

第3講 暗号をつくろう

3_1 指で数える2進法

「いい、これが基本形。これは1。それじゃ、これはいくつ？」などと、指を使った遊びをご存知ですか？
これからお話しするのはちゃんとした理屈のある手遊びです。

例1



これは13

例2



これは28

例3



ではこれは？

これは2進法を使った数の表現なのです。右の手のように

- 親指 1の位
- 人差し指 2の位
- 中指 $2^2 = 4$ の位
- 薬指 $2^3 = 8$ の位
- 小指 $2^4 = 16$ の位

を対応させます。

指が折れている状態で1, 折れていなければ0をあらわします。例えば, 最初の例1, 例2では次の様に考えます。

小指	薬指	中指	人指し指	親指		小指	薬指	中指	人指し指	親指	
指	指	指	指	指		指	指	指	指	指	
(16)	(8)	(4)	(2)	(1)		(16)	(8)	(4)	(2)	(1)	
×	×	×	×	×		×	×	×	×	×	
0	1	1	0	1		1	1	1	0	0	
0 + 8 + 4 + 0 + 1 = 13						16 + 8 + 4 + 0 + 0 = 28					

つまり2進数で

$$1101_{(2)}=13, \quad 11100_{(2)}=28$$

を表わしているのです。

問題. 例3はいくつになるでしょう。

3_2 記数法で暗号を作る

25個のタイルをまとめるときに, 10のかたまりを2個とタイル5個, というようにまとめるのが普通ですが, これを別な方法でまとめてみましょう。

縦・横ともにタイル3個ずつの正方形(9のかたまり)が2枚, 縦3個・横1個の長方形(3のかたまり)が2つ, あとタイル1個. これを $221_{(3)}$ と表わすことにします. ここで(3)は3個ずつまとめることを表わしています.

同様にして4個ずつまとめると $121_{(4)}$ と表わすことができますね. これらの表わし方を3進法, 4進法による表示とといいます.

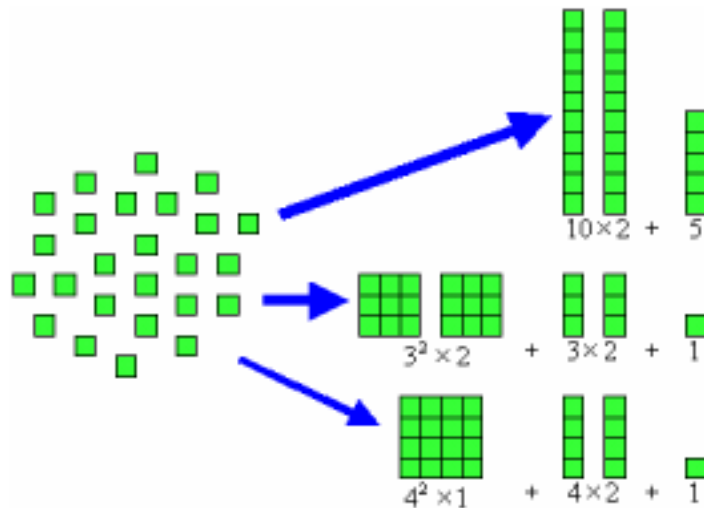
これを計算の上で考えると,

$$25 = 3 \times 8 + 1 = 3(3 \times 2 + 2) + 1 = 2 \times 3^2 + 2 \times 3 + 1$$

というように, 3で割って商と余りを求め, 次にその商を再び3で割って...という計算を繰り返すこととなります。

そこでこれを, 右のように簡便な計算で求めることができます。

$$\begin{array}{r} 3 \left\{ \begin{array}{l} 25 \cdots 1 \\ 8 \cdots 2 \\ \hline 2 \end{array} \right. \end{array}$$



さてこの記数法を用いて暗号を作ってみましょう。

アルファベット 26 文字を数字に置き換え、26 進法表示を考えます。つまり次の図のようにまずアルファベットの a から順に数字を当てはめます。

<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>	<i>f</i>	<i>g</i>	<i>h</i>	<i>i</i>	<i>j</i>	<i>k</i>	<i>l</i>	<i>M</i>
0	1	2	3	4	5	6	7	8	9	10	11	12
<i>n</i>	<i>o</i>	<i>p</i>	<i>q</i>	<i>r</i>	<i>s</i>	<i>t</i>	<i>u</i>	<i>v</i>	<i>w</i>	<i>x</i>	<i>y</i>	<i>z</i>
13	14	15	16	17	18	19	20	21	22	23	24	25

例えば cap(帽子)という文字を数字に置き換えると、2, 0, 15 となります。これを 26 進法表示だと考え、10 進法表示に直すと、

$$2 \times 26^2 + 0 \times 26 + 15 = 2 \times 676 + 0 \times 26 + 15 = 1367$$

となります。つまり cap 1367 ということになります。

逆に 1367 を 26 進法表示すると、右の図から 2, 0, 15 という数字が得られます。きちんと 1 対 1 に対応していますね。

$$\begin{array}{r} 26 \overline{) 1367} \dots 15 \\ \underline{52} \dots 0 \\ 2 \end{array}$$

同様に e g g(卵)という文字を暗号に直してみましょう。e = 4, g = 6 ですから

$$4 \times 26^2 + 6 \times 26 + 6 = 4 \times 676 + 6 \times 26 + 6 = 2866$$

つまり e g g 2866 になります。

問題。

- (1) box(箱)を数字に直すといくつになるでしょう。
- (2) 13223 という数字はどんな文字を表わしているでしょうか？

3_3 シーザー暗号

インターネットや電子メールなどの普及に伴い、プライベートな情報や重要なデータがネットワークを通じて大量に流れるようになりました。インターネットでは、ホームページのデータや電子メールのデータが、コンピュータからコンピュータへとパケットリレー式に送られていきます。

いろいろなコンピュータの間をデータが送られていくとき、このデータを見ることが可能なのです。つまり電子メールなどは、誰か知らない人に読まれてしまう危険性があるわけです。盗聴だけが危険なのではありません。情報の内容を勝手に書き換えてしまったり(改ざん)、誰かが正当なユーザーになりすましてネットワークを悪用(なりすまし)する危険性もあるのです。

それらの脅威を防ぐための解決法として、暗号化が注目を集めています。たとえ、データが盗み出されても第三者に解読できなければ、データとしての価値はないからです。暗号というのは第三者に情報をもらさないようにするために、情報の見た目を変えてしまう手段のことです。暗号と聞くと大げさで、自分には関係ないと思う人も多いでしょう。しかし、既に現在、電子商取引ではクレジットカード番号等の情報を送信する際に暗号化が施されています。

そんな暗号のごく簡単な例を紹介しましょう。暗号の歴史は古代ローマ時代にまでさかのぼり、ジュリアス・シーザーがガリア=ローマ間の通信に用いたといわれる「シーザー暗号」が有名です。このシーザー暗号は、文字をアルファベット順に特定の文字数だけずらすといった非常に簡単なもので、換字式(かえじしき)暗号ともいいます。

例えば「apple」という言葉をアルファベット順に 3 ずつずらすと「dssoh」が得られます。



暗号にする前の元のデータを「平文(ひらぶん)」といいます。シーザー暗号の場合「アルファベット順に3ずつずらす」という規則で暗号を作成しています。これを「暗号方式(アルゴリズム)」といいます。

この暗号文を相手に伝えます。その際、この暗号文が周囲に洩れてしまっても暗号化されている文なので元のデータを知られずに済みます。そしてこの暗号文を得た相手は、この暗号文から平文を得る作業を行う必要があります。この作業のことを「復号」といいます。正当な受信者でない人が暗号文から平文を得ようとする場合は「解読」と呼びます。

さて復号を行う際に問題になるのは暗号化のときに何文字ずらしたか、という情報です。このずらした数がわからなければシーザー暗号を利用したことがわかっていても復号することができません。このずらす数を変えることで様々な暗号のパターンを作り出すことができます。この値のことを「鍵」といいます。



このシーザー暗号には、鍵が1文字ずらす場合から26文字ずらす場合のせいぜい26パターン程度しかないため、全てのパターンで暗号文を逆にずらしてみても何らかの文が得られるかどうかを試してみることが可能です。そこでこのシーザー暗号を改良した「多文字置換暗号」という暗号化を見てみましょう。

これはシーザー暗号を複雑化したもので、平文の文字一字一字に鍵を当てはめその数だけ右にずらす(はみ出た場合は先頭に戻る)というものです。それでは「I am a boy」という文章に鍵「7324」を用いて暗号化してみましょう。

平文	I	a	m	a	b	o	y
鍵	7	3	2	4	7	3	2
暗号文	p	d	O	e	i	r	a

つまり暗号文「p do eira」が得られました。しかし多文字置換暗号も簡単に解読されるケースが多く、それほど安全ではありません。キーワードが繰り返し使用されることや、使用頻度の高い文字を元にキーワードが簡単に推測されてしまうなどの欠点があります。

シーザー暗号以外の古典的な暗号としては、転置式暗号や円盤式暗号などがあります。転置式暗号とは平文の構成要素の順序を変えて暗号文にする方法です。例えば何行かに平文を書いてそれを縦の列に暗号化する。そして更に1列目、2列目、・・・と順番に読んでいくのではなく、例えば1列目、3列目、2列目、・・・といれかえて読んでいく、ということをするのが転置式暗号というものです。例えば「かぎはつくえのにはんめのひきだし」という平文を暗号化すると右の表のようになります。この表は上記の平文を横向きに4行に書いたものです。それを縦向きに1 3 2 4の順番に書き直すと「かくばひはのめだぎえんきつにのし」となります。これが暗号化された文章になります。そしてこの方法で作られた暗号を転置式暗号といいます。

円盤式暗号とは「シーザー暗号」をかたんに作る暗号機のごとで、次のようにして作成します。まず内側の小さい円盤を適当に回して位置を決め、外側の大きい円盤の好きな文字を、長い方の矢印で指します。そのとき、短い方の矢印が指している小さい円盤の文字を読みます。暗号にする文章の文字を長い矢印でさして、そのときの短い矢印の文字を書いていくとどんどん暗号ができていきます。



問題.

- (1) Mathe を鍵「3631」で暗号化してみよう。
- (2) HGWW を鍵「1234」で復号化してみよう。

3.4 RSA 暗号

父から預かった銀行のキャッシュカードのパスワードを忘れた A 君は、父に次のようなメールを打ちました。

父さんへ
 キャッシュカードのパスワードを忘れたので教えてほしい。他人に知られると困るので次の計算で出た数字をメールで教えてくれ。
 『まずパスワードの数字を37乗する。次に出した数値を2491で割る。そのときの余りの数字。』

さてこのメールの内容に関して、いくつかの疑問が生じてきます。

4桁のパスワードの数字を37乗して2491で割るなんて計算、どうやってやるのだろう。

送られてきた数字から本当にパスワードがわかるのだろうか。

このメールを誰かに盗聴されたら、その人にもパスワードを知られてしまわないか。

それでは送信するパスワードを「1234」として、これらの疑問を解き明かしてみましょう。

《疑問》

1234^{37} はそのまま計算すると36回の掛け算をしなくてははいけません。膨大な数になることが予想され、なにより電卓では計算できないでしょう。欲しい値は2491で割った余りなので、2491より小さい数になるはずで、ある整数で割ったときの余りが等しいとき2つの整数は「合同」とであるといい記号「 \equiv 」であらわすことにします。これを用いると、

1234^2	$= 1522756$	755	
1234^4	$= 755^2$	$= 570025$	2077
1234^8	$= 2077^2$	$= 4313929$	2008
1234^{16}	$= 2088^2$	$= 4032064$	1626
1234^{32}	$= 1626^2$	$= 2643876$	925

ここまでで 5 回の掛け算をしています。それでは 1234^{37} を求めてみましょう。

1234^{37}	$= 1234^{32} \times 1234^4 \times 1234^1$	$925 \times 2077 \times 1234$
	$= 1921225 \times 1234$	664×1234
	$= 819376$	2328

つまり A 君の父さんは「2328」という数字をメールで送ればいいことになりますね。

《疑問》

送られてきた数字から A 君はどうやって元の数字を復元するのでしょうか。次の表を見て下さい。この表は左端の数字を上端の数字乗して 21 で割った余りを求めたものです。

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	4	8	16	11	1	2	4	8	16	11	1	2	4	8	16	11	1	2
3	9	6	18	12	15	3	9	6	18	12	15	3	9	6	18	12	15	3
4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4	16	1	4
5	4	20	16	17	1	5	4	20	16	17	1	5	4	20	16	17	1	5
6	15	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6	15	6
7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8	1	8
9	18	15	9	18	15	9	18	15	9	18	15	9	18	15	9	18	15	9
10	16	13	4	19	1	10	16	13	4	19	1	10	16	13	4	19	1	10

元の数字が何であれ 7 乗, 13 乗, 19 乗, ... すると元に戻ることに気づきましたか。ある数字を 17 乗したとすると, 出た数字にまた 5 乗してやる, 即ち $17 \times 5 = 85$ 乗で元に戻るのです。

$$C = M^{17} \quad C \quad M = C^5$$

実は A 君はもらった数字を何乗すれば元に戻るか知っていたのです。まず次の計算をします。

2328^2	1659	2328^4	2217	2328^8	346
2328^{16}	148	2328^{32}	1976	2328^{64}	1179

そして父さんからもらった「2328」を秘密の数字「97」を元に $2328^{97} \div 2491$ を計算します。

$$2328^{97} = 2328^{64} \times 2328^{32} \times 2328^1 \quad 1179 \times 1976 \times 2328 = 2329704 \times 2328 \quad 1441032 \quad 1234$$

こうやって A 君は父さんからパスワード「1234」を手に入れることができました。

《疑問》

「37 乗して 2491 で割ると 2328 になる」ということを, もし他人が盗聴したとしたらパスワードを知られてしまうのではない。実はこれぐらいの数字ではコンピュータに解析させればすぐにわかってしまうでしょう。しかし, 割る数字を 150 桁ぐらいだとどうでしょう。これだとたとえコンピュータでも膨大な時間がかかるのです。

少し理論的なことをお話ししましょう。異なる 2 つの素数 P, Q を決めます。そして $N = P \times Q$ で割った余りの世界を考えます。これを N を「法」とする世界といいます。P - 1 と Q - 1 の最小公倍数を L とするとき, N を「法」とする世界では全ての数は $k \times L + 1$ 乗するとどんな数も必ず自分自身に戻るのです。つまり元の数を X とし, L と素な数 D, E に対して次の式が成り立ちます。

$$(X^D)^E = X \quad (\text{ただし } DE = k \times L + 1)$$

先ほどの例で言えば A 君は 2 つの素数 $P=47, Q=53$ を最初に選んで置き, $N=PQ=47 \times 53=2491$ を法とする世界を作り出したのです。そして 46 と 52 の最小公倍数 1196 と素な数 $E=37$ と選んで父さんに計算させました。その後 $D=97$ で復元させたのです。法とする数 $N (= P \times Q)$ と E は「公開鍵」, D は「秘密の鍵」となります。しかし N と E を公開しても大丈夫なのは不思議ですね。

結局, 重要なのは 2 つの素数 P と Q です。この数字から $N=PQ$ を作り出すのは簡単ですが, 反対に N を 2 つの素数 P, Q の積に表す, つまり素因数分解する効率の良い方法は見つかっていないのです。この暗号の秘密は「素因数分解の困難性」に起因していたのです。