暗　号

（DES 暗号・RSA 暗号・楕円曲線暗号）

025210　中野孝雄　　025215　村田隆一　　025216　左　瑞麟
指導教官　助教授　片岸　一起　　講師　ミャオ　イン

０　はじめに

インターネットを使用して、通信を行う場合、その情報は通信路の途中で、常に盗聴される可能性がある。特に、通信路に、元のままのデータ（平文:Plain Text）を流して、これを第三者に盗聴された場合、意味を判読されて悪用されることが考えられる。盗聴されても意味が判読できないように、情報の発信者が元のデータを暗号化して、通信路に流して、受信者が復号化して、元のデータに戻すのが、暗号化原理の基本である。暗号化は、暗号鍵と呼ばれる送信者固有のデータと送信データとの間で演算を行うことで行われる。復号化は、この逆に、復号鍵と送信データとの間で演算を行う過程である。

本研究では、秘密鍵暗号と公開鍵暗号の考え方について概観し、特にＤＥＳ暗号とＲＡＳ暗号、楕円曲線暗号についてだれにでもわかるように説明することを主眼としている。

１　暗号の歴史

(1)　スキュタレー暗号

現在わかっている最も古い暗号は、古代ギリシャでスパルタの将軍達が使っていたスキュタレー暗号といわれている。この暗号は、まず同じ太さの棒を２本用意し、通信を送る者と受ける者がそれぞれ１本ずつ持つ。通信を送る者は、この棒に細長い紙を巻き付け、これに通信文を棒の長さ方向に書き込む。紙を巻き取ると意味のわからない文章になる。そしてこの紙を離れた場所にいる通信の受け取り手に届ける。途中で敵に奪取されても、棒がなければ通信内容は判読することはできない。受け取った味方は、書いたときに使った棒と同じ太さの棒に紙を巻き付け、棒の長さ方向に読めば、通信文がわかるという仕組みである。

(2)　シーザー暗号

現在まで影響を残している最も古い暗号がシーザー暗号である。これは、その名前が示す通り、古代ローマのジュリアス・シーザーが自分の軍に送る命令を秘密にするために使った暗号である。シーザー暗号は、通信文の文字をアルファベット順に何文字かずらせた文字に変換していき暗号文にする。

(3)　その他の暗号

単文字換字暗号：どの文字をどの文字に変換するかといった表を作っておいて、その表に従って通信文の文字を変換する方法。受けては換字表に従って元の通信文に戻す。また、単文字換字暗号のバリエーションとして、座標換字表を使う方法がある。縦方向、横方向の座標と文字を対応させた表を用いて、元の文章を座標で表した文字の列に変換したものを暗号文とする。

転置式暗号と挿入式暗号：元の文の構成要素の順序を変えて暗号文とするものが、転置式暗号である。例えば、文を逆向きの文字の並びにしたものを暗号文としたり、何行かにわたり横書きにした文を縦の列ごとに並べ替えたものを暗号文とする。一方、挿入式暗号が元の文の構成要素の間に余分な

文字や語を挿入したものを暗号文とするもの。

(4)　アルゴリズムと鍵

暗号化とは「秘密通信のため当事者間のみが了解するルールに従って通信文を第三者に理解できない情報に変換すること」である。この変換のための“当事者間のみが了解するルール”には、「変換の手法（アルゴリズム（計算の手順））」とそのための「鍵」という 2 つの要素が含まれている。例えば、シーザー暗号では、「文字をアルファベット順に何文字かずらす操作」がアルゴリズムで、「前から後ろにずらす文字数」が鍵ということになる。

(5)　多表式暗号

単文字換字暗号は、平文の文字と暗号文の文字が対応しており、平文の文字の出現頻度がそのまま暗号文に反映される。そのため、文字の出現頻度を手がかりに読解されてしまう。そこで、近代以降、単文字換字暗号を基本にして、変換を複雑にした暗号が様々に考え出された。こうした暗号は、一般的に多表式暗号と呼ばれ、現在まで暗号の主流となってきた。20 世紀以降に使われた暗号の大半は多表式暗号に含まれるものである。

(6)　暗号機

19 世紀終盤から 20 世紀になると暗号文を簡単に、もしくは自動的に作成する暗号機が作られるようになったが、こうした暗号機は基本的には多表式暗号の原理に基づいていた。やがて電動式の暗号機が作られるようなり、平文をタイプ入力するだけで、自動的に暗号文が出力、印刷される装置であった。こうした暗号機の開発とともに数学的基礎理論に基づく暗号技術が確立されていった。

暗号機及び暗号技術は第一次世界大戦、第二次世界大戦を背景に軍事目的で多くのものが開発製造された。こうした暗号機の中で最も有名なものがエニグマ暗号機と呼ばれる装置である。エニグマ暗号機は第二次世界大戦前にドイツの会社で製造され、第二次世界大戦中にドイツ軍がそれを改良して軍事用に使った暗号機である。

(7)　コンピュータの暗号

インターネット通信で使用する暗号とは、コンピュータで処理する暗号で、コンピュータで処理する暗号は、シーザー暗号のように単純ではなく、数学的な原理を用いて非常に複雑な処理で暗号化、復号化を行う。アルゴリズムや鍵も単純なものではない。

コンピュータの世界では、データは「ビット（bit：binary　digit）」の並びで表す。ビットとは、コンピュータで扱うデータの最小単位で、１つのビットは「０」または「１」である。1 つのビットでは０と１の２種類のデータしか表現できないが、ビットの数を増やしていけば、より多くのデータを表現することができる。コンピュータの暗号では、鍵はこのような特定のビット数のデータで表されるデータである。一般的には、５６ビットや６４ビット、８０ビット、１２８ビット、２５６ビットなどの大きさの数値データを鍵として使用する。

コンピュータでの暗号は、暗号プログラムとして実現される。暗号のプログラムにはアルゴリズムが組み込まれ、鍵を生成する機能、すなわち数値データを作り出す機能が備わっている。暗号化のプログラムは、暗号鍵にあたる数値データをパラメータ（媒介用の値）にして、元のデータを全く違う状態にし変形をさせる。逆に復号化のプログラムは、同じ数値データを復号鍵にして元の状態に戻す。暗号文は鍵にあたる数値データを取得できれば復号化でき、暗号文を正規の手段で復号化せずに平文に戻すことを読解という。読解されにくい暗号を「強い暗号」という

一般的に暗号の強度は鍵の長さのビット数で表す。ビット数が大きいほど鍵を見つけ出しにくい。例えば、２ビットだと４通りの組み合わせしかないので、多くても 4 回試せば鍵を見つけることができる。しかし、４０ビットになると１兆９９５億１１６２万７７７６通りの組み合わせが可能となり、簡単に試せる数字ではなくなる。

２　秘密鍵暗号と公開鍵暗号

(1)　秘密鍵暗号方式（共通鍵暗号方式）

暗号化した情報のやり取りを可能にするためには、送り手、受け手が変換ルール、すなわち鍵とアルゴリズムを共有しなければならない。そのうえ、暗号の安全を確保するためには、通信の当事者以外の者から、鍵とアルゴリズムを共有しかつ秘匿する必要がある。このような仕組みの暗号方式が秘密鍵(共通鍵)暗号方式である。

秘密鍵暗号方式は、秘密情報の送り手、受け手がともに複号化にも使用する同一の鍵を所有するため共通鍵暗号方式とも呼ばれている。

秘密鍵暗号方式では、鍵とアルゴリズムを秘密通信の当事者間で共有し、それ以外には秘密にしておく必要がある。しかし、現在ではアルゴリズムは万人に公開し、誰でもその内容を知ることができるようにした上で、鍵だけを通信の当事者間だけで秘密にしておくという仕組みが一般的になっている。この方式では、アルゴリズムが知られていても鍵さえわからなければ暗号の読解は非常に難しい。

秘密鍵暗号方式で最も問題になるのは、鍵の管理や配布である。秘密鍵は、情報の送信者、受信者の両方が同一のものを所有しなければならず、第三者には秘密にしておかなければならない。そのため一組の送信者／受信者ごとに一つの共通鍵を持つことになる。よって相手が増えれば増えただけの鍵を持つということが必要になり、管理が大変になってくる。

秘密鍵暗号方式の代表的なものにＤＥＳ暗号、Triple ＤＥＳ暗号化方式等がある。

(2)　公開鍵暗号方式

公開鍵暗号では、平文を暗号化するための鍵(公開鍵)と、暗号化されたデータを平文に復号化するための鍵(秘密鍵)という、二つの異なった鍵のペアを作る。公開鍵は、あらかじめ電文の送信者にネットワークを通して送っておく。送信者は、その公開鍵で暗号化したデータをネットワークを通じて送信する。データを受信した者は、秘密鍵で復号化する。公開鍵と暗号鍵の間には、密接な関係があるにも関わらず、公開鍵から暗号鍵を推測することを非常に困難となるような仕掛けを施している。

公開鍵暗号化方式の代表的な規格として、ＲＳＡ暗号、楕円曲線暗号がある。

３　ＤＥＳ暗号

DES 暗号の基礎

DES 暗号では、平文を暗号化する際に、平文のアルファベットの８文字を１ブロックとして一括して処理をする。すなわち、DES 暗号は８文字＝64 ビットを一単位として扱うブロック暗号である。64 ビットごとに区切られた平文は、16 段の転置や関数表による換字処理を受ける。

DES 暗号は共通鍵暗号なので、暗号化にも、復号化にも同じ鍵を使用する。鍵尾が長さは 64 ビットであるが、うち８ビットは図１に示すように奇数パリティといわれる誤り検出用のビットであるので、実質 56 ビットが鍵の役割をする。この鍵は、半分の長さの 28 ビットずつの２つの鍵にわけられたのち、それぞれのビットの順番をシフトしたり、再び一つに合成したりする変形を受けた後、暗号化のためのデジタル演算処理に用いられる。

ここでいうデジタル演算のしかたは、１＋１＝０で桁上げなしという、Exclusive OR の論理で計算を行う。この演算はデジタル信号処理ではたびたび用いられる、０か１が並んだ各桁が、桁上げや借りもなくそれぞれ独立していて、偶数（０）か、奇数（１）であるかだけを意識した計算方法である。演算は主として平文と鍵の間で行われる。

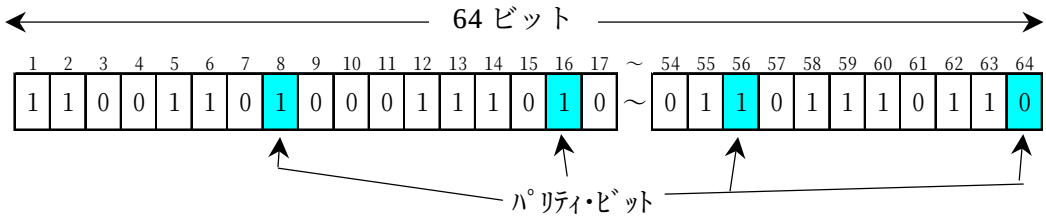

図１：DES 暗号の鍵の構成

初期転置 IP（Initial Permutation）（入力された平文の文字コードをビット単位で並び替える）

DES 暗号の初期転置では文字コードで構成された平文の各ビットをバラバラに分解し、ビット単位の配置を行う。この転置のルールは図２に示すように、転置出力の片方のL_0の最初の８ビットは、文字コード化された平文から 58,50,42,34,26,18,10,2 の偶数番目のビットを拾いあげて出力する。以下、９～16 ビット、17～24 ビット‥‥についても同様に規則表に従って出力を編成し、これを 64 ビットになるまで続ける。

初期転置の終わった、平文データは２つの 32 ビットのブロックに分け、その１つはL_0、もう一つは奇数ビットを集めたR_0として、これ以降、最後に再合成するまでは、別々に処理をすることになる。

IP								
初期転置出力	文字コード化された平文入力ﾋﾞｯﾄ							
1-8	58	50	42	34	26	18	10	2
9-16	60	52	44	36	28	20	12	4
17-24	62	54	46	38	30	22	14	6
25-32	64	56	48	40	32	24	16	8
33-40	57	49	41	33	25	17	9	1
41-48	59	51	43	35	27	19	11	3
49-56	61	53	45	37	29	21	13	5
57-64	63	55	47	39	31	23	15	7

L_0

R_0

図２：初期転置の規則表

暗号化鍵も二つのブロックに分ける

初期転置(IP)した出力は二つに分けたが、同様に鍵も二つに分ける。図３はもともと 64 ビット（正味 56 ビット）の鍵を、二つのブロックに振り分けるための選択転置表（PC-1）と呼ばれるテーブルである。このそれぞれの鍵の長さは 28 ビットで構成され、図４に示すように、鍵半分の C(0)の最初の７ビットは、64 ビット長さの鍵の 57,49,41,33,25,17,9 番目のビットを集めて作成する。８ビット目以降も同様に続け、28 ビットになるまで繰り返す。

この処理は、DES 暗号では鍵についてもビット単位の転置が行われることを意味しており、二分割の処理と同時に実行される。また、この過程で、64 ビットのうちのパリティ・ビットである 8,16,24,･･･番目にあるビットは取り除かれる。

もう半分の鍵 D(0)も同様な処理で作る。このようにして作成した、C(0), D(0)の二つの鍵は、16 個のサブキーK(i)をつくるもとになる。サブキーとは、二つに分けられた平文のブロックごとに、16 段にわたって繰り返される演算に用いる、各段用に多少変形された鍵を意味している。

	鍵出力	暗号鍵						
C(0)	1-7	57	49	41	33	25	17	9
	8-14	1	58	50	42	34	26	18
	15-21	10	2	59	51	43	35	27
	22-28	19	11	3	60	52	44	36
D(0)	1-7	63	55	47	39	31	23	15
	8-14	7	62	54	46	38	30	22
	15-21	14	6	61	53	45	37	29
	22-28	21	13	5	28	20	12	4

図３：56ビットの鍵から 2 つの 28ビットの鍵をつくる選択転置表

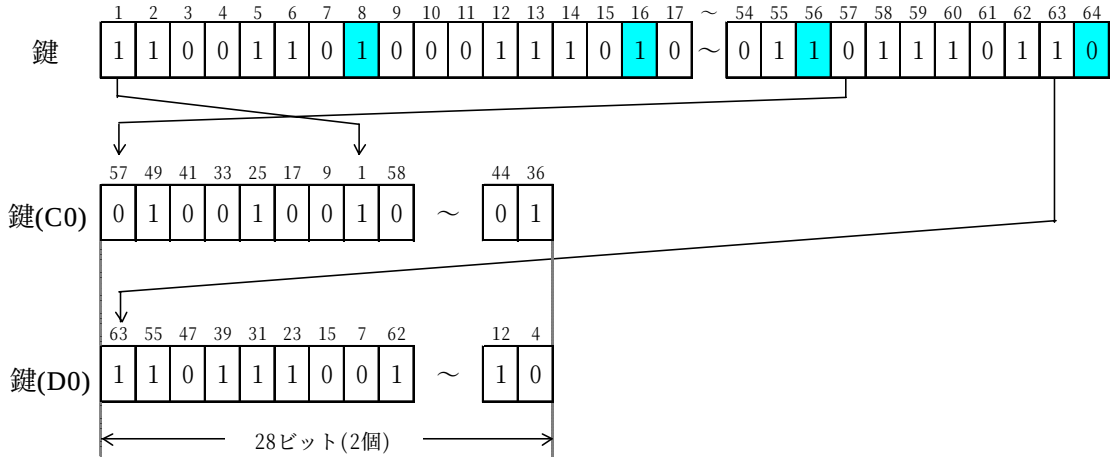

図４：64ビットの DES 暗号鍵から 2 つの 28ビット鍵をつくる

サブキーをつくる

キー・スケジュールといわれる、サブキーをつくる手順を解説する。図５の最上段には、二分割された鍵 C(0)と D(0)が記されている。初段の演算に用いるサブキーは、これらを１ビットだけ左方向にシフトして C(1)と D(1)とする。このシフトする量は、各段で異なるが C ブロックと D ブロックでは共通である（図６参照)。各段の左シフト量は１ビットまたは、２ビットであり、１６段までの間には鍵の長さと同じ 28 ビットがシフトされ、C(16)、D(16)は一巡して最初の C(0)、D(0)と等しくなる。

次の鍵処理の過程では、いままで C、D ブロック独立に左シフトしてきた、二分割された鍵は再び一つに合成される。この際、合成された鍵は 28 ビット×２=56 ビットの長さであるが、このうちの８つを間引いて 48 ビットにする。この選択される 48 ビットは、C(i)と D(i)を連結したのち各ビットに新しく順番をつけ直した上で、図７に示す選択転置表（PC-2）に従って図８のように定められる。削除されるビットは 9,18,27,36,45,54 のビットになる。この選択転置（PC-2）により、選択された 48 ビットの鍵はサブキーK(i)として、以後 16 段繰り返される暗号処理の演算に使用される。以上の鍵作成過程のフローを図９に示す。

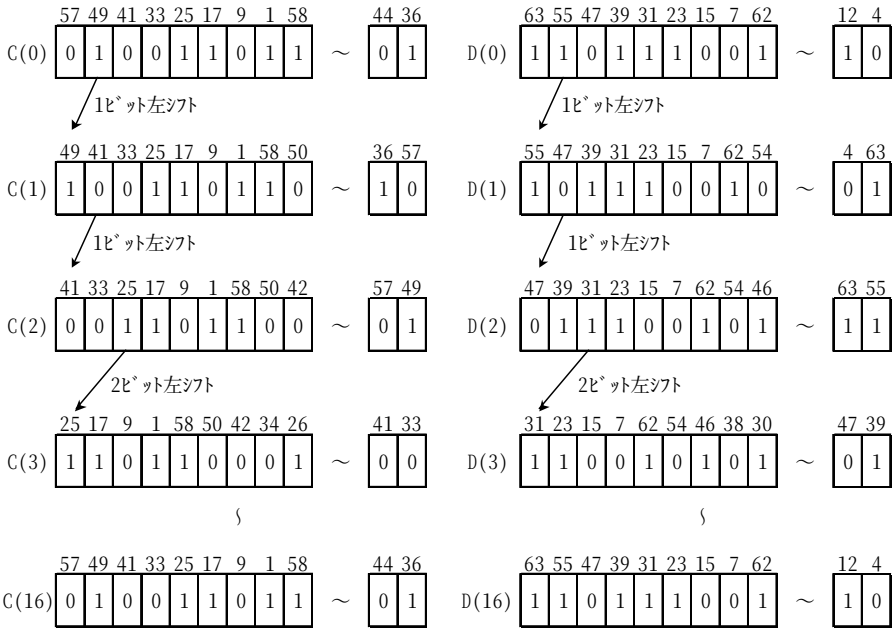

図５：半分の鍵 C(i)、D(i)の生成

段数　i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
シフト数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

図６：左シフトのテーブル

K(i)出力ﾋﾞｯﾄ	各段のC(ｉ),D(ｉ)入力ﾋﾞｯﾄ					
1-6	14	17	11	24	1	5
7-12	3	28	15	6	21	10
13-18	23	19	12	4	26	8
19-24	16	7	27	20	13	2
25-30	41	52	31	37	47	55
31-36	30	40	51	45	33	48
37-42	44	49	39	56	34	53
43-48	46	42	50	36	29	32

図７：サブキーK(i)の合成に用いる選択転置表（PC-2）

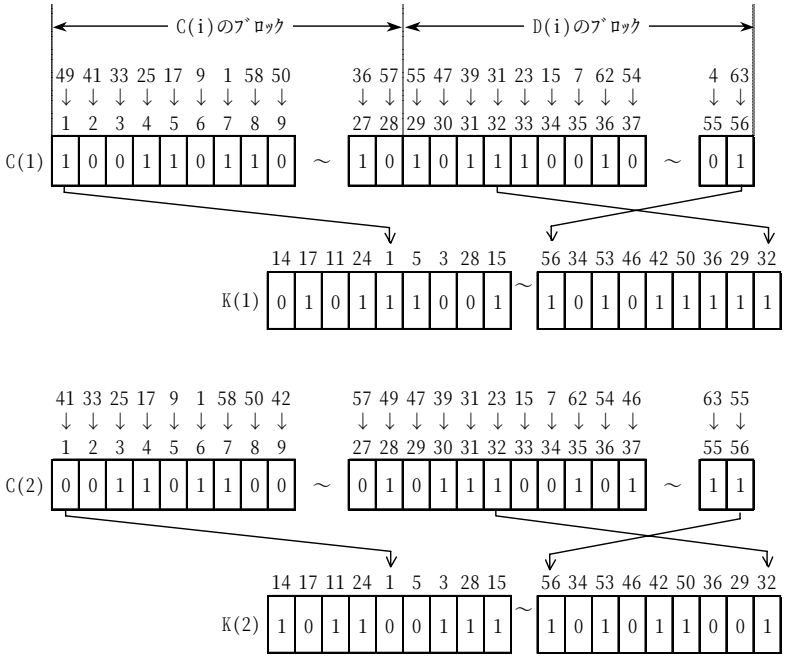

図８：C(i)，D(i)を合成してｻﾌﾞｷｰK(i)を作成

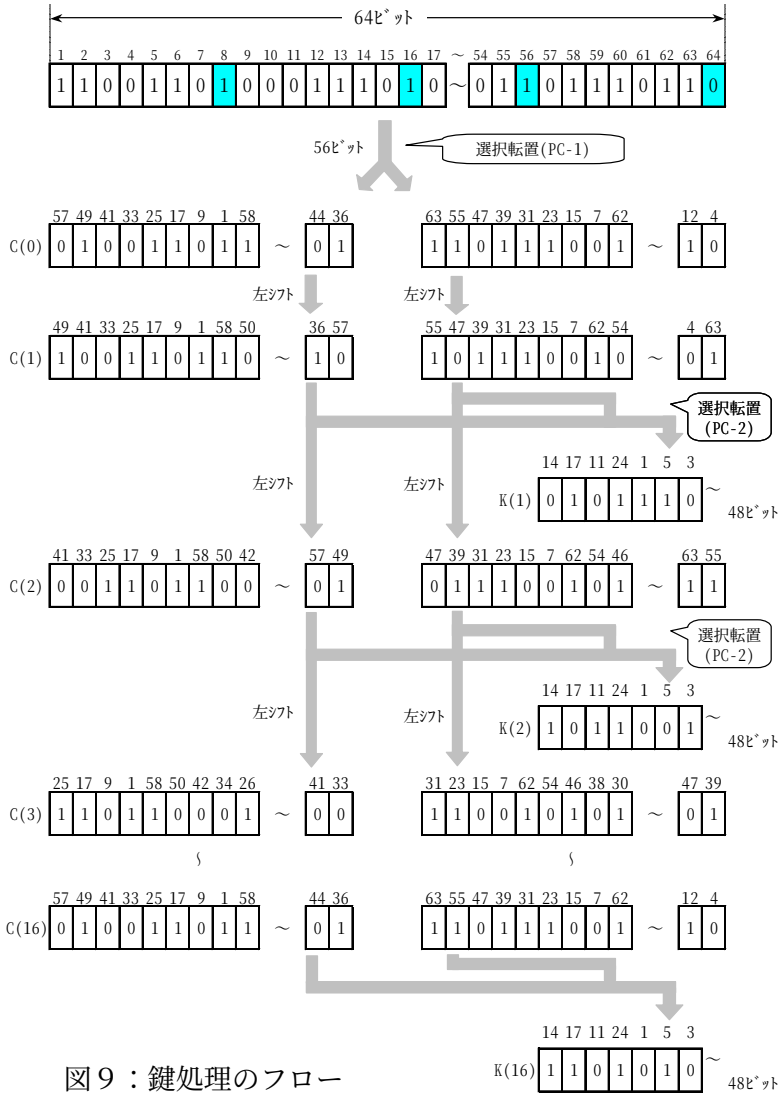

図９：鍵処理のフロー

関数の手はじめ・・・拡大処理

一つの平文ブロック 64 ビットを二分して各 32 ビットずつのＬ、Ｒの２つに分ける（初期転置：ＩＰ）ところまでは、前に説明した。次に暗号処理のうちで DES 暗号の強さを決定するといわれる関数処理と名付けられたプロセスの説明をする。この関数処理はＲ側ブロック（32 ビット）とサブキー（48 ビット）の間で行われる。

まず、32 ビットのＲブロックを 48 ビットに拡大する。拡大の方法は、図 10 の拡大転置表（Ｅ）により、一部のビットを２回使用することで行う。例えば、図 11 に示されるように、Ｒブロックのビット３は拡大Ｒブロックの４番目のビットとして１回のみしか使われないが、ビット５は６番目と８番目に２度用いられている。

このようにして 48 ビットに拡大されたＲブロックの平文系のデータ E{R(i)}は、次の処理で同じヒット数である、次段のサブキーK(i+1)と加算される。たとえば R(0)が拡大された E{R(0)}の場合は、K(1)と加えられる。Ｌブロックの 32 ビットに関しては、この拡大転置を含む関数処理を行わないのが DES 暗号のアルゴリズムである。

出力ﾋﾞｯﾄ	Eﾋﾞｯﾄ選択表					
1-6	32	1	2	3	4	5
7-12	4	5	6	7	8	9
13-18	8	9	10	11	12	13
19-24	12	13	14	15	16	17
25-30	16	17	18	19	20	21
31-36	20	21	22	23	24	25
37-42	24	25	26	27	28	29
43-48	28	29	30	31	32	1

図 10：拡大転置表(E)

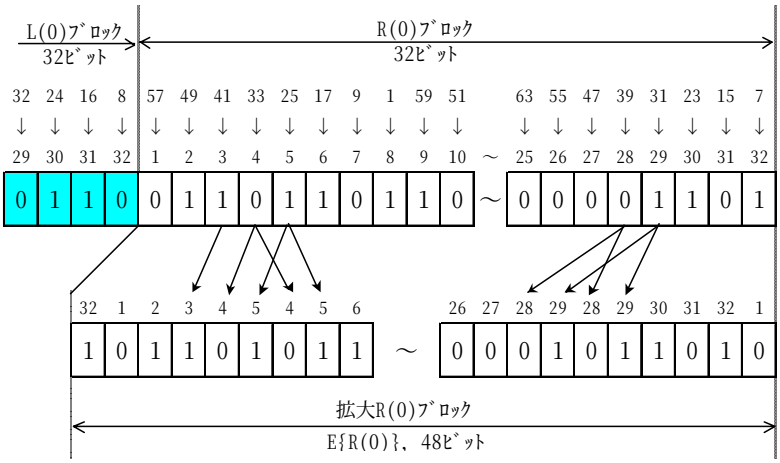

図 11：平文系Ｒ(0)32 ビットの拡大処理

Ｒブロックと次段サブキーを加算

Ｒブロックの平文系データ E{R(i)}と次段のサブキーK(i+1)との加算は、図 12 で示すような Exclusive OR の論理で行う。この論理は 1+1=0 のように答えが偶数であれば(0)、奇数であれば(1)となる。

この加算結果の 48 ビットは６ビットずつ区切って８つのブロックにする。区切られた６ビットの左端と右端の各１ビットをあわせた２ビットが、以降説明する換字表の行を示すポンターｎになり、内側４つのビットを合わせて換字表の列を示すポインターｍになる。

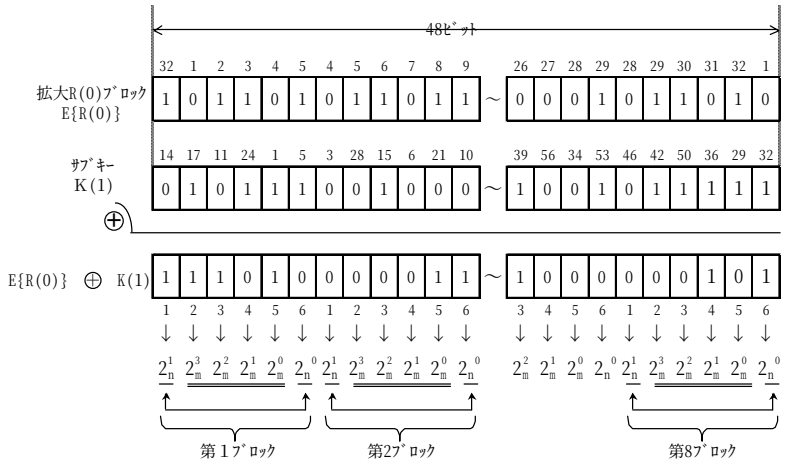

図 12：Exclusive OR の論理による加算

選択関数表による換字処理

図 12 で示した第１ブロックを例に実際に換字処理をする。第１ブロックでは、ｎ＝（１０）で２進法表記を 10 進法に変換するとｎ＝２となる。同様にして、ｍ＝（１１０１）はm=13 となる。これらを用いて図 13 から換字された出力を取り出す。

第１ブロックの例では、S_1 表の２行１３列より「１０」の数字が換字出力として取り出される。第２ブロックの場合は同様に S_2 表１行１列より「１３」が換字出力となる。図 13 中に記されている数値は、いままでの数値が選択するビットの順番を示していたのとは異なり、換字出力そのものを示す数値となる。たとえば、第１ブロックの換字出力である「１０」は、２進表示で（１０１０）、第２ブロックの換字出力「１３」は同じく（１１０１）が出力される。

これら換字関数表による換字処理は、鍵を知っている場合には、結果からもとに戻れる可逆的なプロセスである。ただし、鍵を持たない場合は、もとに戻る道筋が数通りもあり、このうちのどれが正しいかをサブキーが不明な条件下で断定することは不可能になる。この選択関数処理は、非線形なプロセスであるがゆえに、DES 暗号の暗号出力からの鍵の推定を著しく困難にしている。

また、換字前の１つのブロックは６ビットであったが、換字後は４ビットに減少し、全体の８ブロックで 48 ビットだったデータが、32 ビットに縮小されたことになる。

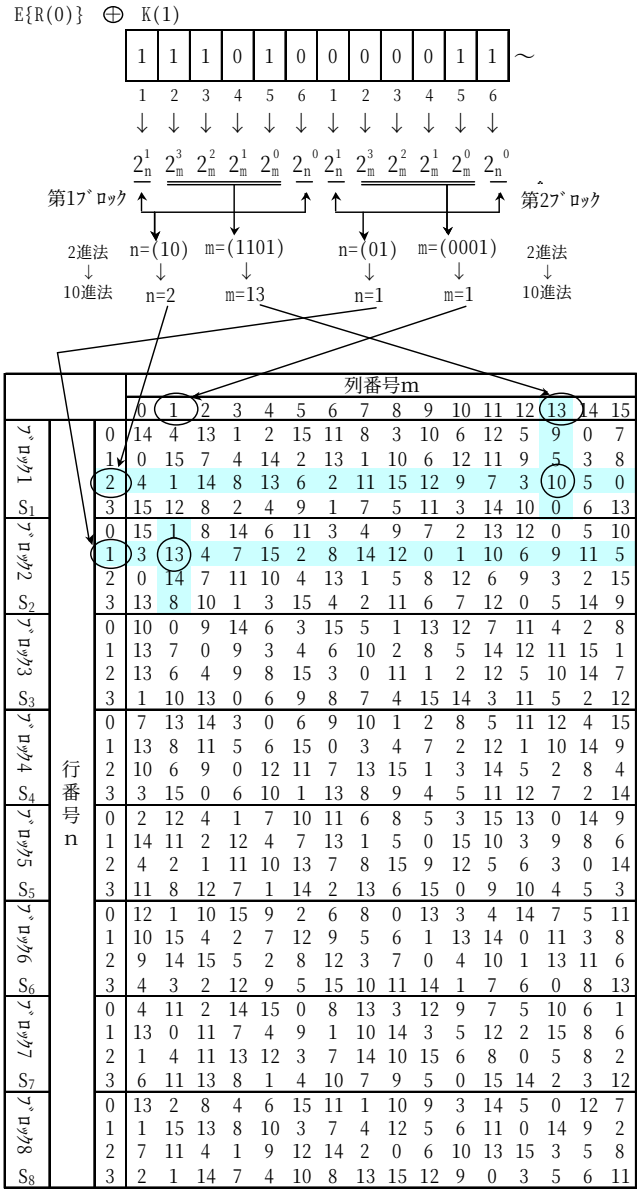

図 13：換字選択関数表

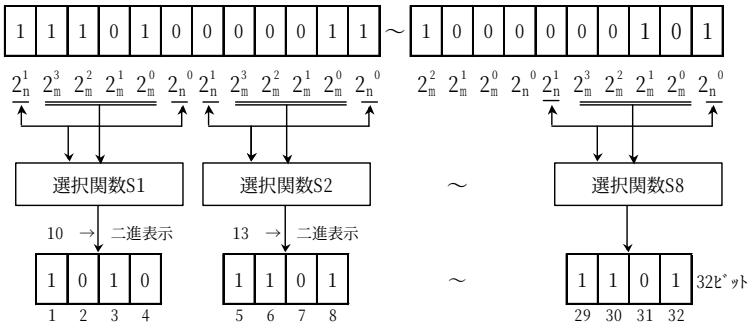

図 14：選択関数表で換字された出力

関数処理後の転置（Ｐ転置）

選択関数用（S_1～S_8）で換字された 32 ビットのデータは、次に図 15 の転置テーブルを用い図 16 に示すような転置（Ｐ転置）を行う。この処理が DES 暗号化のプロセス中で最も複雑であった関数処理の最後のプロセスになる。

転置出力ﾋﾞｯﾄ	入力ﾋﾞｯﾄ			
1-4	16	7	20	21
5-8	29	12	28	17
9-12	1	15	23	26
13-16	5	18	31	10
17-20	2	8	24	14
21-24	32	27	3	9
25-28	19	13	30	6
29-32	22	11	4	25

図 15：選択関数処理後の転置表
（P 転置）

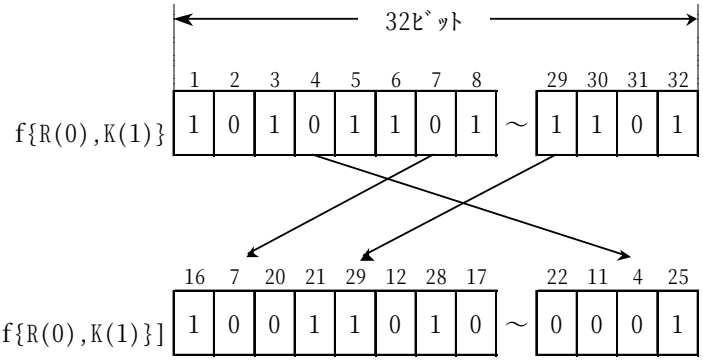

図１６：選択関数処理後の転置

Ｌブロックデータとの加算

Ｐ転置表により転置されたデータは、最後に平文系データの偶数番目のビットを集めたＬブロックと Exclusive OR の演算により、図 17 のように加算され、２段目で使用する R(1)が作成される。これで一段目の処理が終了する。

２段目の処理は、ＬブロックとＲブロックのデータを入れ替えて行う。R(0)は、そのまま L(1)として、R(1)には、これまでにサブキーとの加算や関数処理などを行ってきた前段の最終結果を用いる。

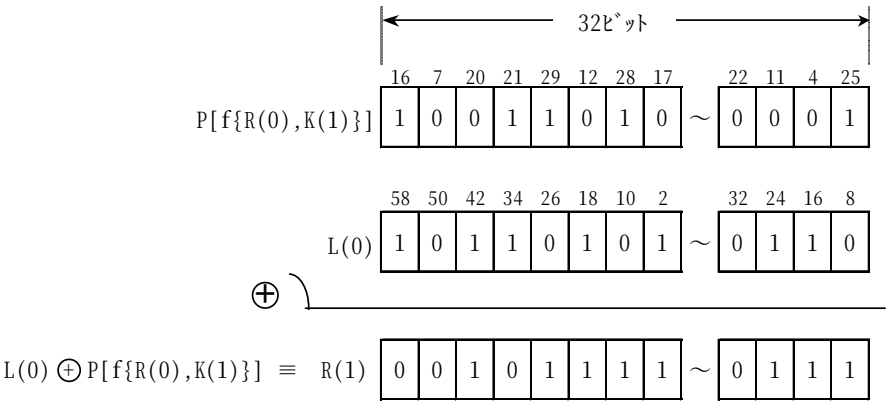

図 17：Ｌブロックのデータ加算

DES 暗号化の全体像

図 18 は DES 暗号の処理の全体像を示している。これまで、説明してきたのと同じ処理を１段目から 16 段目まで続け、最後の 16 段目の処理を終わった出力は、DES 暗号の最後の処理である最終転置を行う。

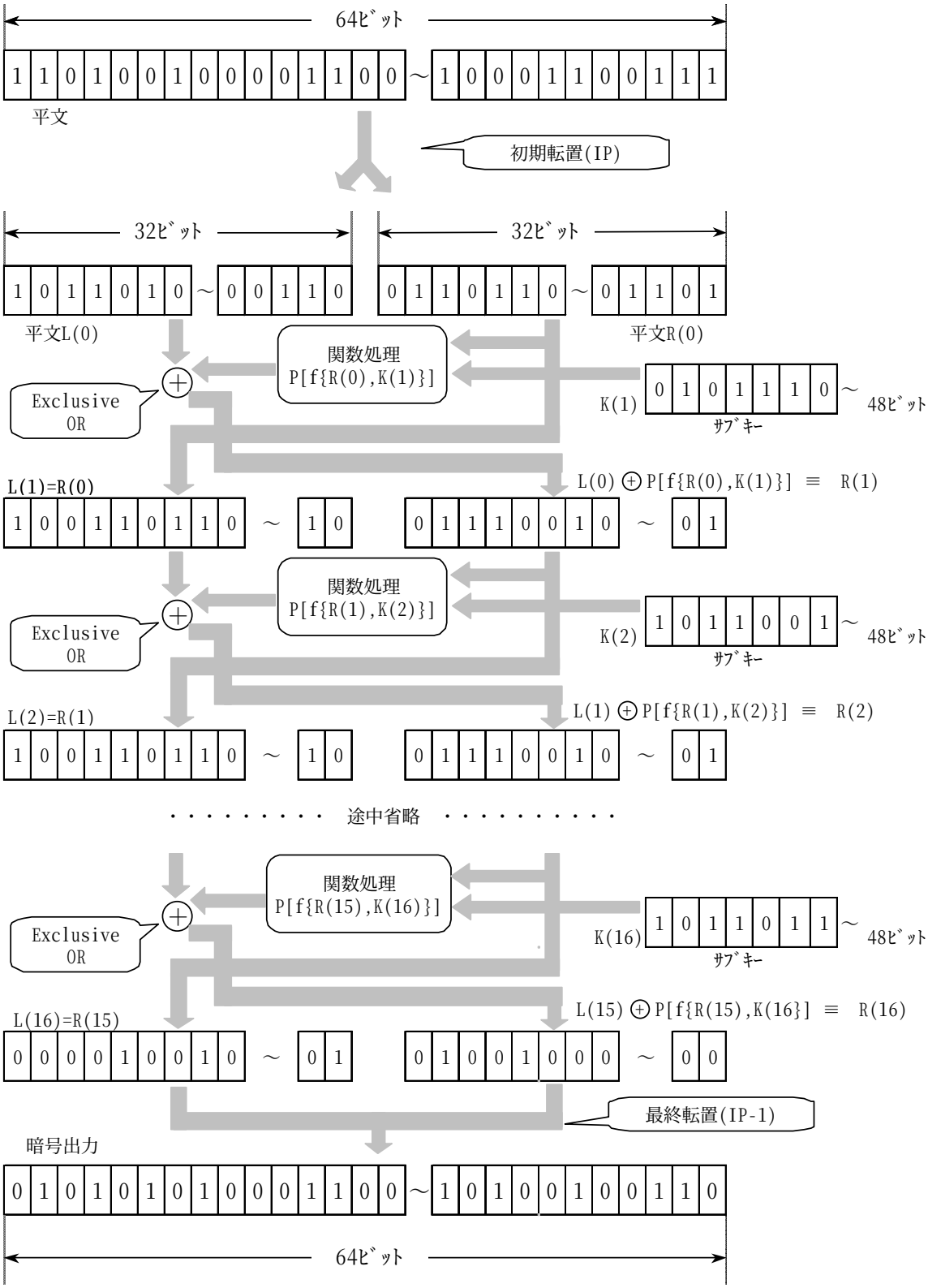

図 18:DES 暗号のフローチャート

最終転置

最終転置は、いままで区分して処理していたＬブロックとＲブロックのデータを連結したのちに図 20 の最終転置表（IP^{-1}）を用いて各ビットの並び替えを行い、この並び替えられた 64 ビットの出力を最終の暗号出力とする。

暗号文出力	最終転置入力ﾋﾞｯﾄ							
1-8	40	8	48	16	56	24	64	32
9-16	39	7	47	15	55	23	63	31
17-24	38	6	46	14	54	22	62	30
25-32	37	5	45	13	53	21	61	29
33-40	36	4	44	12	52	20	60	28
41-48	35	3	43	11	51	19	59	27
49-56	34	2	42	10	50	18	58	26
57-64	33	1	41	9	49	17	57	25

図 20：最終転置表（IP^{-1}）

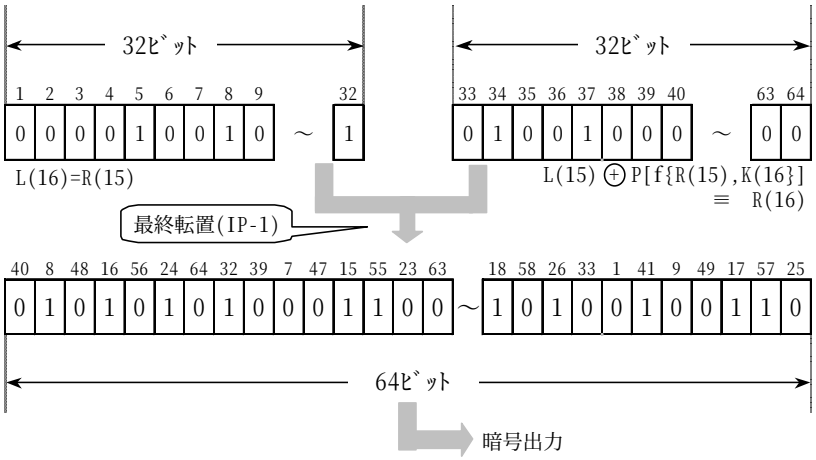

図 21：最終転置と暗号出力

DES 暗号規格の位置付け

DES 暗号化処理の全プロセスは、米国商務省の下部組織である NIST（国立標準技術研究所）の FIPS 文書で公開されている。米国では原子力関係文書などの重要文書のセキュリティを保つことが、国家機密法や原子力エネルギー法などの法律で義務付けられており、これらの文書の暗号化に DES 暗号が使用されている。また、政府機関以外の民間組織でも DES 暗号を使うことが同時に許容されている。

DES 暗号の今後

DES 暗号をもたずに読解をしようとすれば、鍵の長さは実質 56 ビットなので、手当たり次第に鍵を探りあてようとすれば平均して 2 の 56 乗の計算が必要となる。これは 10 進法に直せば 7 京という大きさであり、多くのコンピュータが無制限に自由に使えるだけの費用と時間が必須になる。

最近では、米国 RSA 社などが主催して暗号の安全性を確かめる目的で、賞金付きの暗号読解コンテストが開かれている。1998 年のコンテストでは、あるチームが多数台のパソコンをインターネットでつなぎ込んで、DES 暗号化した暗号文の読解に成功した。1999 年のコンテストでは、同じくインターネットを使っての DES 暗号の読解が、ついに 22 時間という早さで実現した。

1977 年の公布以来、５年ごとに見直しを行い、追加修正を行ってきた DES 暗号も 20 数年しかもちこたえることができずに、過去の暗号として扱わざるをえなくなってしまった。この結果、NIST は AES（Advanced Encryption Standard）と呼ばれる次世代の暗号技術の公募に踏み切り、応募したいくつかの方式が現在暗号強度評価テストなどを受けている。この間のつなぎとして、NIST は ANSI（米国規格協会）が先に規格化したトリプル DES を追認したうえで、DES 暗号を踏まえた改良型として推奨している。

３で使用した参考文献

「わかりやすい暗号学」高田　豊、米田出版、2000.11
「暗号理論の基礎」Douglas R.Stinson、共立出版、1996.11