解　説

公　衆　暗　号　系†

土居範久†† 広瀬　健††† 西村恕彦††††

1. はじめに

暗号は，古来より軍事，外交面に使用されてきているが，特に，データベースおよびデータ通信網の発達により，計算機システム全般にわたる暗号技術の研究と開発が，米国を中心に急激に進展しつつある．我が国でも，暗号についての解説書や調査報告書* が出され始めた．商業上の取引き，契約など企業機密にかかわるもの，銀行業務などの金銭にかかわるもの，医療情報，住民台帳など個人の機密にかかわるものなど，保護の対象となるものは多数ある．これらの社会的要請に加えて，相当に複雑な暗号化および復号が比較的高速でしかも経済的に行えるようになった技術的な背景もある．

こうしたことから，米国商務省標準局は暗号化アルゴリズムを 1973 年に公募し，1977 年にデータ暗号化規格 (Data Encryption Standard. DES と呼ぶ) を制定した[1),3)]．これに対し，1976 年，W. Diffie と M. Hellman が**公開鍵暗号系** (public-key cryptosystem) を提案した[2)]．これ以降，これまで一般に用いられてきたものは**慣用の暗号系** (conventional cryptosystem) と呼ばれるようになった．慣用の暗号系と公開鍵暗号系の重要な相違点は，鍵を用いる方法にある．慣用の暗号系では暗号化および復号に対し**同一の鍵**を用いるのに対し，公開鍵暗号系では暗号化と復号に**異なった鍵**を用いる．

DES は慣用の暗号系であるが，その手順が公開されていること，利用形態が公衆的であることから，**公衆暗号系** (public cryptosystem) とみなすことができる．また，ここ当分は，データ伝送の分野では DES が主流であろうことが予想される．

DES も公開鍵方式も，それらが安全である根拠は，無条件安全性ではなく計算安全性にあることを認識しておく必要がある．

本解説では，暗号系の基本的な概念，DES の思想と方法の概略および公開鍵暗号系の思想と方法の概略について述べる．

2. 暗号系の基本的な概念

ここでは，暗号についてほとんど知識のない人たちのために，その基本的な概念を解説する．

2.1 安全な通信路

通常の暗号は，通信との関連で使用されてきた．その様子を**図-1** に示す．(通信以外の用途としては，情報の保存と検索，たとえばデータベースがあり，そこでは異なった概念が必要である．)

暗号は，高速な通信回線を安全かつ経済的に確保することが不可能であるために，採用される．現代の通信は大部分が無線であって，第三者が簡単にこれを傍受できる．暗号は，傍受可能な，というよりはもともと公開されている通信回線の上で，安全に情報を伝達する手段である．

暗号系を利用できるためには，通常の通信回線のほかに，**安全な通信路**をもっていなければならない．この通信路では，何を送るのだろうか？　それは，暗号の方式と鍵 (key) である．このような通信路が必須で

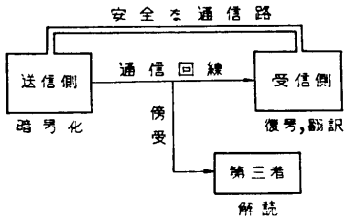

図-1　通信系の概念

† Public Cryptosystems by Norihisa DOI (Institute of Information Science, Keio University), Ken HIROSE (Dept. of Mathematics, School of Science and Engineering, Waseda University) and Hirohiko NISHIMURA (Dept. of Information Science, Faculty of Engineering, Tokyo University of Agriculture and Technology).

†† 慶応義塾大学情報科学研究所
††† 早稲田大学理工学部数学科
†††† 東京農工大学工学部数理情報工学科

* たとえば，協同システム開発株式会社による「市場創出型プロジェクト――“公開鍵方式暗号系”に関する調査研究報告書 (JSD 9-10-PKCS)」などがある．

ある．

暗号についての知識のない人は，方式と鍵を当の暗号文に添えて送ることを考えたりする．あるいは，次回以降に使うべき新しい方式や鍵を，もとの暗号で組んで送ればよいと考えたりする．それは，暗号の強度を副次的に補強するのに利用されることはあるが，本質的に主要な技法とはなりえない．たとえば，いったんこの暗号文が第三者によって破られてしまうと，以後は暗号系の秘密を維持できなくなることからも，明らかであろう．

ただし，高度の，また複雑な（つまり強度の強い）暗号を用いて，より低水準の暗号のための鍵などを送るようなことは可能である．その逆に，弱い暗号を用いて強い暗号の鍵を送ることは，無意味であり，不可能である．

通常の通信回線としては，無線などのごく常識的な通信手段が採用されるのに対して，安全な通信路の方は，特別の任務をもった人間が，直接，書類を携行するなどの能率の悪い手段を，一般には採用せざるをえない．たとえば第二次大戦中の日本軍は，潜水艦や飛行機によって暗号書の配布を行っていたという．米ソ間のホットラインは，海底電線および無線のテレタイプであるらしい．そしておそらく，通信文と同量（つまり大量）の乱数鍵を，事前に外交官が携行するのであろう．これが安全な通信路である．

暗号の鍵は一種の消耗品であって，それを用いた暗号文を送信することによって，徐々に消費されてゆくものである．

暗号は，同一の鍵を繰り返して使えば破られる．したがって，暗号通信の量に比例して，安全な通信路を介して鍵を補給することが，必須である．

2.2 暗号通信員の仕事

現代の暗号機械は，小型のタイプライタないしテレタイプ程度の大きさで，操作性も似たものである．

暗号文の送信にあたって，通信員は，まず所定の数けたの文字（鍵）をセットする．これが擬似乱数列の初期値になる．そして平文を打鍵すると，暗号文が出力される．出力は，表示，印字，穿孔テープなどである．

暗号文の受信にあたっては，まず所定の鍵(初期値)をセットし，暗号文を入力すると，復号された平文が出力される．

暗号機械においては，擬似乱数列を生成する算法は機械の構造によってきまっており，つまりそれは公知のものである．暗号の安全は，基本的に鍵（初期値）を隠すことによって保たれる．ただし，擬似乱数列の初期値だけでなく，その算法に含まれる係数に相当するものもまた，実は設定・変更可能なのであって，これの方が実はさらに厳重に隠される．

その意味では，鍵は2段になっているということもできる．

2.3 暗号機械の弱点

ここでは，暗号文を傍受した第三者が，暗号文を解析することによって，鍵や原文を発見できるという観点から，暗号機械の運用上の注意を述べる．

擬似乱数列の周期が長いことは，望ましい条件ではあるが，十分な条件ではない．通常の暗号機械の擬似乱数列は，比較的短い周期（小周期）の乱数を規則的に修正しながら繰り返してゆくことによって，長い周期を実現している．

一つの初期値から出発して，このような擬似乱数列を連続的に使用したときに，暗号文の長さがある上限を超えると，その暗号文を解析することによって，小周期を検出し，暗号を破ることが可能になる．

同文の電報を多くのあて先に送りたいことがある．あて先ごとに鍵を変えて暗号化して，送信したらどうだろうか．その方が安全ではなかろうか．あるいは，受信地によって強度の異なる暗号系が配布されていることがある．弱い暗号系をもっている受信地には弱い暗号化によって送り，強い受信地には同じ原文を強い暗号で送る．この方が安全ではなかろうか．

実は話はまったく逆である．同一の原文を異なった鍵によって暗号化した暗号文を対照すると，その暗号を破ることができる．

暗号機械を操作するときには，鍵（初期値）をセットして開始する．この鍵は，安全な通信路を介して事前に配布されている．この配布はさまざまの困難を伴うので，なるべく配布する鍵の量は少なくしたい．

そこで，同一の鍵（初期値）を用いて，何通もの暗号文を組み立て，送信することがある．ところが，同一の鍵を用いた暗号文が何通もあるときには，それらを対照することによって，その暗号を破ることができるのである．

電文ごとに異なった鍵を用い，しかも鍵の配布量を減らす工夫として，鍵（初期値）を規則的に修正してゆく方法をとることもできる．これによって暗号系の強度を強めることができるが，通常の暗号機械では，その規則的な修正の痕跡が暗号文の上に現れる．した

がって，完全な解決になるわけではない．

2.4 ホットラインの暗号方式

米ソ間のホットラインに使われている暗号系は，第三者が破る（解読する）ことの不可能な，最も高度なものであると信じられている．しかしその機械は，驚くほど簡単なものであろう．

おそらく，二つの入力部と一つの出力部をもったテレタイプを想定すれば十分であろう．通信員は，平文の紙テープと鍵の紙テープを並行して入力する．機械は，両者のビットの排他的論理和をとって暗号文とする．受信側では，暗号文の紙テープと鍵の紙テープを入力すると，両者の排他的論理和をとることによって，平文に復号される．

本質的にそれだけの方式であろう．これが解読不能である秘密は，鍵にある．鍵として，不規則な無限乱数列を用い，それを1回限りで使い捨ててゆけば，その暗号系は解読不能である．

この単純な方式がホットライン以外では採用できない理由もまた，鍵にある．無限乱数列を作り出し，それを通信文と同量だけ，安全な通信路を介して事前に受信側に渡しておかなければならない．これは，ホットラインなればこそ許される，途方もないぜいたくである．

2.5 復号と解読

広く誤解され，誤用されていることであるが，復号と解読という二つの概念と用語を，明確に区別しておこう．

復号 (decode, decipher) は，受信側にいる暗号通信員の作業を指す．すなわち，暗号文を受信して暗号機械の前に座り，事前に配布されている鍵をセットする．暗号文を打鍵すると，平文が出力される．

暗号機械を用いない場合には，所定の方式と鍵に従って文字を置き換え，あるいはコードブックを引いてコードを語句に置き換える．このような書記的な作業の積み重ねが復号である．

それに対して，暗号文を傍受した第三者の行う複雑な作業が**解読** (cryptanalysis, codebreaking) である．一般には，方式や鍵について事前の知識は何もなく，ただ暗号文だけを資料として，解析を行う．個々の暗号文に対応する平文を見い出すこと以上に，それらの暗号文に適用されている暗号系の方式や鍵，また鍵を作り出す規則などをあばきだすことに，大きな価値がある．

第三者によって暗号文が解読されていることが判明した場合に，暗号の方式をそのままにしておいて，鍵だけを更新しても，ほとんど効果がない．より強度の強い，新しい方式を導入すべきである．その方式およびそこで用いられる新しい鍵は，どうやって伝達するのであろうか．もとの暗号系によって送信することは無意味である．前に述べた「安全な通信路」が，そのために必要なのである．

さて暗号解読の作業は，次のような手順からなる．

（a） 暗号系の強度の測定　暗号文を解析することによって，その暗号系の強度を知ることができる．これが解読の第一歩である．

（b） 方式の推定　実用化されている暗号の方式は，ほとんどが公知であると考えられる．総当りに検討していって，かなり確実性の高い推定ができる．

（c） 鍵の判定　大部分の暗号系においては，暗号の安全は鍵の秘匿に頼っている．したがって鍵の判定は最も困難な作業であって，統計的手法と発見的手法を混合して適用する．

暗号解読者の利用できる武器は，統計学と組合せ数学である．事前の準備として，原文の言語に対する記述統計学的な測定が必要である．文字・文字列の出現確率，母音の出現間隔などといった変量によって，母統計量を定めておく．

暗号文に対応する原文は，その言語の母集団からの一つの標本と考えられる．ある標本について統計量を測定する．変量が正規分布するときには，母平均からの規準化された偏差の2乗和が χ^2 分布に従う．このようにしてその標本が，想定された母集団からの無作為標本である尤度を算出することができる．

一つの暗号文に対して，ありうる鍵を次々に適用して，候補原文をいくつか作り出す．候補原文のそれぞれについて尤度を算出して比較し，候補の原文と鍵を評価することができる．これは，推測統計学の手法そのものである．

一方，鍵の種類は，たとえば26! 通りというふうに，全数検査することの到底不可能な数が選ばれている．したがって，発見的な手法によって組合せの数を削減していかなければならない．

2.6 暗号の方式

暗号の方式は無数にあるといってもよいが，まず初等的には，転置式と換字式を理解しておく必要がある．

転置式 (transposition) とは，原文中の個々の文字の値は変えることなく，文字の位置を組み替えるもので

ある．置換の表示が鍵になる．10文字単位で内部を組み替えるとすると，鍵は10!通りあることになる．

換字式 (substitution) とは，原文中の個々の文字の値を変更し，文字の位置つまり送信順は保存するものである．アルファベットであれば，26文字を26文字に置き換える置換の表示が鍵になり，それは26!通り可能である．

両者の区別は絶対的なものではない．たとえば，送信する各符号内のビット位置を組み替えれば，技術的には転置式であっても，外見上は文字の値が置き換えられることになる．またたとえば，10文字単位で文字位置を組み替えることは，長さ10の文字列の値を置き換えることになる．

換字の算法にはいろいろなものがあるが，次の形式のものは特に興味がある．

$$\text{鍵} \ominus \text{平　文} \longrightarrow \text{暗号文} \pmod{n}$$
$$\text{鍵} \ominus \text{暗号文} \longrightarrow \text{平　文} \pmod{n}$$

この形式によれば，暗号化と復号とがまったく同じ手順・機構で操作できる．法nとしては，2, 10, 26などが採用され，$n=2$のときは，排他的論理和演算となる．

理論的には面白みが少ないが，実用的に広く用いられる方式として，コード式 (code) がある．これは，コードブック（辞書）を引いて，語句や文字列をコードに置き換えるものである．自然言語のもつ冗長性を圧縮できるので，通信文の長さを短縮し，かつ強度を強くできる．

コードブックの大きさがある限界を超すと，実用的には第三者の解読を許さないだけの強度をもつようになるが，反面，その大きいコードブックを安全な通信路で配布し，かつそれを受信側で安全に保管することが困難になる．

実際の暗号系においては，転置式，換字式，コード式の中間的な方式もあり，また幾つかの方式を多段階に適用するのが普通である．

後述のDESの方式[1]は，56ビットを単位として，ビット位置を転置し，ビット値を換字するものであるが，その結果は，長さ8の文字列を同じ長さのコードに置き換えることに相当する．

長さ8のあらゆる文字列をコードに置き換えるということは，きわめて大型のコードブックに相当し，経験的にも高度の強度が期待される．しかもコードブックの配布と保管がきわめて容易かつ安全に行える利点がある．

DESにおいては，鍵の小さな一部分だけを変更しても，その影響がコードブックの全般に及ぶ．したがって，鍵を規則的に修正していっても，その規則の痕跡が暗号文の上に現れにくい．このこともDESの運用上の利点である．

3. DESの思想と方法の概略

米国商務省標準局 (NBS) は暗号化のアルゴリズムを1973年3月に公募した．それに対し，IBM社が1975年に発表したシステムを提出し，NBSにより連邦情報処理規格案として採用された[1),3),4)]．最終案は1977年1月15日に公布され，6箇月後の1977年7月15日に規格として発効した．一般に，**データ暗号化規格** (Data Encryption Standard)，**DES**，IBMアルゴリズム，NBSアルゴリズムと呼ばれる．

DESは転置と換字を組合せた混合方式によるブロック暗号であって，慣用の暗号系である．

3.1 DESの暗号化と復号

DESのアルゴリズムは，64ビットからなるデータのブロックを64ビット（うち8ビットはパリティビット）の鍵の制御の下で暗号化および復号するように設計されている．復号は暗号化に用いたのと同じ鍵を用いて行う．ただし，鍵のビットの位置指定は，復号処理が暗号化処理の逆になるように定められる．

暗号化するブロックは，**初期転置** (initial permutation, IP) が施された後，鍵に従属した複雑な計算が施され最後に初期転置の逆転置 IP^{-1} が施される．鍵に従属した計算は，**暗号関数** (cipher function) f と**鍵決定** (key schedule) と呼ばれる関数 KS とを用いて定義できる．

以下では，ビットで構成される二つのブロックLとRを与えたとき，LRはLのビットの後にRのビットが続いた一つのブロックを示す．

3.2 暗 号 化

暗号化の概要を**図-2**に示す．ここで，鍵に従属した計算の結果を**前出力** (preoutput) と呼ぶ．この計算は，IPによって転置された入力ブロックを入力として用い，要出力ブロックを作成するものであって，暗号関数fで記述されている16回繰返される計算から構成されている．IPおよび前出力に施すIP^{-1}を**図-3**に示す．

暗号関数fは，それぞれ32ビットと48ビットから成る二つのブロックに作用し，32ビットのブロックを作成する．入力ブロックの64ビットの左32ビットをLとし，右32ビットをRとすると，入力ブロックは

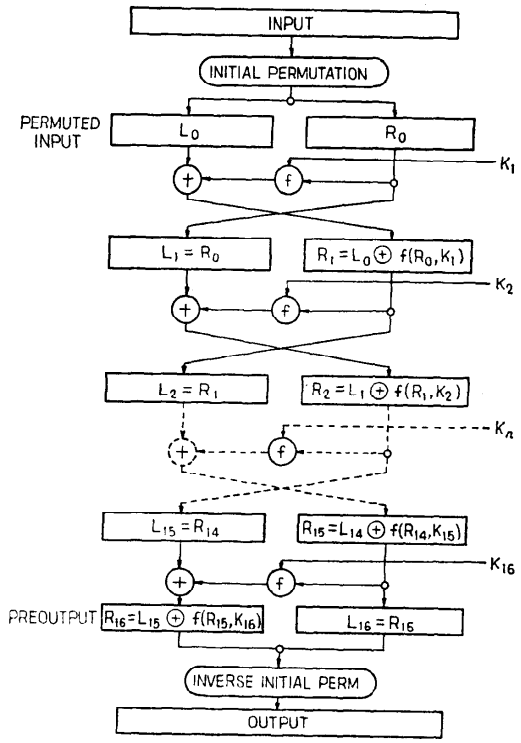

図-2 DES の暗号化の概要

LR と表わせる．64 ビットの鍵から選出した 48 ビットのブロックを K とすると，入力 LR に対して 1 回の繰返し操作の出力 $L'R'$ は，次のように定義できる．

（1） $L'=R$

$R'=L\oplus f(R,K)$

ここで，$\oplus$ は排他的論理和を表わす．

$L'R'$ が 16 回の繰返し後の出力とすると，$R'L'$ が前出力ブロックになる．各々の繰返しでは，64 ビット

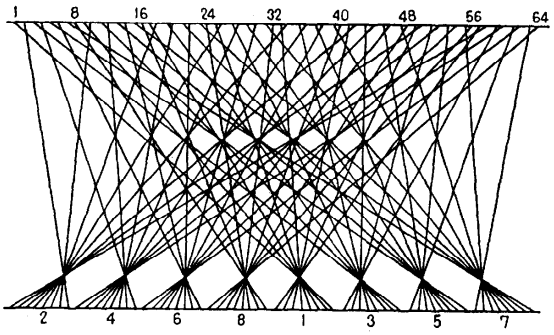

図-3 初期転置 IP および逆初期転置 IP^{-1}

の鍵 KEY から選出された相異なるブロック K が用いられる．

繰返し行われる計算をさらに詳細に記述すると次の通りである．整数 n $(1\leq n\leq 16)$ および 64 ビットの鍵 KEY を入力としてとり，KEY のビットを転置して選出された 48 ビットのブロック K_n を出力する関数を KS とすると，

（2） $K_n=KS(n,KEY)$

である．K_n は KEY の相異なるビット位置を占める 48 ビットで定められる．（1）の n 回目の繰返しで用いられるブロック K が（2）で定まるブロック K_n であるので，KS は鍵決定と呼ばれる．転置後の入力ブロックを LR とし，L_0, R_0 をそれぞれ L, R とする．（1）の L, R をそれぞれ L_{n-1}, R_{n-1} とし K を K_n として，L', R' をそれぞれ L_n, R_n とすると，

（3） $L_n=R_{n-1}$

$R_n=L_{n-1}\oplus f(R_{n-1},K_n)$

となる．ここで，$1\leq n\leq 16$ である．$R_{16}L_{16}$ が前出力ブロックである．

3.3 復 号

前出力ブロックに適用される転置 IP^{-1} は IP の逆転置である．さらに，（1）より

（4） $R=L'$

$L=R'\oplus f(L',K)$

である．したがって，復号するには，各々の繰返しの計算で，そのブロックを暗号化する間に用いたのと同じ鍵ビット K を使うようにすれば，まったく同じアルゴリズムを暗号文に適用すればよい．これは，次のように表わせる．

（5） $R_{n-1}=L_n$

$L_{n-1}=R_n\oplus f(L_n,K_n)$

ここで，復号計算に対する転置後の入力ブロックは $R_{16}L_{16}$ であり，前出力ブロックは L_0R_0 である．

3.4 暗 号 関 数

$f(R,K)$ の概要を図-4 に示す．E は 32 ビットのブロックを入力として，48 ビットのブロックを出力する拡大転置である（図-5）．$S_i(1\leq i\leq 8)$ は**選択関数** (selection function) と呼ばれるもので，DES の強さは，この選択関数にある．各々の S_i は 6 ビットを受けとり 4 ビットを出力する縮小換字である．B を 6 ビットブロックとしたとき，$S_i(B)$ は次のようにして定められる（表-1 参照）．B の最初と最後の 2 ビットで 2 を底とする数 i を表わすと，$0\leq i\leq 3$ である．B の残りの 4

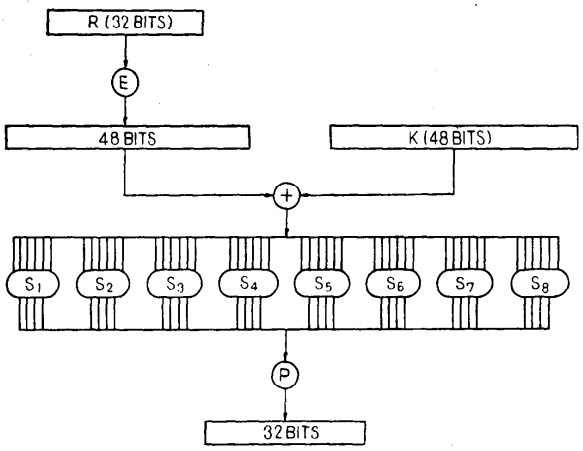

図-4　$f(R, K)$ の概要

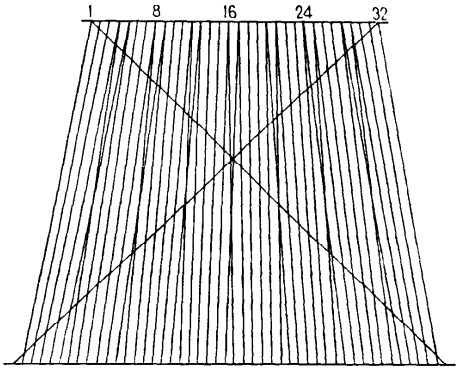

図-5　拡大転置 E

ビットで2を底とする数 j を表わすと，$0 \leq j \leq 15$ である．この i と j を用いて表を引き，i 行 j 列にある数を $S_1(B)$ の値とするのである．

P は図-6に示すような転置である．

3.5　鍵決定の計算

鍵決定の計算の概要は図-7のようになる．ここで PC-1 (permuted choise 1) は 56 ビットの転置であり，PC-2 (permuted choise 2) は 56 ビットを 46 ビットにする縮小転置である．

4. 公開鍵暗号系の思想と方法の概略

1976年に発表された W. Diffie と M. E. Hellman の論文[2]は，これまでの暗号系の研究に転機をもたらした．暗号系は，これまでに用いられてきたものを慣用の暗号系，Hellmanらの提案による方式を公開鍵暗号系と大別して議論されるようになっている．

ここでは，この公開鍵方式の背景と方式の概略を述べる．

4.1　公開鍵方式の背景

「暗号系の基本的な概念」で述べたように，暗号系に関わる一つのポイントは“安全な通信路”である．暗号の方式や鍵はこの通信路によって，安全に配布されなくてはならない．しかも，実用上，この配布は経済的に行われなくてはならない．

一方，計算機とさまざまな通信手段との結合がすすみ，いわゆる“電子郵便”などの情報伝達処理系の実現は間近いと考えられる．この処理系を考えるとき，その情報の機密を保持するための手段は暗号系の導入であろう．さて不特定多数の相互間通信で，情報交換を行うグループの人数を n 人とすれば，起り得る組合せは

$${}_nC_2 = n(n-1)/2$$

である．すなわち，この場合，慣用の暗号系で用意しなくてはならない鍵の個数は $n(n-1)/2$ で，鍵の個数は n^2 に比例して増加する．それだけの経済的で安全な通信路を確保することは不可能であろう．

Diffie-Hellman の提案した公開鍵方式では，鍵の個数は n に比例してふえるだけである．しかも，“安全な通信路”が不要になる[4),6)]．

4.2　公開鍵方式

慣用の暗号系では暗号化の鍵と復号のための鍵は同一のものである．復号のさいには，いわば暗号化の場合の逆に鍵を回す．

これに対して公開鍵方式では，暗号化の鍵と復号の

表-1　S_1

行＼列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

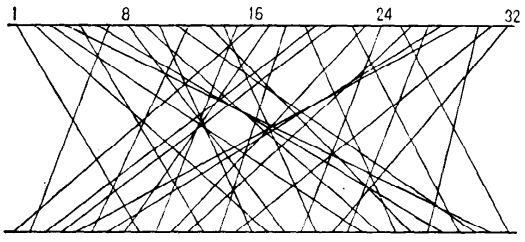

図-6　P

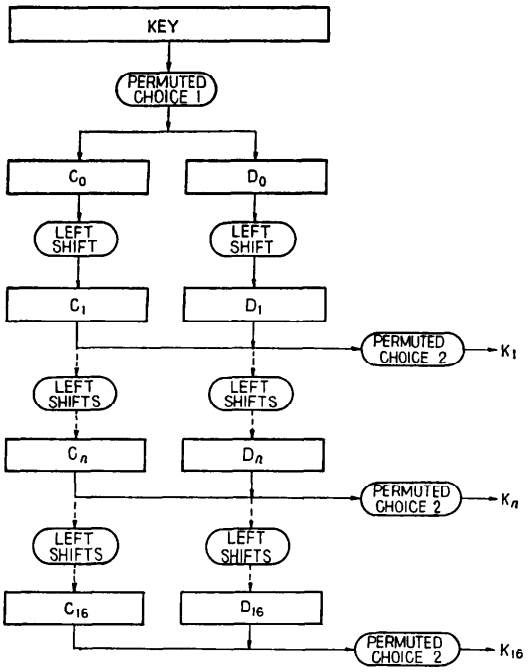

図-7 鍵決定計算

ための鍵を分離し，**暗号化の鍵は公開する**．

A氏は暗号化の鍵 K_e を公開し，復号のための鍵 K_d を極秘に保持する．

（1） A氏への暗号文送信者たちは，A氏の公開鍵 K_e を用いて暗号文を作り送信する．

A氏に送りたい平文を M とし，K_e を用いて暗号化する手続きを E とし，M に E を適用した結果を $E(M)$ と書けば，送信される M の暗号文 C は，

$$C=E(M)$$

である．

（2） A氏は受信した暗号文 C を，A氏のみが知る復号鍵 K_d を用いて復号し平文にする．

K_d を用いて復号する手続きを D とし，C に D を適用した結果を $D(C)$ と書けば，

$$M=D(C)$$

であり，ここで，C を復号できるのは，自ら秘匿している復号鍵 K_d をもつA氏のみである．

かくて，鍵の配布問題は解決され，安全な通信路は不要となる．すなわち，暗号化の鍵は公開されるのであり，復号のための鍵は各個人自らが保持する．

4.3 公開鍵方式が成立する条件と“署名”を可能にする条件

上述の方式が暗号系として意味をもつために，公開鍵 K_e から秘匿されている鍵 K_d が，割り出せないものでなくてはならないのは当然である．それは，原理的に割り出し不可能である必要はないが，実際上，割り出し不可能でなくてはならない．

このような公開鍵方式が成立するための条件をまとめておこう：

（i） すべての M に対して，$E(M)$, $D(E(M))$ が存在して，

$$D(E(M))=M$$

が成立すること．

（ii） E, D の手続きが比較的簡単であること．

（iii） E から D を割り出すことが，実際上，不可能であること．

ところで，（i）が成立することは，E や D の定義に含まれることで，いわば当然であるが，任意の M に対し $D(M)$ が存在するとは限らない．しかし，もしも上記の（i），（ii），（iii）に加えて

（iv） すべての M に対して，$D(M)$, $E(D(M))$ が存在して，

$$E(D(M))=M$$

が成立すること

を満たすように手続き E, D が選ばれているならば，次のような方法によって送信者の確認を行うこと，つまり送信者の“署名”(**計数署名** (digital signature) という）を確認することが可能になる．

A氏がB氏に通信文 M の暗号文 C を送りたい，B氏は，それがA氏からの通信であることを確認したいとする．そのためには次のようにすればよい：

一般に，X氏の公開暗号化鍵 K_e を用いて行われる暗号化手続きを E_X，X氏秘匿の復号鍵 K_d による復号手続きを D_X と書くことにする．さて，

（1） A氏は M からA氏のみが知る手続き D_A によって

$$D_A(M)$$

を作る（$D_A(M)$ の存在は（iv）で仮定されているから，これは一つの暗号化ともみなせる）．

（2） A氏はさらに，B氏の公開鍵による手続き E_B によって，$D_A(M)$ を2重に暗号化し

$$E_B(D_A(M))$$

を作り（暗号化鍵が公開されているということは，暗号化の手続きが公開されていることを意味する），これを M の暗号文 C として，B氏に送る．

（3） B氏は C を，まずB氏の秘密の復号鍵による手続き D_B によって

$$D_B(C)=D_B(E_B(D_A(M)))$$
$$=D_A(M) \qquad ((\text{ⅰ})\text{による})$$

を作り，さらに

（4） A氏の公開鍵による手続き E_A によって

$$E_A(D_A(M))=M \qquad ((\text{ⅳ})\text{による})$$

を作り，平文 M を得る．

以上の(1)～(4)の手続きのなかで，(2)で E_B による変換が行われており，その逆変換 D_B のためにはB氏の秘密の復号鍵が(3)で必要となるから，復号できるのはB氏のみであり情報の機密は保持される．またA氏以外からの，A氏をよそおった通信は(1)での変換 $D_A(M)$ が行われないから，(4)の E_A を適用しても平文が現われず，“偽の署名”であることがわかる．すなわち，(4)の手続きで平文が現われることによりA氏からの通信であることが確認される．(ただし，著者が“署名”を忌避する問題が生じる)．

4.4 公開鍵方式を実現する具体的方法

上述のような手続き E, D, とくに E を知って D を作ることが不可能であるような手続きは存在するであろうか？

原理的には存在しない．M や C は有限であるから，暗号化鍵，暗号化手続きを知っていれば，すべての場合をチェックすることによって解読は可能である．

しかし，いま求められているのは，原理的にも不可能なものというわけではなく，実際上不可能であれば十分なのである．通信文の内容によっては，1週間，6箇月，あるいは10年間の機密保持で十分というものもあろう．解読に1,000年かかるとすれば，それは永久的な機密保持とほぼ同等の意味をもつ．

具体的に有効な方法が提示されたのは，1978年2月で，MITの，R.L. Rivest, A. Shamir, L. Adlemanらによるもので，“RSA 体系”あるいは“RSA 法”と呼ばれている[5),6)]．

この方法は，素数の判定が比較的容易であるのに対して，素因数分解は非常に手間がかかる，という事実を利用するものである．これらの詳細については，本誌の「展望：公衆暗号系の実現可能性と問題点」にゆずるが，その方法は次のようである：

2つの素数 p, q をとり，

$$n=p\cdot q$$

とおく．次に，

$(p-1)(q-1)$ と互いに素な数 r

と

$d\cdot r\equiv 1 \pmod{(p-1)(q-1)}$ なる数 d

をとる．

この n と r が暗号化のための公開鍵であり，d が復号のための秘密の鍵である．

平文は符号化されて自然数列になっているものとする．その数列を適当に区切って，n より小さい整数 M の列とみなす．

暗号化の手続き $E: M\mapsto C$ は，

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

とする．

復号のための手続き $D: C\mapsto M$ は，

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

である．

この方式が前述の(ⅰ)～(ⅳ)を満たす．

手続き E では，高々 $2\log_2 r$ 回，手続き D では高々 $2\log_2 d$ 回の乗算ですむのに対し，解読に当っては n の素因数分解が必要になり，n が200桁とすれば（つまり，p, q を100桁程度にとれば），現在一番速いといわれる算法でも 1.2×10^{23} もの演算を必要とする．一つの演算を1μ秒で実行するとしても，3.8×10^9 年の時間を必要とする．

1978年9月には，R. Merkle と Hellman が，「1次元詰め込み問題」あるいは「ナップサック問題 (Knapsack problem)」と呼ばれる NP 完全問題に基づく方法を提示した[6),7)]．これは MH 法と呼ばれ，その概略は次のようである：

“s に対する $(a_1, a_2, \cdots, a_n)$ のナップサック問題”とは，「正の実数列 $a_1, a_2, \cdots, a_n$ と正実数 s に対し，$\{a_1, a_2, \cdots, a_n\}$ の部分集合 $\{a_{i_1}, a_{i_2}, \cdots, a_{i_m}\}$ で，その和 $\sum_{k=0}^{m} a_{i_k}$ が，s に等しいか，s より小さくて s にもっとも近いものを求めよ」という問題で，一般には 2^n 種類の組合せを調べれば必ず解がみつかり，逆に，これ以外の有効な算法は知られていない．*

ところが，与えられた数列 $a_1, a_2, \cdots, a_n$ について，

(＊) $a_1+a_2+\cdots+a_{k-1}<a_k$ $(k=2, 3, \cdots, n)$

なる性質があったとすれば，この問題は次のような手続き (♯) で簡単に解が得られる．すなわち，

```
a:=s;
for k:=n step −1 until 1 do
    if a≥a_k then a:=a−a_k; x_k:=1
    else x_k:=0 fi;
```

* ナップサックという言葉は，George B. Dantzig が1957年に，「ナップサックにかん詰めなどを詰め込んでハイキングに行く際に70ポンド以下しか背負えないとき，その効用を最大にする」という例を用いて，新たなORの問題を提起したことに由来するものと思われる．

を実行し，$x_i=1$ となる番号 i の a_i を集めればよいのである．

さて，(*)を満たす正整数 $a_1, a_2, \cdots, a_n$ を選び，

$$(w, n)=1^* \quad \text{かつ} \quad m>a_1+a_2+\cdots+a_n$$

なる整数 w, m をとり，この w, m から

$$w\cdot v\equiv 1 \pmod{m}$$

を満たす v を定める．

ベクトル $(a_1, a_2, \cdots, a_n)$ と，この v が秘密の復号鍵である．

次に，

$$b_i\equiv w\cdot a_i \pmod{m}, \quad i=1, 2, \cdots, n$$

を満たすベクトル $(b_1, b_2, \cdots, b_n)$ を作る．これが公開される暗号化鍵である．

通信文は適当に符号化され，1と0の列に変換されているものとし，これを長さ n に区切り，

$$M=(x_1, x_2, \cdots, x_n), \quad x_i\in\{0, 1\}$$

ごとに送信されるものとする．

暗号化の手続き $E: M\mapsto C$ は，

$$C=\sum_{k=1}^{n} b_k\cdot x_k$$

とする（$(b_1, b_2, \cdots, b_n)$ は暗号化の公開鍵）．

したがって，暗号化手続きの手間は $x_i=1$ の場合の b_i の n 回以下の加算である．

復号のための手続き $D: C\mapsto M$ は，

$$s\equiv v\cdot C \pmod{m}$$

を作り，s に対する $(a_1, a_2, \cdots, a_n)$ のナップサック問題を解くことである（$(a_1, a_2, \cdots, a_n)$，v は復号鍵）．

$$s\equiv v\cdot C\equiv \sum_{k=1}^{n} v\cdot(b_k\cdot x_k)\equiv \sum_{k=1}^{n} v\cdot(w\cdot a_k)\cdot x_k$$

$$\equiv \sum_{k=1}^{n} (v\cdot w)\cdot a_k\cdot x_k\equiv \sum_{k=1}^{n} a_k x_k \pmod{m}$$

であるから，復号のための手間は(♯)の手続きによって，1回の乗算と n 回以下の減算ということになる．

しかし，$n=100$ としても，復号鍵を知らなければ $2^{100}\fallingdotseq 10^{30}$ の組み合せをチェックすることになる．

以上の RSA 法および MH 法が現在知られている代表的な例といえよう．

なお，MH 法では，前述の条件(iv)が成立しない．したがって“署名”をすることはできない．

5. おわりに

以上，暗号系の基本的な概念，DES および公開鍵暗号系の思想と方法について概説した．今後，我が国でも，データベース，データ通信網の発達に伴って，暗号が導入されることは必至であろうと思われるので，我が国でも，この方面の研究を十分進める必要がある．我が国の通信機器業界は DES の導入をほぼ決定したようであるが，DES についてもいろいろと批判があることを十分認識しておく必要がある．公開鍵方式の研究は，残念ながら，それほど行われていないのが現状である．

* w と n は互いに素である．

参考文献

1) National Bureau of Standards: Data Encryption standard, Federal Information Processing Standards Publ. 46 (1977). [Cryptologia, Vol. 1, No. 3, pp. 292-306 (1977) にも掲載されている．]
2) Diffie, W. and Hellman, M.: New Directions in Cryptography, IEEE Trans. on Information Theory, Vol. IT-22, No. 6, pp. 644-654 (1976).
3) Diffie, W. and Hellman, M.: Exhaustive Cryptanalysis of the NBS Data Encryption Standard, Computer, Vol. 10, No. 6, pp. 74-84 (1977).
4) Davies, D. W. and Bell, D. A.: The Protection of Data by Cryptography, NPL Report, COM 98 (1978).
5) Rivest, R. L., Shamir, A. and Adleman, L.: A Method for obtaining Digital Signatures and Public-key Cryptosystems, CACM, Vol. 21, No. 2, pp. 120-126 (1978).
6) Lempel, A.: Cryptology in Transition, Computing Surveys, Vol. 11, No. 4, pp. 285-303 (1979) [西村和夫訳：暗号学の変遷，コンピュータサイエンス，bit 別冊，pp. 109-125 (1980)].
7) Merkel, R. and Hellman, M.: Hiding Information and Receipts in Trapdoor Knapsacks, IEEE Trans. on Information Theory, IT-24 (1978).
8) Simmons, G. J.: Symmetric and Asymmetric Encryption, Computing Surveys, Vol. 11, No. 4, pp. 305-330 (1979) [一松信訳：対称および非対称暗号化，コンピュータサイエンス，bit 別冊，pp. 127-148 (1980)].
9) Popek, G. J. and Kline, C. S.: Encryption and Secure Computer Networks, Computing Surveys, Vol. 11, No. 4, pp. 331-356 (1979) [土居範久訳，暗号化と安全な計算機ネットワーク，コンピュータサイエンス，bit 別冊，pp. 149-173 (1980)].
10) Hellman, M. E.: The Mathematics of Public Key Cryptography, Scientific American, Vol. 241, No. 3, pp. 146-157 (1979) [一松信訳：新しい暗号体系，サイエンス，Vol. 9, No. 10, pp. 100-112 (1979)].

(昭和55年10月6日受付)