本의 Purple 등이 이에 屬하는데 週期는 길다 하더라도 無作爲性이 없다는 缺陷 때문에 解讀이 可能해서 2次 大戰當時 往往 깨지는 수가 있었다. 또한 換字暗號에 屬하는 重要한 暗號의 하나는 one-time-pads이다. 키(key)의 特性으로 無作爲性(randomness)과 反復이 없는 無週期 때문에 理論的으로는 暗號文을 盜聽하더라도 平文이나 키를 決定할 만한 端緖를 잡을 수 없기 때문에 堅固한 暗號이다. 그러나 사용키는 한번 쓰면 버려야 하므로 實用性이 없다.

合成暗號(product cipher)는 둘 또는 그 이상의

暗號를 合成시킨 것으로 最初의 것은 第1次 世界大戰時 獨逸의 ADFGVS暗號를 들 수 있다. 그리고 IBM이 提案한 DES(Data Encryption Standard)는 美國商務省標準局(National Bureau of Standards : NBS)이 1977年에 公式暗號알고리즘으로 採擇하였는데 이 알고리즘은 美國의 標準으로 制定되었다. DES는 64 비트의 平文(plaintex)과 56 비트의 키(key)가 置換과 順列의 組合으로 16段을 거친 代表的인 블럭暗號이다. DES는 現在 美國에서 31個의 會社와 日本의 富士通이 製品으로 生産하고 있으며 金融機關에서 主로 使用하고 있다. 日本의 FEAL(Fast Data Encipherment Algorithm)은 1988年頃 NTT가 開發한 暗號器로서 DES를 模倣하여 改良한 暗號化 速度를 高速化시킨 것이라 한다. 日本 NTT는 이 暗號를 完全히 解讀하는 個人이나 團體에게 賞金 1,000,000 yen을 걸고 1991年 8月 31日까지 時限附로 應募를 기다리고 있다. 美國의 國家保安廳(National Security Agency : NSA)은 1988年 이후 DES를 代置할 수 있는 새로운 暗號알고리즘 開發에 拍車를 加하고 있으며 美國內 一部 企業에서는 하드웨어 製作에 들어 간 것으로 알고 있다. 勿論 이 暗號의 알고리즘은 極秘일 뿐만 아니라 키의 길이도 祕密이며 輸出도 當然히 禁止되고 있다.

公開키 暗號(public-key crytosystems)에서는 暗號化 키(公開)와 復號化 키(祕密)가 서로 다르며 각 個人은 自己의 公開키를 公開綴에 公表해 둔다. 또한 公開키 暗號는 復號用 키를 當事者만이 알고 있는 祕密키로 保有하기 때문에 키 管理問題(key management problem)는 解決된다. 即, 送信者 A와 受信者 B와의 祕密 通信을 交換할 때 A는 公開綴에서 B의 公開키를 使用하여 暗號化한 다음 暗號文을 B에 送信한다. 그러면 B는 自己의 祕密키를 利用하여 復號하게 되고 비록 盜聽者가 公開키에 의해 解讀을 試圖하더라도 不可能하기 때문에 祕密이 保全되는 것이다. 認證(authentication)機能에 관해서는 A는 自己의 祕密키로 署名(digital signature)하고 B는 A의 公開키를 가지고 復元해서 A가 眞正한 署名人인가 認證하는 것이다.

5. 暗號의 激動期(1970年代)

컴퓨터 및 高度의 情報技術의 利用이 점차 增大됨에 따라 푸라이버시(privacy)는 法的, 社會的, 道德的 關心事가 아닐 수 없다. 個人이 自身에 관한 어떠한 情報가 收錄, 保管, 使用 및 露出됨으로서 個人의 프라이버시 侵害의 威脅을 받게 되자 美政府는 1974年에 機密保障法(Privacy Act)을 制定하고 施行에 들어 갔다. 이 法은 컴퓨터 및 데이타 保護에 관한 重要한 法律이다. 同法의 趣旨下에 設立된 프라이버시保護調査委員會(Privacy Protection Study Comission)는 1977年 7月에 大統領과 議會에 提出한 最終報告書에서 「個人情報로 因해 惹起된 多大한 損害 및 不公正의 危險을 最少化하고 個人識別이 可能한 記錄의 保全, 機密 및 保護를 保證하기 爲한 合理的인 管理, 解析的 保護手段을 設定해야 한다」고 同法에 附與된 義務를 좀더 具體化하고 現實化해야 한다고 同法에 修正을 主張한 것이다. 例컨대 1934年에 制定한 證券去來法(Securities and Exchange Act)를 修正한 1977年에 施行한 外國不正行爲防止法(Foreign Corrupt Practices Act)은 資産 또는 資産을 表示하는 데이타(data)를 保護하는 手段으로 暗號의 具現化를 力說하고 있다. 證券去來所의 上場한 모든 株式의 發行者는 企業資産의 去來 및 處分 등을 正確하고 公正하게 反映하는 帳簿, 記錄, 支出을 詳細히 作成하고 維持하도록 要求하고 있다.

이 두 告示文은 美商務省標準局(NBS)이 政府部處 및 民間分野에서 데이타保護에 관한 明白하고 緊急한 必要性을 認識하고 컴퓨터 데이타의 暗號化에 對한 標準알고리즘을 採擇할 것을 1973年 5月 15日字 官報(Fedral Register)에 告示發表하고 NBS는 1974年 8月 27日字로 再次 暗號알고리즘을 公募했다. 이에 따라 1974年 8月 6日 IBM(International Business Machines Corporation)은 同社가 開發한 候補알고리즘(candiate algorithm)을 提出하였다. NBS는 이 候補알고리즘의 强度評價를 NSA에 依賴했다. 이것이 提案된 데이타暗號標準規格(Data Encryption Standard : DES)의 基本이

된 것이고, 이어서 政府外의 組織에 의해 採用될 可能性에 對備하여 集中分析한 結果 絶對 깨지지 않음을 認識하였다. 1975年 3月 17日 NBS는 DES를 聯邦規格(Fedral Standard)으로 採擇할 것을 公表하고 1977年 7月 15日 正式으로 提案된 DES를 聯邦標準規格으로 決定했다. DES는 또 컴퓨터 및 情報處理 委員會의 勸告에 따라 1980年 美國規格協會(American National Standards Institute : ANSI)에 의해 데이타 暗號알고리즘(Data Encryption Algorithm)으로 採擇하게 된 것이다. 暗號標準의 開發은 長期間이 所要됨으로 DES는 事實 美政府 規格으로 採用된 3年 後에야 비로소 ANSI에 의해 DES를 正式 採用하게 된 것이다. 去來 데이타에 認證이라든가 顧客과의 電子財務取扱 등 金融業界에서는 全的으로 DES를 利用하고 있다.

다음에는 어떻게 해서 民間次元에서 禁止된 暗號硏究를 公開하게 되었는가 하는 事由를 併記하고자 한다. 1977年 여름에 일어난 事件은 한 通의 便紙로부터 發端된 것이다. 1977年 10月 10日 New York州 Ithaca市에서 IEEE情報理論 그룹 主催로 「暗號學國際學術大會」를 開催하기로 決定하고 演士 또는 論文發表者로는 Standford大의 Martin Hellman, MIT의 Ronald Rivest, Bell硏究所의 Aaron Wyner와 IBM科學者 등으로 이미 內定된 狀態였다. 學術會는 勿論 公開發表이고 蘇聯을 包含한 外國科學者도 招請될 豫定이었다. 그리고 發表論文의 要旨도 發送段階에 있었다. 그 當時만해도 東西間 和解무드가 없는 狀態여서 暗號라는 機密을 要하는 內容을 蘇聯 등에 公開한다는 것은 想像을 超越한 일이었다. 同年 8月頃 主催側인 IEEE가 學術大會 準備에 奔走하고 있을 때 약 두 페이지 정도의 怪異한 內容이 적힌 便紙 한通이 날아 든 것이다. 그 便紙內容인 즉 暗號學에 關聯된 分野의 論文을 發表하는 그 自體뿐 만 아니라 그런 發表論文集을 國外로 流出한다는 것은 1954年 制定된 軍需物資統制法(Munitions Control Act, 現在의 Arms Export Control Act)에 違背된다는 것이다. 더욱 聯邦政府는 國務省을 通해 最新 武器, 컴퓨터, 原子力祕密 其他 機密에 屬하는 모든 裝備를 國外로의 流出을 統制하고 있다는 것이다. 便紙의 發信者는 Maryland州 Bethesda에 住所를 둔 J.A.Meyer였다. 그는 그의 便紙에서 IEEE이 直接 關與된 過去, 現在 및 將來의 學術活動 內容의 一部가 國務省이 制定한 ITAR法(International Traffic in Arms Regulations)에 抵觸된다는 것이다. 따라서 10月 10日 開催를 앞둔 Ithaca學術會는 勿論이고 지난해 Sweden의 Ronneby에서 開催된 暗號學術會에서 Hellman이 發表한 몇 篇의 論文과 또 이번에 發表할 論文의 複寫本을 蘇聯에 郵送한다는 것은 있을 수 없으며 또 許可할 수도 없다는 것이다. 또한 Meyer는 警告하기를 「IEEE 科學者들은 ITAR法에 對해 잘 모르는 것 같으며 이 法은 極秘 또는 對外祕에 屬하는 技術데이타의 出刊 및 輸出을 禁止하고 있을 뿐만 아니라 더우기 原子祕密과 暗號에 관한 出版物도 特別措置法에 依해 制約을 받는다」라고 했고, 더 나가 「더우기 몇 사람의 學者들이 主動이 되어 그 動機가 어떻든 發表論文을 準備하고 있는 모양인데 그 사람들은 政府制約에 큰 짐이 되고 있다는 것을 認識하지 못하고 있는 듯하다. DES 알고리즘과 類似한 暗號論文을 論題로 發表한다는 것은 政府의 認可 或은 輸出許可 없이는 政府政策에 違背된다는 것과 ITAR法의 技術的 侵害라는 것쯤은 IEEE는 認識해야 할 것이다. 事實, 내가 IEEE會員의 立場에서 提言하지만 IEEE는 이 事態는 愼重히 考慮해야 하며 이 最新 暗號技法이 것 잡을 수 없이 國內外로 퍼질 때에는 그것은 單純한 學問硏究 以上의 事態를 비져 낼 수 있다는 것을 銘心해야 할 것이다」라고 맺고 있다. Meyer는 ITAR法의 該當條項들을 同封해 왔고 IEEE側은 論文出刊을 일단 停止하겠다는 뜻을 Meyer에게 回答함과 同時에 IEEE 情報理論硏究會에 이 사실을 통고, Meyer 便紙의 內容을 그대로 받아드려 論文準備中인 科學者들은 發表豫定인 各自의 論文을 所屬機關과 相議하고 政府의 許可를 받도록 하라는 것이었다. 또한, 각 發表者는 事前에 Washington, D.C.의 國務省武器統制局(Office of Munitions Control)에 認可를 얻도록 했던 것이다. 따라서 科學者들은 國務省과의 相議없이는 自身의 專攻分野(暗號) 論文을 出版할 수 없다는 새로운 事實에 驚愕치 않을 수 없었다. 그래서 IEEE 情報理論硏

研究委員長인 F. Jellinck는「나는 그따위 法律은 믿기 어려우며 만일 事實이 그렇다면 無罪가 認定될 때까지 科學者들은 罪人 取扱을 당해야 하느냐?」하면서 興奮했다.

Stanford大의 Hellman과 MIT의 Rivest와 같은 科學者는 各自 自己大學의 法律顧問에게 이 問題解決을 머님기고 法律的 解釋이 完結될 때까지 默默히 기다릴 수 밖에 없게 된 것이다.

Hellman은 Stanford大 辯護士팀이 이 件에 對해 合法的인 方法을 摸索하지 않는 限 또 이 問題가 將次 法廷으로 飛化될 境遇 Stanford大가 自己를 擁護하지 않는다 해도 自己는 99% 10月 會議에 꼭 參席하겠다고 말했다. 한편 難處한 立場에 놓인 사람은 MIT의 Rivest이다. 그는 自身이 開發한 暗號方式이 解讀不能인 優秀한 것임을 詳細히 說明하고 自己의 論文을 要請하는 어느 누구에게도 보내 줄 用意가 있다는 것을 1977年 8月號 Scientific America誌에 記載했다. 이에 따라 그의 論文을 願하는 書信이 殺到해 왔고 特히, 그러한 要請은 外國으로 부터 많이 왔다. 공교롭게도 Meyer 便紙事件의 渦中에서 그는 Meyer와 IEEE로 부터 警告를 받았던 것이다. 따라서 Rivest는 MIT 辯護士팀으로 하여금 그의 論文이 ITAR法에 抵觸되는지의 可否가 判定될 때까지 論文配布를 一時 保留하게 된 것이다. 이 時點에 Science誌는 과연 Meyer가 누구이며 그의 警告 動機가 무엇인가를 調査한 結果 NSA 電話簿에서 그가 NSA 要員임을 알아 낸것이다. Science誌는 Meyer 事務室에 電話를 걸었으나 그 自身에 對해서 또는 NSA의 어느 職員이고 심지어는 그가 NSA에 任職中이라는 事實을 是認하지 않았다. 따라서 Science誌는 Meyer의 便紙事件에 관해 NSA 公報室에 正式으로 書面 質疑하기로 나섰다. 그러나 NSA 代辯人 Boardman은「NSA는 그 便紙와 無關하며 그것이 事實이라면 Meyer가 個人資格으로 썼을 것이다」라고 말하고 代辯人은 Meyer와 그의 便紙를 確實히 알고 있는 듯 함에도 不拘하고 그 便紙를 읽어 보았다든가 Meyer가 NSA에 在職中이라는 것에 대해서는 一切 밝히지 않고 있다. 그런데 한가지 二律背反的인 解釋은 國務省武器統制 副局長 Hataway는 Meyer의 便紙에 對한 論評에서 그 便紙內容에 對해 否定的인 解釋을 내렸다. 即, 公開할 수 있는 刊行物과 그 內容이라면 輸出統制法規에서 除外된다고 말했다. 年間 23,000件 以上의 各種 民願認可對象을 處理해야 할 統制局으로서는 暗號와 暗號裝置에 관한 許可事項은 全的으로 NSA統制를 받아야 한다고 有權解釋을 내렸다. 따라서 Meyer는 分明 IEEE 情報理論研究會의 研究活動에 對한 NSA의 檢閱을 建議한 것으로 解釋되는 것이다.

NSA는 特히 敵性國家로의 漏出을 防止하기 위해 暗號에 대한 研究開發을 極秘로 해야 한다는 主張과 그러한 暗號技術이 民間 및 商業側面에서 絶對有益하다는 主張의 兩面性으로 對立되었다. 그런데 言論과 美議會는 公衆電話 및 데이타 通信의 盜聽行爲와 그 可能性을 擧論하기 始作했고, 通信保安에 대한 慾求가 高潮되기 시작했던 것이다. 어느 누구고(政府, 企業, 個人) 自己의 通信을 秘化할 수 있는 能力만 있다면 푸라이버시(privacy)에 대한 威脅은 防止될 수 있으므로 구태여 NSA가 暗號研究結果의 發表를 否定하는 態度는 時代的으로 맞지 않다는 輿論이 擡頭되기 始作한 것이다.

暗號學者들은 解讀不可能한 暗號를 開發하거나 偶然히도 NSA가 이미 開發해서 機密分類된 暗號를 開發했을 境遇 그들은 自身이 開發한 暗號를 私有機密分類(self-classfication)해야 한다고 主張하였다. 따라서 NSA는 一般人의 研究結果가 出版物을 通해 公開될 경우 國家安保에 重大한 影響을 끼친다는 一貫性 있는 政策이 없다는 것이 이번 事件으로 말미아마 드러난 것이다. 또 Hellman 등의 主張은 IEEE論文集 最近號는 擴散帶域通信(spread spectrum communications)만을 全的으로 다룬 特輯임으로 이는 分明히 敵後方에서 我軍까리 秘密交信할 수 있는 軍事通信에 屬한다고 指摘하고 NSA는 이에 對한 統制가 없는 理由는 무엇이냐고 反駁하고 나섰다. 事實, 1976年에 Diffie와 Hellman은 公開키 暗號시스템이란 槪念을 이미 提示하였고 이에 刺戟을 받은 Rivest와 그의 同僚는 具體的인 RSA 暗號알고리즘을 開發 1978年에 發表한 것은 有名한 事實이다. 그의 研究가 發表된지 近 1年이 지난 지금에서 聯邦法에 抵觸된다는 Me-

yer의 警告는 論理에 맞지 않는다는 主張이다. 하여튼 이러한 一連의 事件들이 얼키고 설킨 環境속에서 暗號學者들은 民間次元에서 研究는 꾸준히 繼續되고 1980年代의 暗號文化의 基礎를 確立했으니 1970年代는 文字 그대로 門戶開放의 激動期라 할 수 있다.

6. 暗號의 開花期(1980年代)

暗號研究의 活動狀況으로 볼 때 1980年代 10年間은 現代 暗號의 黃金期라 하겠다. 1970年 後半에 發表된 Diffie-Hellman의 公開 키 暗號의 概念을 비롯하여 公開 키 分配法(1976), Merkle-Hellman의 Knapspack 暗號 알고리즘(1976), DES 暗號의 美聯邦標準化(1977), Rivest-Shamir-Adleman의 RSA暗號(1978), McEliece의 符號를 利用한 暗號시스템(1978), Shamir의 速決署名方式(1978) 및 Rabin의 署名暗號(1979) 등 이러한 研究論文들이 暗號文化 胎動에 促進劑 役割을 한 것은 分明하다. 그 後 1980年代에 접어들면서 公開 키 暗號를 中心으로 活潑한 研究가 展開되었고 上中下의 優劣로 分類될 수 있는 公開 出版된 暗號關聯 發表件數만 해도 約 4,000件에 달하였다. 1983年 美國에서 처음으로 國際暗號研究學會(The International Association for Cryptologic Reserch : IACR)가 創立되었고, 우리나라에서도 1990年 12月 12日 韓國通信情報保護學會(Korea Institute of Information Security and Cryptology : KIISC)가 創立되었으니 美國의 暗號學會創立後 滿 七年만의 일이다.

美國 IACR가 主催하는 國際暗號會議로는 Crypto와 Eurocrypt를 들 수 있다. Crypto 暗號學大會는 1981年 以來 每年 8月頃 California大 Santa Barbara 캠퍼스에서 開催하는 것이 慣例로 되어 있다. 그리고 Eurocrypt는 1982年 以來 每年 4, 5月頃 歐洲 여러 곳에서 開催되었다. 그 外의 國際會議로서는 濠洲에서 開催하는 Auscrypt와 1991年 12月에 처음으로 日本에서 開催될 豫定인 Asiancrypt가 있다. 그밖에도 每年 9月頃에 IEEE가 主催하는 컴퓨터科學의 基礎理論에 權威있는 國際會議로서 FOCS(Symposium on Foundations of Computer Science)와 ACM이 主催하는 STOC(Symposium on Theory of Computing) 등이 있는데 暗號에 관한 論文이 該當 session에서 發表되고 있다. Crypto와 Eurocrypt에서 發表된 論文(Conference Proceedings)은 Springer-Verlag社에서 出版되고 其他 重要한 論文은 IEEE 情報理論誌 그리고 英國의 IEE Electronics Letters, Cryptologia 및 Journal of Cryptology 등의 學術雜誌에서 發表되고 있다.

暗號技法과 暗號解讀은 不可分의 關係가 있다. 어느 한사람이 새로운 暗號알고리즘을 暗號論文誌에 寄稿하면 다른 專門家들은 提案된 暗號를 解讀하기 爲해 全力을 傾注해서 깨게 되고, 또 다시 改善型이 나오면 그 暗號의 解讀을 시도하게 되고 이런 식의 過程을 되풀이하게 된다. 따라서, 暗號解讀(cryptanlysis)方法의 考案自體로 因해 暗號技法發展에 多大한 寄與를 한다는 것을 우리는 否認할 수 없을 것이다. 例컨데 1978年 Merkle-Hellman이 發表한 Knapsack暗號는 1982年 Shamir가 法變換(modulo transform)을 1回 試圖하므로써 이 MH 暗號의 解讀에 成功하였다. MH 暗號를 여러번의 法變換을 통해 反復施行하므로서 强度를 높이고자 試圖한 反復 MH 暗號 亦是 1984年 Brickell에 依해 完全히 解讀되었다. 이 때문에 Merkle로 부터 1,000弗의 賞金을 받은 일을 크게 話題가 되기도 하였다. 이것이 Knapsack 暗號(MH 暗號)가 解讀되어 깨진 公開 키 暗號의 代表的인 例라고 하겠다. 1978年에 提案된 RSA 暗號는 公開 키 暗號方式中 가장 有名한 것이다. 이 RSA 公開 키 暗號는 祕話機能과 認證機能을 兼備한 優秀한 暗號이며 大端히 큰 數를 素因數分解해야 할 難題를 根據로 한 아직 完全히 解讀이 않된 狀態로 安全性을 保有하고 있는 暗號인 것이다. 離散對數的解法의 難題라는 点을 利用한 Diffie-Hellman의 키 配分方式의 安全性도 離散對數(discrete logarithm)의 計算이 어렵다는 点에 根據를 둔 것이지만 ElGamal 暗號도 그 安全性이 大端히 큰 數를 法(modulo)으로 하는 離散對數의 計算難을 노린 RSA 暗號에 匹敵할 만한 機能을 갖춘 優秀한 暗號라 하겠다.

1980年代의 暗號應用은 認證(authentication), 署名(digital signature), 電子郵便(electronic

mail), 그리고 1986年 以來 急速히 硏究對象이 된 零知識證明(Zero-Knowledge Interactive Proofs : ZKIP)問題 등을 들 수 있다. 여기서 잠시 이러한 것들의 基本理論에 대해 紹介해 보기로 하자.

[I] 認證(Authentication)

認證이란 컴퓨터 通信網을 通해 相對方의 正體를 確認하는 技法이고 暗號시스템에 따라 다음 두가지로 分類된다.

[1] 祕密 키 暗號시스템의 境遇

使用者 A와 使用者 B가 通信用 祕密 키(secret key) K를 共有했을 境遇 一般的인 認證 節次는 다음과 같다. 于先, 記號를 說明하면 IA, IB는 各各 A 또는 B에서 發生하는 亂數를 表示하고 이것을 確認因子(identifier)라 부른다.

(1) B는 A로 E_K(IB)를 送信한다.

(2) A는 E_K(IB)를 復號한 後 E_K(IB, IA)를 B로 送信한다.

(3) B는 E_K(IB, IA)를 復號한 後 IB′, IA′를 얻은 다음 IB=IB′이면 B는 A를 認證(authentication)했다고 看做한다. 그리고 E_K(IA′)를 A로 送信한다.

(4) A는 E_K(IA′)를 얻은 後 IA=IA′가 確認되면 A는 B를 認證했다고 看做한다.

[2] 公開 키 暗號시스템의 境遇

(1) A는 B의 公開 키 K_PB로 暗號化한 E_{KpB}(IA, A)를 B로 送信한다.

(2) B는 自己의 祕密 키 K_SB를 利用하여 E_{KpB}(IA, A)를 復號하고 IA와 A를 얻은 後 A에게로 다시 E_{KpA}(IA, IB)를 送信한다.

(3) A는 E_{KpA}(IA, IB)를 自己의 祕密 키 K_SA로 復號하여 IA′와 IB′를 各各 얻는다. 萬若 IB=IB′이면 B는 A를 認證했다고 看做한다.

이와 같이 해서 컴퓨터 通信網에서 相互認證을 遂行하게 되는 것이다.

公開키 認證方式으로서는 (1) Shamir(1978)가 Knapsack 問題를 基本으로 한 認證方式을 提案했으나 Odlyzko(1984)에 依해 解讀되어 깨졌고 (2) ElGamal(1985)는 離散對數의 難解点을 利用한 認證方式인데 아직 正式으로 解讀된 바 없다. (3) Ong-Schnorr-Shamir(1984) 認證方式은 因數分解와 二次 congruence를 利用한 認證方式인데 不幸하게도 Pollard(1987)에 의해 破壞된 것이다. (4) Rivest-Shamir-Adleman(1978)認證方式은 認證 뿐만 아니라 祕話通信에서도 適用되는 有名한 시스템이다. (5) Simmon(1984)이 提案한 方式은 因數分解를 基本으로 한 것이고 (6) Seberry-Jone (1986)의 方式은 Shamir의 速決認證方式을 改良한 것이다. 그 外에도 많은 暗號學者들이 各自의 技法을 提案하고 있으나 이만 이것으로 줄이기로 하겠다.

[II] 디지탈 署名(Digital signatures)

銀行去來 등과 같은 商用, 軍事分野의 作戰命令 및 指揮, 그리고 契約協商 등과 같은 컴퓨터 通信網을 利用한 應用分野는 디지탈 署名이 要求된다. 旣存의 디지탈 署名은 仲裁方式(arbitrated signature scheme)과 非仲裁直接方式(true signature scheme)으로 區分된다. 仲裁方式 디지탈 署名技法은 發信者 S가 署名한 情報를 仲裁人(arbitrator) A를 經由해서 受信者 R에 傳達되므로 A가 證人役割을 하기 때문에 紛爭의 素地가 減少 乃至는 解決된다. 非仲裁直接方式은 仲裁人 A의 介入없이 바로 發信者 S가 受信者 R에 署名된 情報를 直接 보내게 되고 이에 對해 受信者 R이 그의 眞否를 確認 및 認准하는 技法을 말한다. 旣存의 祕密 키 暗號시스템과 近者의 公開 키 暗號시스템 共히 署名의 眞否를 가려내는 技法으로 應用될 수 있으나 公開 키를 使用해서 解決을 摸索하는 非仲裁直接方式이 簡便하므로 다음과 같은 過程에 따라 公開키 暗號시스템을 利用한 디지탈 署名方式에 對해 紹介코자 한다.

送信者 A는 自身의 祕密 키(secret key) K_SA를 利用하여 平文 X를 暗號化하고 署名文(signed message) $Y=E_{KsA}(X)$를 만든 다음 다시 使用者 B의 公開 키(public key) K_PB로 署名文 Y를 暗號化한 $Y'=E_{KpB}(Y)$를 受信者 B에 보낸다. B는 Y′를 受信

하여 自身의 祕密 키 K_{SB}를 利用하여 復號하므로써 $Y=E_{KsA}(X)$를 求하게 되고, A의 公開 키 K_PA를 利用하여 다시 復號化하면 平文 X를 얻을 수 있다. 한편, B는 $D_{KsA}(X)$를 追後의 紛爭에 對備하여 貯藏해 둔다. 따라서 그 後 A가 $Y=E_{KsA}(X)$를 보낸 事實이 없다고 主張하면 $D_{KsA}(X)$를 仲裁審判官에 보내 A의 公開 키 K_PA를 利用하여 元來의 平文 X를 生成할 수 있는가의 判斷을 求한다. $D_{KsA}(X)$는 오직 A에 依해서만 生成할 수 있으므로 上記의 技法이 디지탈 署名으로 利用되고 있다.

디지탈 署名에는 Diffie와 Lampo[illegible]가 提案한 方式과 Rabin(1978)에 依해서 開發된 對稱祕密變換法(symmetric cryptographic transformation : SCT)를 基礎로 한 署名方法이 있다. 그리고 1981年에 DES 알고리즘을 利用하여 Matyas-Meyer가 提案한 署名方式이 있으며, 이밖에도 Davies와 Price(1980)가 考案한 디지탈 署名方式으로 公開 키 시스템을 應用한 것이 있다. 日本 方式으로는 Okamoto-Shiraishi(1985) 署名方式이 있는데 RSA 署名方式 보다 高速이라는 長點이 있으나 不幸이도 Brickell과 Delaurentis(1986) 등에 依해 破壞되었다. 그 外에도 몇가지 署名方式이 더 있으나 여기서 省略하기로 한다.

[Ⅲ] 電子郵便(Electronic mail)

電子郵便은 원하는 受信者가 當時 컴퓨터에 記錄되어 있지 않은 境遇라도 컴퓨터網을 通해 受信者에게 작은 量의 情報(message)를 보내려고 할 때 利用된다. 使用者 A가 使用者 B에게 情報를 보내려고 할 때 B가 컴퓨터에 記錄되어 있지 않더라도 시스템 自體가 情報傳送을 處理해서 B의 郵遞函에 貯藏시키면 B는 自己의 通信 키를 알고 있으므로 그것으로 보내온 情報를 復號化하여 그 便紙內容을 읽을 수 있게 된다. 一般的으로 公開 키 暗號시스템에 의해 電子郵便을 利用하는 便이 祕密 키 暗號시스템을 利用하는 것보다 簡便하다.

[1] 祕密 키 暗號시스템의 境遇

(1) 使用者 A는 于先 키 分配 센터(key distribution center)로부터 使用者 B의 暗號化 키 K_B를 찾아내고 (2) A는 키 K_B로 通信文 X를 暗號化하여 暗號文 $Y=E_{KB}(X)$를 만든 다음 (3) Y를 B에 傳送해서 B의 郵便函에 貯藏하면 (4) B는 自己의 키 K_B로 暗號化된 通信文 X를 復號節次 $X=D_{KB}(Y)$로 復元하여 읽어 볼 수 있다.

[2] 公開 키 復號시스템의 境遇

公開 키 暗號시스템을 電子郵便시스템에 應用하여 情報를 送受信하는 節次는 다음과 같다.

(1) 使用者 A는 公開綴(public directory)에서 B의 公開 키 K_PB를 얻는다.

(2) A는 K_PB를 利用하여 情報 X를 暗號化한다. 即, $Y=E_{KpB}(X)$.

(3) A는 暗號文 Y를 使用者 B의 郵遞函에 貯藏한다.

(4) B는 自身의 祕密 키 KsB를 알고 있으므로 이 키를 利用하여 復號하면 情報 $X=D_{KsB}(Y)$를 읽어 볼 수 있다.

[Ⅳ] 零知識相互證明法(ZKIP)

어떤 情報를 알고 있으면서 그 內容을 相對方에게 公開하지 않고 納得시키는 方法을 零知識證明(Zero Knowledge Interactive Proof : ZKIP)이라 한다. 이 方法은 1986年부터 本格的인 硏究에 들어갔고 認證分野에 까지 應用되는 새로운 技法으로 登場하게 되었다. 例컨데 本人 確認을 爲해 現在 使用하고 있는 祕密情報(secret password)方式의 缺點을 補強한 새로운 手法인 것이다.

Blum(1982)의 電話上으로 銅錢 던지기(coin flipping) 놀음이 史上 最初의 零知識證明이라 할 수 있다. 그 後 Goldwasser, Micali와 Rackoff(1985) 등의 RSA 暗號를 利用한 ZKIP, Benaloh와 Yung (1986) 등의 選擧問題, 그리고 Crepeau(1986)의 知的놀음(mental pocker) 등이 零知識證明에 對한 適用例들이다. 또 Fiat와 Shamir(1986)은 認證問題에 零知識證明을 適用했다. 事實 ZKIP의 應用分野에는 本人의 確認 以外에 메시지 認證, 다지탈 署名 및 그룹 所屬認證(group membership authentication) 등이 있는데 그룹所屬認證은 다시 會員名簿方式과 會員證保有方式으로 大別된다.

[V] 暗號應用分野(EFT, PIN, Database Security)

오늘날과 같은 競爭社會에서 金融業, 特히 銀行界는 顧客에게 最上의 서비스를 提供하기 爲해 暗號技術의 導入을 外面할 수 없는 形便이 되었다. 1970年代부터 銀行들은 自體內의 컴퓨터網을 利用하여 遠距離에 있는 支店顧客들에게 安全하게 現金을 支拂할 수 있는 方途에 대해 여러가지로 摸索해 왔다. 그러한 現實의 첫번째가 電子送金(Electronic Funds Transfer: EFT)이다. 따라서 컴퓨터 端末을 保有한 支店들은 現金支拂, 旅行者手票賣買, 各種料金告知書 取扱 및 航空票豫約 등등의 業務를 迅速히 處理하게 된 것이다. 그런데 EFT 서비스網이 構築되기 前에 풀어야 할 問題는 安全과 保護의 解決策이다. 即, 어떤 去來直前에 무슨 方法으로든 顧客을 識別하는 問題가 先行되어야 한다는 것이다. 勿論 顧客認證의 좋은 方法은 銀行카드外에 祕密個人識別番號(Personal Identification Numbers: PIN)를 利用하는 것이다. 따라서 PIN과 銀行카드의 保護는 必然的으로 EFT 保全에 絶對的이다. 銀行카드는 紛失, 盜難 및 僞造의 素地가 있으므로 EFT 시스템內에서 貯藏 또는 移送등은 禁物이다. 따라서 不當資金流出을 防止할 唯一한 方法은 祕密 PIN 뿐이다.

다음으로 가장 重要한 課題는 데이타베이스(database)內의 情報祕密을 維持하기 爲한 暗號應用이다. 이미 알고 있는 바와 같이 데이타베이스는 많은 使用者들이 共有하는 各種情報를 컴퓨터 시스템에 貯藏한 集合體를 말한다. 예컨데 保安裝置(security shell)를 거치지 않고 컴퓨터 情報를 곧바로 빼내는 不當行爲는 一種의 데이타 變造인 것이다. 데이타베이스는 意圖的이든 偶發的이든 人爲的으로 變造될 素地를 안고 있다. 컴퓨터의 한 部類인 데이타베이스의 保護는 全的으로 OS(operating system)에 달려있다. 保安裝置가 完備된 複雜한 OS일지라도 情報의 不法流出에 대한 不安은 常存하는 것이다. 補助記憶裝置에 貯藏된 모든 情報 데이타를 效率的으로 保護하기 爲해서는 可能한 限 여러가지 保護對備策이 講究되어야 하는데 全的으로 暗號技法에 依存하는 수 밖에 없다.

[VI] 運營體制(Operating System: OS) 保安 및 暗號化 키 管理

컴퓨터 시스템에 있어서의 OS는 하나 以上의 使用者에게 시스템의 同時使用을 可能케하는 多重프로그램(multiprograming)機能을 提供하고 있다. 따라서 여러 使用者가 同時에 하나의 시스템上에서 動作되므로, 한 使用者의 計算結果(computing result)는 다른 不法的이고 惡意的인 使用者로부터 保護되어야 한다. 이를 위해 OS는 메모리(memory), 파일(file), 特定客體(specified object)에 대한 액세스 制御 및 使用者 認證에 對한 保安對策을 마련해야 한다. 컴퓨터 시스템에서의 OS 保安은 上記 客體에 對한 保安機能을 提供하는 것으로서, OS에 對한 保安으로서, OS 設計時 뿐 만 아니라 이를 利用할 때 매우 重要한 役割을 遂行하므로 이에 對한 持續的인 硏究가 遂行되어야 할 것이다.

컴퓨터 通信網 또는 컴퓨터 시스템에서는 用途에 따라 여러 種類의 暗號化 키가 存在한다. 컴퓨터 通信網에서의 暗號方式 適用形態는 크게 終端間(end-to-end) 暗號方式, 링크間(link by link) 暗號方式, 노드間(node-to-node)暗號方式으로 區分되며, 이와 같은 컴퓨터 通信網에서 暗號化 키의 生成, 分配 그리고 管理는 暗號化 키의 保安性이 全體 暗號시스템의 保安性에 커다란 影響을 미치는 것을 考慮할 때 매우 重要한 硏究 主題가 된다. 컴퓨터 保安을 위한 暗號化 키는 파일 保安을 위한 暗號化 키와 通信保安을 위한 暗號化 키로 나누어지며, 各各의 用途에 따라 이들 暗號化 키는 階層化되어 디스크(disk)나 테이프(tape) 등과 같은 安全한 場所에 保管되어 있다가, 이들은 暗號化 키에 對한 生成, 分配 그리고 管理를 總括하는 暗號化 키 管理프로그램(key manager)에 依해 利用, 變更(transform) 및 傳送된다. 이를 指稱하여 暗號化 키 生成, 分配, 管理라 하며 이는 컴퓨터 시스템 및 通信網에서 매우 重要한 役割을 遂行한

끝으로 正數論과 抽象代數學이 暗號開發에 絶對的인 一翼을 擔當하게 된 것이 事實이며 暗號解讀에 特殊 高性能 컴퓨터(special super computer)가 必須不可缺하다는 것 또한 否認할 수 없는 事實이다. 素因數分解法, 離散對數學 그리고 週期性 打破와 無作爲性을 故意로 만들기 위한 非線形結合法 등 理論數學者의 힘을 빌어야 하겠고 또 暗號解讀에 必要한 計算複雜度를 硏究하는 複雜度理論(complexity theory)의 完璧한 定立이 時急히 遂行되어야 할 것이다. 한 例로 RSA 公開 키 알고리즘에서 보듯이 整數 n의 素因數分解에 관한 問題에서 n의 값이 클수록 n=pq와 같이 p와 q로 素因數分解가 實行 不可能하게 된다. 한번의 演算處理가 10^{-9}秒 걸린다 할 때 n=70인 境遇 處理時間이 100日 以上이 所要되며 n=100인 境遇는 處理時間이 約 75年이나 걸리게 되니 이러한 演算處理를 할 수 있는 컴퓨터 開發이 果然 우리나라에서 實現될 것인지 暗澹할 뿐이다. 따라서 우리는 奮發할 수 밖에 없다. 1660年에 Fermat가 發表한 定理가 正數論의 基礎가 되었고 約 100年 後인 1736年에 Euler가 Fermat의 定理를 證明한 것이다. 1770年에 Waring이 Wilson의 理論을 發表했는데 1771年 Lagrange에 의해 Willson의 定理를 證明하는데 成功하였다. 그것이 2次 congruence 硏究에 큰 도움이 된 것이다. 特히 18世紀 偉大한 數學者인 Euler(1707~1783)는 Fermat의 定理를 一般化시키고 1760年에 그의 有名한 定理인 「gcd(a, n)=1일 때 $a^{\phi(n)}\equiv 1 \pmod n$」라는 Euler의 定理를 提案했으니 지금으로부터 232年前 일이다. 이 定理가 RSA 暗號에 適用될 줄 누가 敢히 짐작이나 했을 것인가. 209年前에 죽은 Euler는 그의 무덤에서 微笑를 짓고 있을 것이고 數論을 가르치는 數學者들은 現代 暗號硏究와 더불어 快哉를 부르게 되었으니 學問의 眞理는 萬古의 鐵則임을 새삼 實感케 한다.

넘어야 할 險峻한 산은 疊疊인데 해는 西山에 떨어지니 호랑이 밥이 안되려면 우리 모든 暗號學者들은 정신을 바짝 차리고 서로를 激勵하며 뭉쳐야 할 것이다.

7. 結 言

制限된 時間과 限定된 紙面關係로 包括的이며 充分한 內容의 論述을 提示하지 못한데 대해 매우 悚懼스럽게 생각한다. 美國이 1977年에 暗號에 대한 門戶를 開放한 이래 14年에 걸친 硏究活動으로 그 業績 또한 대단하며, 美, 日, 歐 先進國들의 暗號에 대한 硏究開發을 開花期라 한다면 우리나라의 暗號에 대한 關心과 硏究側面에서 볼 때 아직은 發芽期에 該當할 것이다. 歐美의 發表論文은 過去 10年 동안 4千餘篇의 論文을 學術誌 등에 發表했으니 그 또한 큰 業績이라 아니할 수 없을 것이다. 우리나라도 過去 數年간 뜻있는 專門家 및 政府에 의해 이 分野의 硏究와 開發이 疏忽했다고는 보지 않지만 本 學會의 出帆을 契機로 民間次元에서 暗號와 情報保護에 대한 本格的인 關心과 硏究를 하게 된 것을 참으로 多幸으로 생각한다. 한가지 우리 暗號學者들이 바라는 것은 政府次元에서 美國의 國家保安廳(NSA)과 같은 全擔機關이 時急히 設立되었으면 하는 所望일 것이다.

參 考 文 獻

1. Diffie, W. and Martin Hellman : "New Direction in Cryptography", IEEE Trans. Inform. Theory, vol. IT-22, pp. 644-654, 1976.

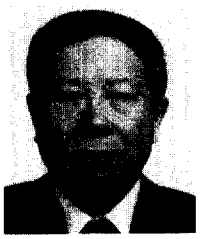
2. ——— : "Privacy and Authentication : An Introduction to Cryptography", Proc. IEEE, vol. 67, pp. 397-427, 1979.

3. Ayoub, F. and K. Singh : "Cryptographic Techniques and Network Security", IEE Proc., vol. 131, no. 7, pp. 684-693, 1984.

4. Meyer, C. H. and S. M. Matyas : Cryptography : A New Dimension in Computer Data Security, John Wiley, New York, 1982.

5. Brickell, E. F. and A. M. Odlyzko : "Cryptanalysis : A Survey of Recent Results」, Proc. IEEE, vol. 76, no. 5, pp. 578-590, 1988.

□ 著者紹介



李 晩 榮(正會員)

1924年 11月 30日生
서울大學校 電氣工學科 工學士(BSEE)
美國 Colorado大學校 工學碩士(MSEE) 및 工學博士(Ph.D.)
美國 Virginia 州立大 工大教授
美國 California Institute of Technology, JPL 研究員
國防科學研究所 第1副所長/韓國電子通信 社長/三星半導体通信社長/
漢陽大 副總長/現 漢陽大 名譽教授/韓國通信情報保護學會 會長
著書： Error Correcting Coding Theory, McGraw-Hill, New York, 1989.