36. 公衆暗号系の実現法†

西　村　和　夫††

1. はじめに

暗号とは何かを明確に定義するのはむずかしい．古くは，特定の二者の間で秘密の通信を行うための技術が暗号であった．ただし，秘密通信を行うためには“あぶりだし”なども使用することができるが，この類のものは除く．発信者は**平文** (plaintext) を**暗号化** (encryption) して送り，受信者は受け取った**暗号文** (cryptogram) に**復号** (decryption) の手続きを施して元の平文を得る．途中の伝送路から第三者が暗号文を入手しても，それを**解読** (cryptanalysis) することはできない——というのが理想的な暗号である．

暗号は，国家間の軍事や外交の道具として使われてきたが，一般人にも知的な遊びの対象として広まっている．我が国でもその例として，平安時代から作られている折句がある．しかし，暗号の技術と理論が急速に進歩したのは第二次大戦の前後である．

シャノン (C. E. Shannon) が確立した情報理論[1),2)]により，言語がもつ冗長性などの概念が定量的に扱えるようになった．この理論によって，どんな暗号もその暗号文がある文字数を越えると，使われている鍵を一意に決定できることが判った．この文字数を一義点 (unicity point) という．ただし，無限長の乱数を鍵とする暗号は，この一義点が無限大になり，(当然のことながら) 鍵を一意に決定することができない．

シャノンはまた，第三者による暗号解読が可能であるとした上で，その手間が正当な受信者による復号の手間の何倍かかるかという比が暗号の強度として重要な尺度であることを指摘している．これは後に示す現代の暗号の基礎的な考え方である．

暗号の技術は近年さらに飛躍的に進歩している．これは，公衆データ通信網やデータベースシステム，また国際間為替決済サービスなどの実現に対応して，システムの安全性，データの機密保護，認証の問題が顕著になってきたためである．実際，通信衛星によるデータ通信を含む通信の問題，分散処理とデータベース，プライバシの問題，コンピュータ犯罪など，このところ論議の的になっている問題は，そのほとんどが暗号技術と関わりをもっている．

このような状況を背景として，米国商務省標準局 (NBS) は1973年にコンピュータのデータの暗号化に用いるアルゴリズムを公募した．それに応募したIBMの提案がデータ暗号化規格 **DES** (data encryption Standard) として1977年に発効した[3)]．DESのハードウェアはIBMやモトローラなどで実現され，伝送データの保護をする商用の装置が発売されている．

一方，**Diffie** と **Hellman** は1976年に漸新な暗号系の概念を発表した[4)]．この方式は暗号系を非対称にして暗号化の鍵と復号の鍵を別にし，暗号化の鍵は公開してもよいというものである．この方式は**公開鍵暗号系** (**public-key cryptosystem**) と名付けられ，認証（発信者の捺印）もできることから注目を集めている．

したがって，暗号は単に秘密通信をするためだけの技術ではなく，認証や個人の照合，さらにシステムの安全性に関する技術へと変わってきている．

本稿では，まず暗号が直接果たす機能について述べ，次いでDESや公開鍵暗号系の仕組と運用のしかたについて簡単に説明する．それらの詳細は各参考文

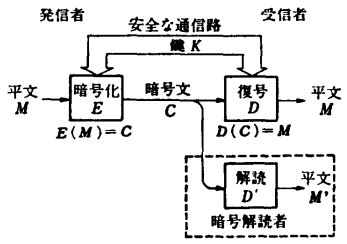


図-1　一般的な暗号系の概念

† Some Methods for Public Cryptosystem by Kazuo NISHIMURA (Department of Mathematical, Science Faculty of Science and Technology, Keio University).

†† 慶応義塾大学理工学部数理科学科

献に記載されており，本誌でも紹介されている[5),6)].

2. 暗号系の機能

2.1 秘密通信

暗号はもともと秘密の通信をするための手段であった．発信者は平文（普通の文章）の通信文 M を暗号化の関数 E で暗号文 C に変換して送り，受信者は復号の関数 D で元の平文に戻す．つまり，

発信者：$E(M)=C$

受信者：$D(C)=M$

である（**図-1**）．なお，通常は便宜のために暗号化と復号の関数に**鍵** K をパラメタとして用い，それぞれ E_K, D_k として使用する．

ここで通信の秘密には3つのレベルがある．(1)通信の内容の秘匿，(2)通信の方式の秘匿，(3)通信の存在自体の秘匿である．たとえば，鍵を使ったある方式の暗号で通信するとき，鍵を秘密にすれば(1)が，その方式を秘密にすれば(2)が，暗号文を秘密インクで書けば(3)が実現できる．しかし，近代的な考え方では，(2)や(3)は期待できないものとしている．傍受している第三者は暗号文をすべて入手することができ，暗号の方式も知っているものとするのである．

(1)の通信の内容を秘匿することだけが目的ならば，(復号の関数 D は秘密にしておく必要があるが) 暗号化の関数 E は必ずしも秘密にしておく必要はない．この考え方は Diffie と Hellman によって導入された[4)]．

2.2 照合

銀行の現金自動支払機や，機密を要する部屋の入室管理，そしてコンピュータの利用資格審査などでは，個人が正当な資格をもつ者かどうかを判定しなければならない．このときの一手法として，パスワードによる**照合**がある[7)]．利用者は自分の識別名 (ID) とパスワード (P) を照合システムに入力する．システムは登録してある ID と P の表を引いて，入力したものと照合する．表を引く代わりにパスワードを磁気カードから読み取ることもある．

このとき，表にパスワードがそのまま保存してあると危険である．主記憶装置や磁気テープ上のパスワード・ファイルを物理的に読み出すことは容易だからである．そこで，パスワードをそのまま保存せずに，複雑な変換を施したものを保存しておく方法が考案されている．つまり，パスワード P を

$C=E(P)$

と暗号化した暗語 C を保存しておくのである．照合するときも P を E で変換してから行う．

このとき関数 E は，その詳細を知っても逆変換を陽に構成することができないものであれば都合がよい．たとえば，大きな整数を法とする剰余環上で整数 P を3乗するだけでも，それから元の値に戻すのは大変である[6)]．このような関数を一方通行関数 (one-way function) とよぶ．

UNIX*では，変換 E として DES を変形したものを使用している．利用者は誰でも E の仕組（プログラム）と暗号化されたパスワードファイルを見ることができるが，それから元のパスワードを知ることはできない．

2.3 認証

商取引においては，通信の内容を秘匿するよりも通信文の発信者を保証するほうが大事なことが多い．これを**認証** (authentication) という．普通は認証を捺印や署名で行っているが，これではとても安全とはいえない．認証には2つの役割がある．(1)受信者は発信者を確認することができ，(2)発信者は通信の事実を否定できない（受信者の擁護）．認証は軍事や外交においても重要であり，敵の偽造した情報による攪乱を防ぐことができる．

復号の関数 D が，これから暗号化の関数 E を構成することができないという一方通行関数の性格をもっているものなら，暗号化の関数 E を（受信者に対してさえも）秘密にすることにより，認証を行うことができる．認証文 $C=E(M)$ を作ることができるのは，E を知っている発信者だけだからである．ただし(2)の役割を実現するためには，発信者が E を盗まれたことにして事後に発信の否定をすることができないような工夫が必要である．

3. DES

3.1 DES の仕組

DES は古来からある転置と換字を巧妙に組み合わせた暗号である．その仕組の概要を **図-2** に示す．その詳細な記述と解説は文献3), 10) などにある．DES は56ビットの KEY を用いて64ビットのデータ（ブロックという）をビット単位に処理する暗号である．

DES による暗号化は本質的に

$$\begin{cases} L_i=R_{i-1} \\ R_i=L_{i-1}\oplus f(R_{i-1},, K_i) \end{cases} \quad (i=1,2,\cdots,16)$$

---

* UNIX はベル研究所の登録商標です．

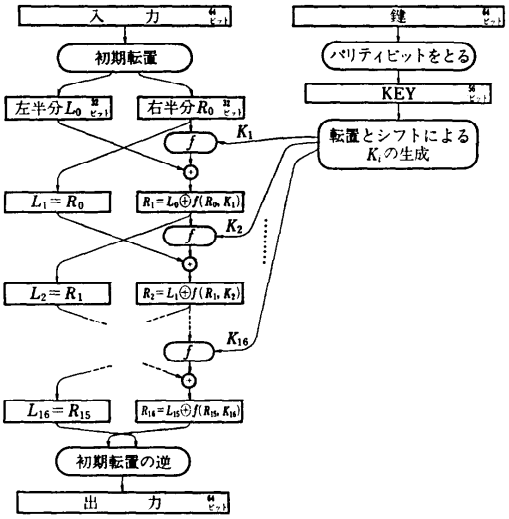


図-2 DES の仕組の概要

を16回繰り返すだけのものである．K_i の生成と f は複雑であり，特に f の計算の途中には6ビットのデータを4ビットに縮小する換字の表を引く部分があって，逆向きの解説を極めて困難にしている．なぜなら，4ビットのデータからその元の6ビットを推定しようとしても，4つの候補があって一意に定まらず，しかもこれが何回も起こるからである．

鍵を知っている受信者が暗号文を復号するときには

$$\begin{cases} R_{i-1}=L_i \\ L_{i-1}=R_i \oplus f(L_i, K_i) \end{cases} \quad (i=16, 15, \cdots, 1)$$

と逆順に求めていけばよい．このとき f や K_i は暗号化のときと同じものを使えばよいことに注意する．暗号化と復号で異なるのは K_i を逆順に用いることだけであり，f の逆関数は全く必要がない．つまり，f は K_i をパラメタとする疑似乱数を生成するための一方通行関数として働いている．64ビットのデータを暗号化するときには，この疑似乱数を加える（排他的論理和または論理差をとる）ことしかしていない．データを半分の 32 ビットずつに分けて片方は次のステップにそのまま渡すのは，復号を容易にし，暗号化と復号を同一の手続きで行えるようにするためである．

DES は考え方によっては，64ビットの入力データから 64 ビットの出力を得るコード表とみなすことができる．表の要素は 2^{64} 個あることになる．ただし，この表は 64 ビットの鍵をパラメタにしていて，鍵の1ビットが変化するとき，表の配列が大きく変わる．DES が取り得る表の種類は $2^{64}!$ ではなく，2^{56} 通りである．

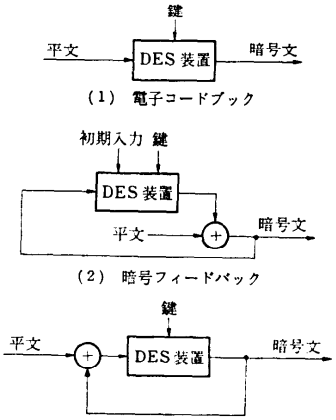


図-3 DES の利用形態

3.2 DES の運用

DES を利用する形態として，次の3通りが考えられている[3]．

(1) 電子コードブック
(2) 暗号フィードバック
(3) ブロック連鎖

これらを図示すると図-3のようになる．

DES への直接入力は64ビットつまり8バイトであるが，これをすぐに8文字の英字データに割り当てて使用するのは若干危険である．英文は3.2ビット／字程度の冗長度をもっているので，DES の鍵の一義点は (56/3.2 の) 17.5 字にしかならない[8]．つまり，2ブロックのデータによって鍵が一意に定まるのである．ただし，一意になるからといって，それがすぐに求まる訳ではない．2ブロックの平文と暗号文の組があれば，2^{56} 個の鍵の全数検査などをして鍵を決定することができるという意味である．いずれにせよ，平文のデータはハフマン・コードを利用するなどして，圧縮して冗長度を小さくしておくことが望ましい．

暗号フィードバックやブロック連鎖においては，初期入力や平文の先頭部分に乱数を入れ，これを暗号化したものと次の平文との論理差をとっている．これによって，通信の先頭部分のきまり文句を平文とみなした解読（選んだ平文による攻撃）に対して強くなっている．平文のあるブロックの影響は次のブロックにしか及ばないので，転送中に誤りがあっても2つのブロックが失われるだけで済む．逆にいえば，通信文の途中の2ブロックによる平文を推定した解読に対して

はさほど強くない．運用するときは，(DES を含む) 他の暗号と組み合わせて2重・3重の暗号化をしたほうがより安全である．

DES のような，暗号化 E と復号 D に同じ鍵を用いる暗号は，送受信者間で共通の鍵を設定するための通信路を確保するのにコストがかかる．また多数の相手と通信するときに，それぞれ異なる鍵を用いると，その鍵の管理にコストがかかる．

DES をハードウェア化したチップは既に市販されており，それを使った通信装置も実用になっている．

4. 公開鍵暗号系

公開鍵暗号系の概念は1976年に Diffie と Hellman によって提唱された[4]．これは暗号学に大きな変化をもたらし，これまで用いられてきた (DES のような) 送受信者で同一の鍵を使用するものは"慣用の暗号系"とよばれるようになった．

公開鍵暗号系は，暗号化の関数 E を一方通行関数にして，E から復号の関数 D を知ることができないようにするものである．したがって，暗号化の関数 E は公開することさえできる．そうすれば，一人の受信者に対して多くの発信者から同一の E を用いた暗号文を送ることができる．

ところで，受信者だけは復号の関数 D を知っていなければならない．したがって，E は完全な一方通行関数ではなく，何らかの種を知っていれば D を構成することができる落し戸一方通行関数 (trapdoor one-way function) である必要がある．たとえば，受信者がこの種を作って E と D を作成し，E を発信者に (公のもとで) 送ることにすれば，この系を実現することができる．しかし，各受信者ごとに全く異なる E と D を作るのは，送受信者共に負荷がかかる．実際には鍵 e と d をパラメタとする関数 E_e と D_d を決めておき，暗号化の鍵 e は公開するようにする方法が提案されている．

秘密の関数 D と暗号化の関数 E とは

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

となる関係をもつ．もしこれらを逆に組み合わせても

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

となるものなら，認証に使うこともできる．認証付きの通信文を送りたい発信者は，平文 M を $D(M)=S$ として送信し，受信者はこれを $E(S)=M$ と復元する．この受け取った認証文 S を作成することができるのは，秘密の関数 D を知っている発信者だけである．

公開鍵暗号系では，認証付きの秘密通信を行うこともできる．A氏とB氏が，それぞれ暗号化と復号の関数の組 (E, D) と $(\mathcal{E}, \mathcal{D})$ を用意しており，互いに E と $\mathcal{E}$ を相手に知らせてあるとする．もし A が B に認証付きの秘密通信をしたいのなら，A は $\mathcal{E}(D(M))=C$ を作って B に送る．B はこれを $E(\mathcal{D}(C))=M$ として元の文書をとり出すことができる．

多数の人が鍵をパラメタとした共通の関数を使って通信するときにも，各自が秘密にしなければならないのは自分用の復号の鍵だけである．したがって鍵の保存は容易である．しかし，公開されている暗号化の鍵が確かに (いま通信を送りたい当の) 相手のものであることを保証するのは意外にむずかしい．公開鍵暗号系でも，鍵の管理の問題は最後までつきまとうであろう．鍵の配布や更新，そして認証を証明するためのプロトコルがいろいろ考えられている[6),7)]．

4.1 RSA 法

公開鍵暗号系を実現するための方法は多数あるが，最初に提案されたのは Rivest, Shamir, Adleman らが1977年に提案した **RSA 法**である[11)]．方式の概要は各所に掲載してある[5),6),11)]ので，ここでは例を用いた図を用いて説明する (**図-4**)．

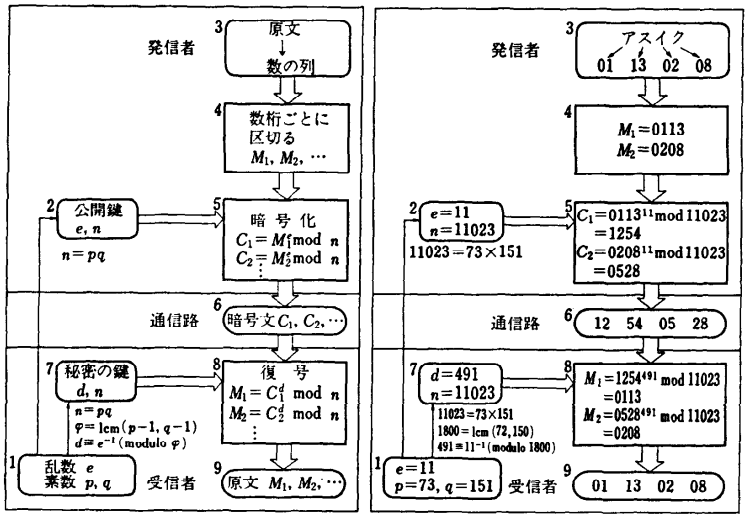
図中の φ は，もともと n のオイラー関数値 $(p-1)(q-1)$ であったが，ここでは $(p-1)$ と $(q-1)$ の最小公倍数にしてある．最小公倍数のほうが積よりも小さいので，復号におけるべき乗の手間を少なくすることができる．

RSA 法は暗号化も復号も，剰余環の上でべき乗をするものであり，これが落し戸一方通行関数になっている．落し戸の種は n が (大きな) 素数 p, q の積になっていることであり，この2数を知らない解読者が公開鍵 e と n から秘密の鍵 d を求めるためには n を因数分解しなければならない．今のところこれには $\exp((\ln n \cdot \ln\ln n)^{1/2})$ 程度の計算量を必要とし[12)]，n が200桁の整数であれば，1演算を $1\,\mu s$ で行ったとしても 10^9 年くらいかかる．これに対し，暗号化や復号には $1\,ms$ しかかからない．

4.2 MH 法

Merkle と Hellman は1978年にナップサック問題を応用した方法を発表した[13)]．これは **MH 法**，ナップサック法などとよばれている．

ナップサック問題とは，n 個の正数 $a_1, a_2, \cdots, a_n$ のうちのいくつかの和が与えられたとき，使われた a_i を求める問題である．これは NP (非決定性多項式時



(a) 方式の概要 (b) 数値例

図-4 RSA 法

間) 完全な問題であり，今のところ n 個の組合せの全数検査法などの非能率的な解法以外は知られていない．MH 法では整数 a_i に $a_1+a_2+\cdots+a_{i-1}<a_i$ という制約をつけ，高々 n 回の減算で解が得られるように仕組んでおく．そして，大きな素数 m を法とする剰余環のうえで a_i を e 倍して $b_i=ea_i \bmod m$ としてから公開する．見かけ上は b_i に上記の不等式関係は現れていない．m と e が落し戸の種であり，a_i と $d \equiv e^{-1} (\mathrm{modulo}\ m)$ が秘密の鍵である．発信者が暗号文を作るときは，平文を2進数列に直してから n ビットごとに区切り，その中のビットが1に対応している番号の b_i を加えて和を作ればよい．受信者は和を法 m のもとで d 倍してから a_i を大きい順に引いていく．引けたときビットを1にしていけば，元の2進数に復号することができる．

MH 法には，鍵の数が多く，認証ができないという欠点がある．また落し戸を仕組んでいるために NP 完全問題ではないのではないかと疑われており，解読の方法も研究されている．これに対し，a_i の上位と下位に乱数を付け加える (Graham-Shamir の方法) などの対策も講じられている．

また，公開鍵暗号系を実現するためには，RSA 法や MH 法のほかにも多数の方法が考えられている．

4.3 公開鍵配布系

公開鍵配布系 (public key distribution system) は，Diffie と Hellman が公開鍵暗号系の概念と同時に考え出したものである[4]．これは DES などの慣用の暗号系を運用する際に，送受信者間で共通の鍵を設定するためのものであり，秘密の通信を行うものではない．

彼らの具体案は，やはり剰余環上でのべき乗を利用したものである．素数の法 n と整数 m が定めてあれば，A氏とB氏は次のようにして共通の鍵 K を決定することができる．まず，AとBはそれぞれ秘密の整数 X と Y を決め，それぞれが $\alpha=m^X \bmod n$ と $\beta=m^Y \bmod n$ を計算して相手に (公開して) 渡す．Aは受け取った β を X 乗し，Bは α を Y 乗して，共通の鍵 $K \equiv \beta^X \equiv \alpha^Y \equiv m^{XY}$ (modulo n) を得ることができる．

5. おわりに

DES と公開鍵暗号の登場により，暗号は大きく変わってきている．ディジタル通信で認証ができるようになれば，公文書などもディジタル化することができるようになり，そのメリットは測り知れない．DES は今のところ良い暗号であるが，計算機技術の進歩によって近い将来にその使命を終える日が来るであろう．公開鍵暗号系には，公開鍵の正当性の証明やその配布の方法，認証の証明の方法，安全性の証明など問題は多いが徐々に解決されているので，実用になる日も遠くないであろう．データ通信網の発達により，暗号はもはや一部の人間が隠しもっているものではなく，一般に広く使用されるものになってきている．

参 考 文 献

1) Shannon, C. E.: The Mathematical Theory of Communication, Bell System Technical Journal (1948).
2) Shannon, C. E.: Communication Theory of Secure Systems, Bell System Technical Journal, Vol. 28, pp. 656-715 (1949).
3) National Bureau of Standards: Data Encryption Standard, Federal Infomation Processing Standards Publ., 46 (1977).
4) Diffie, W. and Hellman, M. E.: New Directions in Cryptography, IEEE Trans. Inform. Theory, Vol. IT-22, No. 6, pp. 644-654 (1976).
5) 土居範久, 廣瀬 健, 西村恕彦: 公衆暗号系, 情報処理, 22巻, 1号, pp. 38-46 (1981).
6) 土居範久, 廣瀬 健, 一松 信, 西村和夫: 公衆暗号系の実現可能性と問題点, 情報処理, 22巻, 1号, pp. 47-54 (1981).
7) 小山謙二: 認証とディジタル署名, 情報処理, 24巻 (1983) [掲載予定].
8) Denning, D. E.: Cryptography and Data Security, Addison-Wesley (1982).
9) Knuth, D. E.: The Art of Computer Programming, Vol. 2, 2nd ed., Addison-Wesley pp. 386-389 (1981).
10) 土居範久: 米国のデータ暗号化規格 DES, bit, Vol. 13, No. 2, pp. 102-113 (1981).
11) Rivest, R., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, CACM, Vol. 21, No. 2, pp. 120-126 (1978). [初版は MIT/LCS/TM-82, MIT (1977)].
12) Dixon, J. D.: Asymptotically Fast Factorization of Integers, Math. Comp., Vol. 36, No. 153, pp. 255-260 (1981).
13) Merkle, R. and Hellman, M. E.: Hiding Information and Receipts in Trapdoor Knapsacks, IEEE Trans. Inform. Theory, Vol. IT-24, pp. 525-530 (1978).

(昭和58年2月16日受付)