暗号とは 2 者間で情報交換を行う際に，悪意のある第三者にその内容が伝わらないようにする仕組みである．このような仕組みは古代から必要され，様々な暗号方式が考案されてきた．これらの暗号は現代の高度な情報化社会では役に立たないものとなってしまっているが，暗号の考え方を理解するために，簡単な暗号の紹介から始める．実際に話を始める前に，まず基本的な約束事から始める．

まず暗号化す前の意味が理解でき直接利用できる文を**平文** (plaintext) といい，暗号化した特別な知識・解読作業なしでは読めないよう文を**暗号文**という．ここでは，簡単のために扱うのは英文に限ることし，平文は小文字で表し，暗号文は大文字を用いて表すことにする．平文を暗号文に変換することを**暗号化**（encryption）といい，暗号文を元の平文に戻すことを**復号**（decryption）という．

暗号化方式を数学的に扱うために，伝達文（メッセージ）は数で表すとする．そのために，アルファベットに次のように番号を振ることにする．

a	b	c	d	e	f	g	h	i	j	k	l	m
00	01	02	03	04	05	06	07	08	09	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

そして，すべての計算は mod 26 で行う．通常は，英文はスペースと句読点を用いて書かれるので，それらにも番号を振るべきであるが，その場合は mod 27, mod 28, . . . を用いて計算される．

情報の交換を行う際の登場するのは，送信者と受信者，そしてそれを盗聴しようとする者などであるが，暗号の解説を行うには，これらの登場人物を無味乾燥な A, B などとはせず，慣習により次のように名付る．

送信者（sender）　Alice
受信者（receiver）　Bob
盗聴者（attacker）　Eve

● シーザー暗号

まず最初に，単純な古典的暗号であるシーザー暗号について述べる．**シーザー暗号**（Caesar cipher）は古代ローマの独裁者 Julius Caesar (100-44 B.C.) に因んで名付けられた暗号化の方法で，平文で用いられるアルファベットを 3 つだけ前にずらすことによって暗号化する方法である．

例 1.　平文：　i came i saw i conquered
　　暗号文：　L FDPH L VDZ L FRQTXHUHG

上の表で i には 8 が対応するので，下の表で $8+3=11$ に対応する L を対応させるといった具合に暗号化する．例 1 では出てこないが，例えば，y を暗号化しようとすると $24+3\equiv 1 \pmod{26}$ なので，B が対応する．

00	01	02	03	04	05	06	07	08	09	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

入学年度		学部	学 科		組		番　号			検	フリガナ	
		B		1							氏 名	

1 “hello world” をシーザー暗号により暗号化せよ．

2 暗号文 “YHQL YLGL YLFL” はシーザー暗号で暗号化されているとわかっている．これを復号し平文に戻せ．

数学的には平文の文字を数 x で表すとき，$E(x)=x+3 \pmod{26}$ という関数を考え，$E(x)$ の値に対応する文字を暗号とする．また，復号するためには $E(x)$ の逆関数である $D(x)=x-3 \pmod{26}$ を用いればよいことが容易にわかる．

● シフト暗号

シーザー暗号の拡張として，文字を 3 文字ではなく，一般に k 文字ずらして暗号化する方法が考えられる．すなわち，k を整数として，暗号化する関数と復号のための関数をそれぞれ

暗号化：　$E_k(x)=x+k \pmod{26}$
復号：　$D_k(x)=x-k \pmod{26}$

と定義する．この暗号化の仕組みを**シフト暗号**という．

例 2. 簡単のために，E_k，D_k を拡大解釈し，x の代わりに文字列をそのまま代入して表すとすると，次のようになる．

$E_2(\text{example})=\text{GZCORNG}$
$E_3(\text{example})=\text{HADPSOH}$
$E_1(\text{hal})=\text{IBM}$
$E_3(\text{cold})=\text{FROG}$

3 $k=7$ として “i came i saw i conquered” を暗号化せよ．

4 $k=7$ として “KPZWSHJL ZLCLU SLAALYZ” を復号せよ．

【裏に続く】

コンピュータが使える現代では，シフト暗号は安全とは言えない．鍵 k として使える数は 26 種類しかないので，ブルート・フォース攻撃（brute-force attack，力ずくの攻撃）によって簡単に解読されてしまう．例えば，“MJ AI AMWL XS VITPEGI PIXXIVW” という暗号文がシフト暗号で暗号化されたものだと疑われたとき，これを様々な k の値について，D_k を用いて復号を試みると，

$$\begin{aligned}
k = 1: &\quad \text{li zh zlvk wr uhsodfh ohwwhuv}\\
k = 2: &\quad \text{kh yg ykuj vq tgrnceg ngvvgtu}\\
k = 3: &\quad \text{jg xf xjti up sfqmbdf mfuufst}\\
k = 4: &\quad \text{if we wish to replace letters}\\
k = 5: &\quad \text{he vd vhrg sn qdokzbd kdssdqr}\\
&\quad \cdots
\end{aligned}$$

となり，平文は “if we wish to replace letters” であると解読できる．

● アフィン暗号

鍵の数を増やすために，単純なシフト $x \mapsto x + k$ だけでなく，1 次関数一般 $x \mapsto ax + b$ を利用することを考える．すなわち，暗号化する関数を

$$E_{(a,b)}(x) = ax + b \pmod{26}$$

と定義する．1 次関数 $y = ax + b$ はアフィン関数という別名を持つので，この暗号化方式をアフィン暗号という．ここで，a, b は任意の整数 mod 26 といいたいところだが，暗号は鍵さえ用いれば，もとの平文を忠実に再現できなければならない．そのためには，$E_{(a,b)}(x)$ が逆関数を持つこと，すなわち，$y = ax + b \pmod{26}$ が x について解けることが必要である．$y = ax + b \pmod{26}$ は，a が $\mathbb{Z}/26\mathbb{Z}$ 内で逆元 a^{-1} を持つとき，またそのときに限り解くことが出来，$x = a^{-1}(y - b)$ となるので，復号関数を

$$D_{(a,b)}(x) = a^{-1}(x - b) \pmod{26}$$

と定義できる．

3 $(a, b) = (9, 2)$ として，$E_{(9,2)}$ を用いて “affine” を暗号化せよ．

4 鍵として用いることの出来る (a, b) は全部で何通りあるか．［ヒント：Euler の関数を用いる．］

鍵を増やす素朴なアイディアとして，26 文字 a, b,. . . , z の任意の置換を考えることができる．この場合，26 文字の異なる順列の数は 26! あるから，ブルート・フォース攻撃によって解読するには最悪 $26! = 4 \times 10^{26}$ 個の鍵を試さなければいけないことになる．しかし，この程度の数であれば，現代のコンピュータ技術では難なく解けてしまう．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)