マルチメディア通信と分散処理 30－4
（１９８６．７．２５）

暗号化技術の最近の動向

辻井重男　　伊東利哉
東京工業大学　工学部　電気・電子工学科

セキュリティ技術の動向について暗号化技術を中心に解説する。小文では、まず慣用鍵暗号及び公開鍵暗号の概要を述べ、それらの相違を明らかにする。そして、慣用鍵暗号の代表としてＤＥＳを、公開鍵暗号の代表としてＲＳＡを簡単に紹介する。また、暗号アルゴリズム利用モードについて、ＩＳＯ標準案を中心に述べ、各利用モードの特徴をまとめる。最後に、暗号化技術の応用として、幾つかのディジタル署名方式を紹介し、それらの比較を行い、さらに安全な秘密鍵の共有を実現する公開鍵配送方式（Public-Key Distribution System；ＰＫＤＳ）について言及する。

Recent Trends on Encryption Technique

Shigeo TSUJII　　Toshiya ITOH
Faculty of Engineering,
Tokyo Institute of Technology

This paper surveys recent trends on encryption technique. First, the difference between the conventional cryptosystem and the public-key cryptosystem is described, and representative systems, DES algorithm and RSA scheme, are introduced briefly. After it, some modes of operation for 64 bits block cipher algorithm are shown and summary of their features is given. Finally, digital signatures and public-key distribution system are given as applications of the encryption technique. Some digital signatures are introduced and compared. A public-key distribution system (a method of sharing secret-keys) is refered and its security is considered.

１．暗号化方式の概要

マイクロエレクトロニクスの目覚ましい進歩により、情報通信システムのネットワーク化・ディジタル化が急速に進んでいる。このような大量の情報を高速に処理、蓄積、伝送するシステムにおいて、情報の盗聴、改ざん、破壊等を防ぐ手段として暗号化技術が注目されている。小文では、上述のような情報セキュリティを確保・向上する手法として、工学的側面から暗号化技術について解説する。

１．１ 暗号化方式の分類［１，２］

暗号化方式は、（１）慣用鍵（共通鍵）暗号方式と（２）公開鍵暗号方式の２つに大別される。これらの詳細は、２．、３．で述べるとし、ここではこれらの相違を明らかにするために概略を記すに留める。

（１）慣用鍵（共通鍵）暗号方式

慣用鍵暗号方式は、送信者と受信者が共通の秘密情報Ｋを共有することを基本としている。送信者は逆変換が一意に存在する任意の変換ｆにより、平文Ｐを秘密情報Ｋを用いて（例えば、Ｐ＋Ｋ，Ｐ×Ｋ等）暗号文Ｃ＝ｆ（Ｐ：Ｋ）に変換する。受信者は、受け取った暗号文Ｃに対し、秘密情報Ｋを用いてf^{-1}を施すことにより（例えばＣ－Ｋ，Ｃ／Ｋ等）平文Ｐを復元する（図１．１参照）。

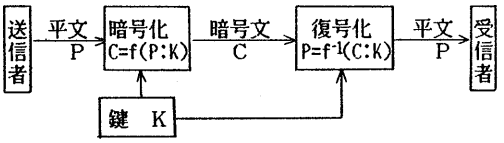


図１．１ 慣用鍵暗号の通信形体

（２）公開鍵暗号方式

公開鍵暗号方式は、暗号化の鍵と復号化の鍵が異なる点が慣用方式と大きく異なる点である。平文Ｐは暗号化用の鍵K_Eで暗号化されるが、受信側ではK_Eと異なる復号化用の鍵K_Dにより復号化が行われる（図１．２）。公開鍵暗号方式を実現するには、K_Eで暗号化された暗号文はK_Dによってしか復号できず、且つK_EからK_Dを求めることが実際上不可能となるようにしなければならない。

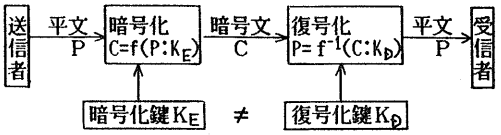


図１．２ 公開鍵暗号の通信形体

１．２ 鍵 管 理

慣用鍵暗号系においては、通信当事者に対して一対の秘密情報Ｋが必要であるので、複数局間の通信系では鍵管理が問題となる。これについては、公開鍵配送方式による方法が提案されているが、詳しくは６．で述べる。

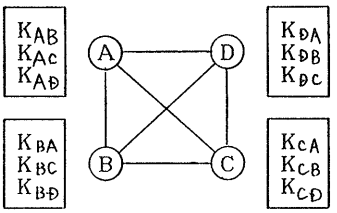


図１．３ 慣用暗号系における鍵管理

一方、公開鍵暗号系においては、各局が一対のK_E、K_Dを生成し、K_Eを公開、K_Dを秘密に管理するので、鍵管理の問題は解消される。

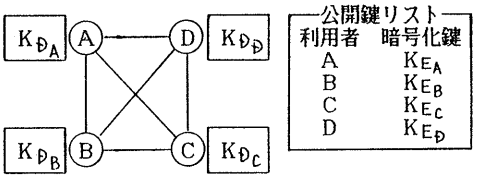


図１．４ 公開鍵暗号における鍵管理

２．慣用鍵暗号方式

２．１ 慣用鍵暗号方式の基本単位

（１）換字式暗号

平文の記号を別の記号に置き換えるもので、シーザー暗号［２］が最も基本的である。又、平文の統計的性質を消去する為に、多表式換字方式が用いられる。

（２）転置式暗号

平文中の記号を一定の規則により並び換えるもので、簡単なものとしては、横書きした平文を縦に読んでい

く等である。

（３）挿入式暗号

平文中の各記号の間に余分な記号を挿入し平文を隠すものである。しかし、暗号強度を強めるためには、平文の数倍の長さの記号を挿入する必要があり、暗号文長の増加に伴い通信効率の低下が著しい。一般に、この方式は殆ど使用されない。

（４）（１），（２），（３）の組み合せ

Lucifer 暗号（ＤＥＳの原型）、ＤＥＳ等。

２．２　ＤＥＳ（Data Encryption Standard）

ＤＥＳアルゴリズムは、６４ビットの平文を入力とし、６４ビットの鍵を秘密情報として、６４ビットの暗号文を出力するシステムである。鍵の６４ビットのうち、８，１６，‥‥，６４ビット目は、それぞれ対応するバイトの奇数パリティになっており、鍵の設定、配送、蓄積などのエラー検出に用いる。ＤＥＳの暗号化アルゴリズムの全体を図２．１に示すが、これは換字法と転置法の組み合せの１６段の繰返しである。

（１）暗号化処理

暗号化処理は図２．１暗号化処理部で実行される。初段の初期転置ＩＰ、最終段の最終転置IP^{-1}は、64ビット出力するもので、互いに逆変換になっている。また、図２．２にｎ段目の暗号化処理、図２．３にｆ（Ｒ，Ｋ）の計算を示す（詳しくは文献［１］参照）。

（２）鍵生成

鍵生成は図２．１の鍵生成部で実行される。パリティビット８ビットを含む６４ビットが鍵生成部に入力され、縮約転置により５６ビットに変換される。この左半分の２８ビットがC_0、右半分の２８ビットがD_0となり、以下順次左シフトを繰り返し（表２．１）、さらに縮約転置により４８ビットに変換され各段の暗号化処理部への鍵入力となる。

処理段数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ｼﾌﾄ 回数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

表２．１　左シフト回数

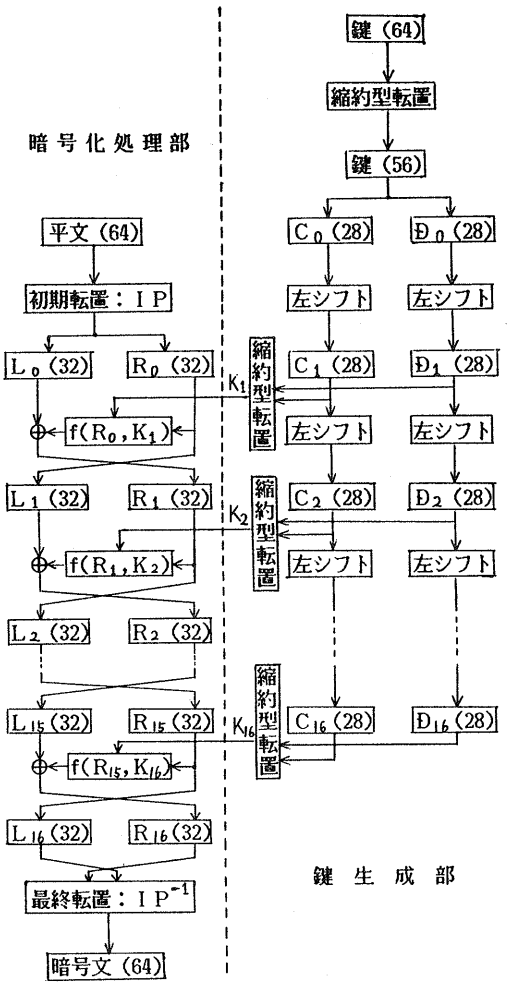


図２．１　ＤＥＳアルゴリズム

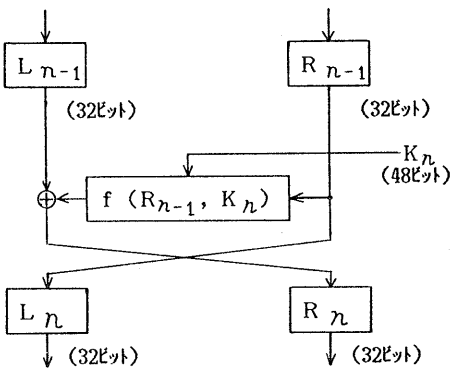


図２．２　ｎ段目の暗号化処理

（３）復号化処理

復号化処理は暗号化処理と全く同じアルゴリズムにより実行される。復号化処理は、

$$\left.\begin{aligned} R_{n-1} &= L_n \\ L_{n-1} &= R_n \oplus f(L_n, K_n) \end{aligned}\right\} \quad (2.1)$$

により実行される。

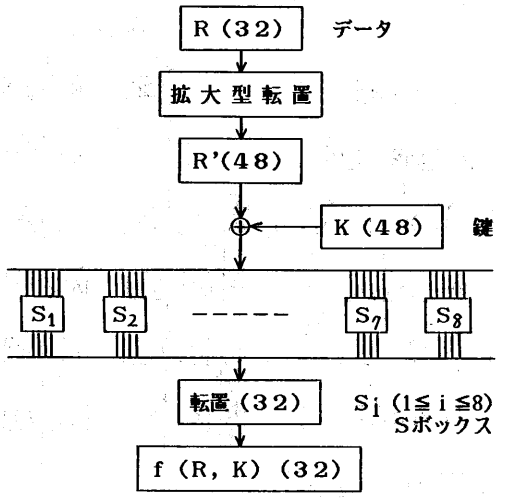


図2．3　f（R，K）の計算

以上が代表的慣用鍵暗号系ＤＥＳの概要である。ＤＥＳの安全性については、鍵の長さが不十分であると指摘されている［3，4，5］。またＮＳＡ(National Standard Agency)も、ＤＥＳ製品について、1988年までは安全性は保証するが、安全保証期間を1993年まで延期することはできないと述べている。

一方、暗号強度の評価基準の一つとして、M指標［6，7］なる概念が提案されており、これに基づいて暗号化アルゴリズムＦＥＡＬ(Fast Encipherment Algorithm)が開発されている。

３．公開鍵暗号方式

公開鍵暗号方式は、1976年 Diffie，Hellmanによりそのアイデアが示された［8］。これは従来の暗号の常識を破る画期的な方式として大いに注目され、米国、ヨーロッパ、日本等で盛んに研究が行われている。特に、1978年 Rivest，Shamir，Adlemanにより考案されたＲＳＡ暗号系［9］は、その解読の困難さ、アルゴリズムの簡単さにより高く評価されている。本節では、ＲＳＡを中心に公開鍵暗号方式について述べる。

３．１　落し戸付一方向性関数

現代の暗号化方式は、暗号化アルゴリズムは公開し、鍵を秘密にすることにより暗号の強度を保証している。慣用鍵暗号方式は、この点で極めて自然な発想に基づいた方式であると言える。これに対し、公開鍵暗号方式が、暗号化アルゴリズムと暗号化鍵を公開しても秘密通信が実現できるのは、以下に述べる落し戸付一方向性関数(Trapdoor Oneway Function)に基づいている。

ある関数ｆ（ｘ）（ｆ；Ｘ→Ｙ）が

(i) $\forall x \in X$に対しｆ（ｘ）が効率良く計算できる

(ii)殆ど全ての$y \in Y$にたいして、$x = f^{-1}(y)$を計算することは実際上不可能である。

を満足する時、ｆ（ｘ）は一方向性関数（Oneway Function）であると言う。また、このような一方向性関数ｆ（ｘ）に対し、

(iii) ある落し戸（Trapdoor）情報ｋにより、$\forall y \in Y$に対し、$x = f^{-1}(y : k)$が効率良く計算できる

時、ｆ（ｘ）を落し戸付一方向性関数（Trapdoor Oneway Function ）と言う。

一方向性関数としては、素因数分解、ナップザック問題、離散対数等があり、これらを用いた公開鍵暗号系［9,10,11,12,13,17］が提案されている。

３．２　ＲＳＡ暗号系［９］

ＲＳＡ暗号系は、大きな２つの素数ｐ，ｑ（共にｍビット）の積を計算するのはＯ（mlogm loglogm）［14］と容易であるが、その積を２つの素数に素因数分解するのはＯ（$\exp\sqrt{m \log m}$）［15］と（ｍが大きくなると）極めて困難であるという事実に基づいている。

ＲＳＡ暗号系は以下のように構成される（暗号化／復号化操作の正当性については［１，９］参照）。

パラメータ設定

①大きな素数ｐ，ｑ（１０進１００桁）を選ぶ

②Ｌ＝ＬＣＭ（ｐ－１，ｑ－１）とすると、

ＧＣＤ（ｅ，Ｌ）＝１ ┐
ｅ・ｄ≡１（ｍｏｄ Ｌ） ┘ なるｅ，ｄを計算する

公開鍵：e，n（＝pq）
秘密鍵：d，p，q

〈暗号化〉

0≦M≦n－1なる平文Mに対し、

$C \equiv M^{e} \pmod{n}$

により暗号文Cを定義する。

〈復号化〉

受信した暗号文Cに対し、

$C^{d} \equiv M \pmod{n}$

により平文Mを復元する。

RSA暗号系の安全性はn（＝pq）の素因数分解の困難さに基づいているが、RSA暗号系の解読とnの素因数分解が同値であることは示されていない（[9]では秘密鍵dを求めることとnを素因数分解することは同値であることが示されている）。他に素因数分解の困難さに基づく公開鍵暗号系としては[10, 11]があるが、これらは暗号の解読と素因数分解が同値であることが示されている。

以上述べた以外の公開鍵暗号系としては、線形符号の復号の困難さに基づくMcEliece [16]、離散対数の難しさに基づく Elgamal [17]、有限体（特にGF（2^{m}））上の非線形連立方程式を解くことの困難さに基づく松本 [18]、辻井 [19] 等がある。

4．暗号利用モード

本節では、暗号利用モードについてISO標準案を中心にのべる。ISOにより規定されている暗号利用モードは以下の4種類である。

（1）ECBモード（Electric Code Book）

暗号アルゴリズムをそのまま繰り返し利用する（図4．1）。

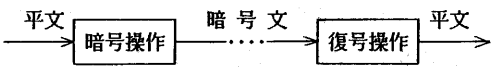


図4．1　ECBモード

（2）CBCモード（Cipher Block Chaining ）

図4．2にCBCモードのブロック図を示す。送信側では64ビット単位に暗号文をフィードバックし、平文ブロック64ビットとEORをとる。受信側では、受信系列を64ビット単位にフィードフォワードし復号器出力と64ビット単位でEORをとり、平文ブロックを復元する。

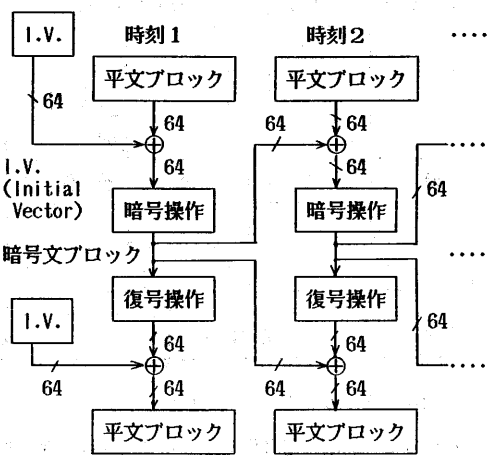


図4．2　CBCモード

（3）CFBモード（Cipher Feed Back）

図4．3にCFBモードの動作を示す。このモードは適当な I.V.（Initial Vector）を暗号化した64ビットのうちKビット単位で平文のKビットとEORをとり伝送路へ出力し且つ入力側にフィードバックする。受信側ではこれと逆操作を施すことにより平文データを再生する。

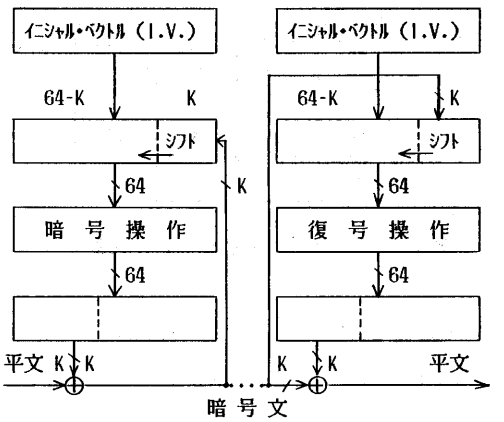


図4．3　CFBモード（Kビット）

（4）OFBモード（Outoput Feed Back ）

図4．4にＯＦＢモードのブロック図を示す。これはＣＦＢモードと似ているが、帰還の方法が異なり誤り伝播がない。このため、品質の悪い通信路での暗号通信に適している。

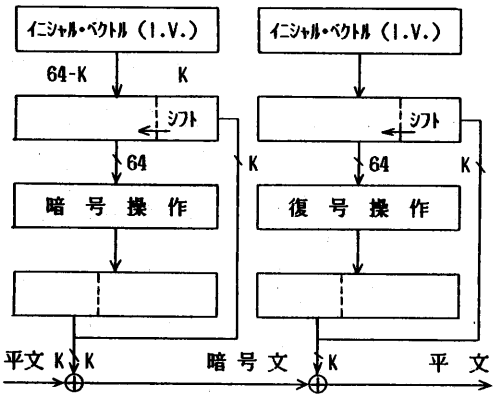


図4．4　ＯＦＢモード（Ｋビット）

ＥＣＢモードは、暗号化アルゴリズムを繰り返しそのまま用いているので、

（ｉ）鍵を固定した場合、同一の平文は常に同一の暗号文に変換される

（ii）伝送路での単一誤りが復号後６４ビットに波及する

（iii）暗号文を正しく復号するにはブロック同期やフレーム同期が必要である

等の問題がある。上記（ｉ），(ii),(iii）の問題点から各モードを特徴付けると表4．1のようになる。

	(i)	(ii)	(iii)
CBC	○	×	×
CFB	○	×	○
OFB	○	○	○

表4．1　各暗号利用モードの性能

5．暗号処理ハードウェア［30］

今までに発表されている主なＤＥＳ－ＬＳＩについては［30,20,21,22］を、ＲＳＡ－ＬＳＩについては［30,23,24］を参照されたい。

6．暗号化技術の応用

暗号化技術の第一の目的は送受信者間の秘密通信の実現にある。しかし、公開鍵暗号方式の特徴を利用することにより、ディジタル署名、鍵配送が比較的容易に実現できる。本節では、公開鍵暗号方式によるディジタル署名、及び公開鍵配送方式（Public-Key Distribution System）と呼ばれる鍵配送方式について述べる。

6．1　ディジタル署名

ディジタル信号により通信を行う場合、声色や筆跡等の特徴により送信者を認識することは一般に不可能であり、また第３者によるコピーも容易であるので、ディジタル情報に適用できる認証方式（ディジタル署名方式）が必要となる。

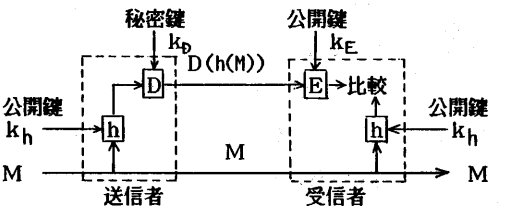
ディジタル署名は、次の３条件、

（１）署名文が第３者によって偽造できない

（２）署名文が受信者によって偽造できない

（３）署名文を送ったという事実を送信者が後で否定できない

を満たすことが要請される。　条件（３）は（信頼できる）調停者を置かない限り実現出来ないが、条件（１），（２）に関しては、公開鍵暗号系を用いることで容易に実現できる（図６．１参照）。



h：任意の一方向性関数（可逆である必要はない）

図6．1　ディジタル署名

ＲＳＡ暗号系を例にとって考えてみる。hは任意の一方向性関数で必ずしも可逆である必要はない。送信者は、平文情報Mにhを施し、h（M）を求め、これに自分の秘密鍵dにより署名文S

$$S \equiv \{h(M)\}^{d} \pmod{n} \qquad (6.1)$$

を計算し受信者に伝送する。受信者は、署名文Sに対

し送信者の公開鍵eを用いて、

$$S^e \equiv \{h(M)\}^{de} \equiv h(M) \pmod{n} \quad (6.2)$$

を求めると同時に、直接送られてきた平文情報Mからh(M)を計算し、両者が等しいかどうかを調べることで送信者の身元を確認する。

このディジタル署名法は改良型ディジタル署名法と呼ばれ、一方向性関数hにR暗号の暗号化関数を用いる方法[25]、DESのCBCモードを用いる方法[26]等が提案されている。

上記以外のディジタル署名方式としては、通信文復元法、認証子照合法があり、また調停者の有無により調停署名、直接署名に分類される。以下、これらについて簡単に説明する。

（1）通信文復元法

送信者は意味のある平文に対し、復号用の鍵k_Dを用いて復号変換を施し署名文を生成し受信者に送る。受信者は、送られてきた署名文に対し、暗号化鍵k_Eを用いて暗号化変換を施し通信文を復元する。復元された通信文が意味のあるものならば受信者は通信文の送信者と内容が正当であると認証する。しかし、この方式は復元された通信文の意味処理が困難であるという欠点を有する。

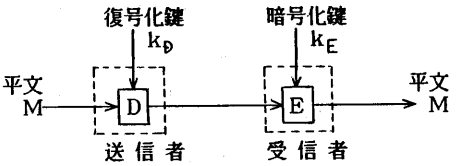


図6．2 通信文復元法

（2）認証子照合法

送信者は通信文に秘密鍵k_hでスクランブルhを施して認証子を生成し、生のままの通信文とともに受信者に送る（ここでスクランブル関数hは任意の一方向性関数で必ずしも可逆である必要はない）。受信者は送られてきた通信文に同一の秘密鍵k_hでスクランブルhを施し、送られてきた認証子と一致するかどうかをチェックする。もし一致したならば受信者は、通信文の送信者と内容が正当であると認証する。この方式は、送受信者間で同一の秘密鍵保有しなければならないので鍵配送が困難であるが、意味処理が不要であるという利点を有する。

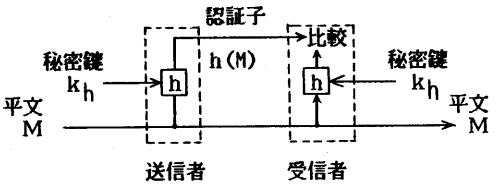


図6．3 認証子照合法

（3）改良型ディジタル署名

通信文復元法と認証子照合法を組み合せ、互いの欠点を補った方式である。

これらの特徴を表6．1にまとめる。

署名法			安全性条件		
暗号法	検査法	構成法	1	2	3
慣用暗号	通信文復元法	直接署名	○	×	×
		調停〃	○	×	○
	認証子照合法	直接〃	○	×	×
		調停〃	○	×	○
公開鍵暗号	通信文復元法	直接〃	○	○	×
		調停〃	○	○	○
	認証子照合法	直接〃	○	○	×
		調停〃	○	○	○
	改良型ディジタル署名法	直接〃	○	○	×
		調停〃	○	○	○

○：満たす　×：満たさない

表6．1 各署名法の特徴

6．2 公開鍵配送方式

公開鍵暗号系では送受信者間で共通の秘密鍵を保持することはないので鍵配送の必要はないが、慣用鍵暗号系においては鍵配送は重要な問題である。本節では公開鍵配送方式[8]（Public-Key Distribution System：PKDS）として知られる方式について簡単に述べる。

まず次のような一方向性関数を考える。

$$y \equiv a^x \pmod{p} \quad (6.3)$$

（p：素数，a：原始根，$1 \leq x \leq p-1$）

式（6．3）において、xからyを求めるのは容易

であるが、yからxを求めるのは離散対数（Discrete Logarithm）と呼ばれ極めて困難である。A、Bが秘密鍵を共有する場合は、上記の一方向性関数を用いて以下の様な手順で鍵配送を行う。

A、Bはそれぞれ任意に乱数r_A、r_Bを生成する。素数P、原始根aを公開とし、AはBに

$$S_A \equiv a^{r_A} \pmod{p} \qquad (6.4)$$

BはAに

$$S_B \equiv a^{r_B} \pmod{p} \qquad (6.5)$$

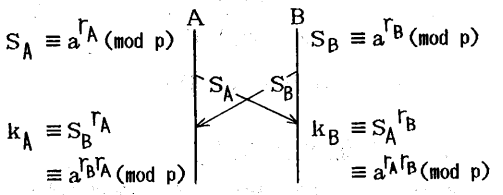
をそれぞれ伝送する。AはBから送られてきたS_Bと乱数r_Aから

$$k_A \equiv S_B{}^{r_A} \equiv a^{r_B r_A} \pmod{p} \qquad (6.6)$$

を、BはAから送られてきたS_Aと乱数r_Bから

$$k_B \equiv S_A{}^{r_B} \equiv a^{r_A r_B} \pmod{p} \qquad (6.7)$$

をそれぞれ計算する。式（6.6）、（6.7）より$k_A = k_B$であるから、以上の手順によりA、B間で鍵k（$=k_A=k_B$）を安全に共有することができる。第3者がこれと同一の鍵を得るには、S_A（$\equiv a^{r_A} \pmod p$）あるいはS_B（$\equiv a^{r_B} \pmod p$）からr_Aあるいはr_Bを求めなければならず、これは先に述べた離散対数問題を解くことになるので極めて困難である。図6.4に公開鍵配送方式のブロック図を示す。



p，a：公開，　r_A，r_B：任意乱数

図6.4　公開鍵配送方式

以上がPKDSの基本的な考え方であるが、これ以外にも幾つかの方式が提案されている［27, 28］。

【参考文献】

1.一松信：データ保護と暗号化の研究（日本経済新聞社）
2.一松信：暗号の数理（ブルーバックス）
3.Diffie,W and Hellman,M.E.,"Exhaustive Cryptanalysis of NBS Data Encryption Standard,"Computer,vol.10 No.6,pp.74-84,June,1977
4.Yasaki,E.K.,"Encryption Algorithm ; Key Size is the Thing," ibid,vol.22,No.3,pp.164-166,Mar.1976
5.Schltz,B.,"DES Critic Says He Can Crack Code for S 23," COMPUTER-WORLD,pp.15,June,19,1978
6.宮口他，"暗号／認証アルゴリズム強度評価指標"，信学技報 CS85-146,pp.75-82,1986
7.宮口他，"暗号強度指標と暗号の国際標準化"，1986年暗号と情報セキュリティシンポジウム資料
8.Diffie,W and Hellman,M.E.,"New Directions in Cryptography," IEEE,vol.IT-22,No.6,pp.644-654,Nov.1976
9.Rivest,R.L.,Shamir,A. and Adleman,L.,"A Method for Obtaining Digital Signatures and Public=Key Cryptosystem," Com. of ACM,vol.21,No.2,pp.120-126,1978
10.Williams,H.C.,"A Modified of the RSA Public-Key Encryption Procedyre," IEEE,vol.it-26,No.6,pp.726-729,Nov.,1980
11.Williams,H.C.,"Some Public-Key Crypto-Functions as Intractable as Factorization," Advances in Cryptology,Proc.of Crypto 84,pp.66-70,1984
12.Merkle,R.C. and Hellman,M.E.,"Hiding Information and ignatures in Trapdoor Knapsacks," IEEE,vol.IT-24,No.5,pp.525-530,Sept.1978
13.Chor,B. and Rivest,R.L.,"A Knapsack Type Public Key Cryptosystem Based on Arithmetic in Finite Fields," Advances in Cryptography,Proc.of Crypto84 pp.54-65,1984
14.Aho et.al,"アゴリズムの設計と解析"(サイエンス社)
15.Dixon,J.D.,"Asymptotically fast factorization of integers," Math.of Comput.,vol.36,No.153,Jan.1981
16.McEliece,R.J.,"A public-key cryptosystem based on algebraic coding theory," DSN Progress Rep.,pp.42-44,Jet Propulsion Lab.,Jan.and eb.,1978
17.Elgamal,T.,"A public-key cryptosystem and a signature scheme based on discrete logarithm," IEEE vol.IT-21,n0.4,July,1985
18. 松本他，"多変数多項式タブル非対称暗号系" 信学技報 IT85-88,pp.55-60,1986
19. 辻井他，"非線形連立方程式の順序解法による公開鍵暗号方式" 信学技報 IT85-90,pp.67-72,1986
20.Fairfield,R.C.et.al.,"An LSI Digital Encryption Processor (DEP)," Advances in Cryptography,Proc.of Crypto84,pp.115-143,1984
21.Davio,M.et.al.,"Efficient Hardware and Software Implementation for the DES," Advances in Cryptography,Proc.of Crypto84,pp.144-146,1984
22.Hoornaert,F.et.al.,"Efficient Hardware Implementation of the DES," Advances in Cryptography,Proc o of Crypto84,pp.147-173,1984
23.Rivest,R.L.,"A Description of a Single-chip Implementation of the RSA Public-Key Cryptosystem," NTC Conference Record,vol.3,1980
24. 宮口庄司，"RSA公開鍵暗号系の高速計算法と暗号LSIの構成"，情報処理学会論文誌，vol.24,No.6,pp.764-771 Nov.1983
25. 小山謙二，"公開鍵暗号による高速かつ安全なディジタル署名法"，信学論，vol.J67-D,No.3,pp.305-310,1984
26.Davis,D.W.,"Applying the RSA Digital Signature to Electronic Mail," IEEE Computer ,pp.55-62,1983
27. 岡本他，"多項式演算によるディジタル署名方式"，信学論，vol.J68-D,No.5,pp.1157-1164,1985
28. 松本他，"複数局が秘密の共有情報を生成するための方法について"，信学技報 IT85-34,pp.13-18,1985
29. 高木貞治：初等整数論講義　第2版（共立出版）
30. 秋山，八星：暗号処理ハードウェア　bit vol.17, No.10,pp.104-114,0.1985