$\sigma(z)=0$ を解いて，$z=\alpha^9,\alpha^{11},\alpha^{14}$ を得る．$\alpha^i-z=\alpha^i(1-\alpha^{-i}z)$ より，それぞれ $\alpha^{-6},\alpha^{-4},\alpha^{-1}$ を用いて誤り位置 $\mathscr{E}=\{1,4,6\}$ となる．これは $\boldsymbol{e}=\boldsymbol{y}$ を示す．□

本章のまとめ

1° q 元 BCH 符号の復号手順は次の通りである．

(1) **受信多項式** $y(z)$ よりシンドローム $s_j=\sum_{i=0}^{n-1}y_i\alpha^{ij}\quad(j=1,2,\cdots,2t)$ を求める．$s_j=0\ (j=1,2,\cdots,2t)$ ならば誤りなしとして完了，$s_j\neq 0$ となる j があれば (2) へ．

(2) **シンドローム多項式** $S(z)=s_1+s_2z+\cdots+s_{2t}z^{2t-1}$ を計算する．$r_{-1}(z)=z^{2t},r_0(z)=S(z)$，$i=1$ とする．また，$a_{-1}(z)=0$，$a_0(z)=1$ とする．

(3) ユークリッド復号法により**基本方程式**を解く．すなわち

$$r_{i-2}(z)=q_i(z)r_{i-1}(z)+r_i(z)$$

$$\deg r_{i-1}(z)>\deg r_i(z),i=1,2,\cdots$$

を実行する．$\deg r_i(z)\leq t-1$ のとき停止する．

(4) **誤り位置多項式** $\sigma(z)=\gamma a_h(z)$ として求め，**チェン探索**により $\sigma(\alpha^i)=0$ となる i を求める．ただし，γ は $\sigma(0)=1$ とするための係数である．

(5) **誤り数値多項式** $\eta(z)=(-1)^h r_h(z)$ から誤り数値 $e_i=-\eta(\alpha^i)/\sigma'(\alpha^i)$ を求め第 $i+1$ の記号を $y_i-e_i=\hat{x}_i$ とする．

2° 誤り訂正のための復号アルゴリズムの計算量は $O(t^2)$（特別な場合，$O(n\log_2^2 n)$）程度である．

演 習 問 題

［**16.1**］ 2元 (15,5,7)BCH 符号を考える．

(1) 生成多項式 $G(z)$ の例を示せ．

(2) 情報多項式 $u(z)=1+z^2+z^4$ のとき，符号多項式 $x(z)$ を求めよ．

(3) 誤り多項式 $e_1(z)=1+z^6+z^7$，$e_2(z)=1+z^7+z^9+z^{12}$ のとき，それぞれ誤り訂正を行え．

［**16.2**］ 2^4 元 (15,11,5)RS 符号を考える．

(1) 生成多項式 $G(z)$ を示せ．

(2) 符号語 $\boldsymbol{x}=1\alpha^8 0\alpha^7\alpha^{13}\alpha^{14}\alpha 000\alpha^{13}\alpha^6\alpha^9\alpha\alpha^3$ とし，
受信語 $\boldsymbol{y}=1\alpha^8 0\alpha^{11}\alpha^{13}\alpha^{14}\alpha 000\alpha^2\alpha^6\alpha^9\alpha\alpha^3$
とするとき，誤り訂正を実行せよ．

V 暗号と情報セキュリティ

17
暗号系と情報セキュリティ技術

映画「007 ロシアより愛をこめて」では，主人公のジェームス・ボンドがイスタンブールのソ連大使館で女性暗号解読員 T. ロマノアの手引きで携帯用タイプライタのようなケースに入った暗号翻訳機レクターを盗み出すシーンがある．爆破されるビルの中からケースをもって地下水路を逃げる様子は当時の冷戦の縮図のようで印象深い．

第 2 次世界大戦ではドイツ軍のエニグマ暗号が活躍した．エニグマ暗号法では異なる素数の周期をもつ数枚の歯車を組み合わせて長い周期の暗号鍵を作成する．この暗号機は堅牢で実用性が高い．日本帝国海軍もドイツ製エニグマ暗号機を購入し，海軍独自の改造をして九一式暗号機を作った．外務省はこれにさらに手を加え九七式欧文印刷機を作り外交用暗号として用いた．これは米国でパープル暗号と呼ばれ周期を推定したり，言語の冗長性（文字の出現頻度）などを用いてかなり高い割合で解読されていた．残念ながらこれがわが国の敗戦の一因であったことは疑う余地もない．最近ではサイバー（電脳）戦争（例えば，敵国のコンピュータをウィルスに感染させ軍事指令系統を麻痺させるなど）が研究されようとしており，暗号というと外交・軍事で余り明るいイメージはない．

しかし一方で，暗号技術は電子現金，電子決済，電子商取引，著作権保護など経済社会をささえる基盤としても注目されている．いずれにせよ，情報の価値が増し，不正に対する何らかのセキュリティ（保護）対策が必要なのである．本章ではそのために必要な暗号技術を紹介する．

まず，歴史的な源流として情報理論からみた暗号について述べ，次に 1970 年以降のアルゴリズム論・計算量理論の立場から生れた新しいタイプの暗号系を示す．前者はシャノンにより情報量の立場から考察されバーナム (G. Vernam) **暗号**といわれる乱数列を鍵とし，鍵に対応する値だけ加えたりずらしたりするもので情報理論的に最も安全（鍵を知らない限りどんな方法を用いても暗号解読が不可能）である．ただし，鍵の使い捨て（one time pad）方式で，長い鍵の系列を必要とするから実用的ではない．後者は，計算量的に安全性を保証するもの（鍵を知らないと計算機の性能と計算時間の点から暗号解読が不可能）で，暗号化のアルゴリズムが公開されるという特徴がある．1977 年米国標準暗号 **DES**（data encryption standard）に代表される**秘密鍵暗号**（**慣用暗号**，**対称暗号**，**共通鍵暗号**ともいう）系と 1976 年ディフィー（W. Diffie）とヘルマン

(M. Hellman) により考え出された**公開鍵暗号**（**非対称暗号**ともいう）系で鍵の一部を公開するという画期的なもので，後の 1978 年にリベスト (R. L. Rivest)，シャミヤー (A. Shamir)，アードルマン (L. Adelman) によって提案された **RSA 暗号**がよく知られている．

なお，暗号系のモデルを図 17.0.1 に示す．情報源 $\mathscr{M}$ から出力された通常の誰にも意味が理解できる平文を m，これを**暗号化鍵** K_E を用いて暗号器により暗号化し意味が理解できない**暗号文** c に変換し通信路に送り出す[1]．通信路には誤りはないものとし，復号器の入力 c から復号鍵 K_D により復号し元の平文 m を受信者 $\hat{\mathscr{M}}$ に出力する．これを次のように表わす．

$$\begin{aligned} &\text{暗号化 } C: \quad c = C_{K_E}(m) \\ &\text{復　号 } D: \quad m = D_{K_D}(c) \end{aligned} \tag{17.0.1}$$

ここで

$$m = D_{K_D}(C_{K_E}(m)) \tag{17.0.2}$$

が成立しなければならない[2]．ここでは，m, c とも 2 元記号または 10 元記号とし，数十ビット以上，あるいは 10 進数数百桁のブロックごとに暗号化，復号化するブロック暗号を示すが[3]，1 ビットあるいは 10 進数 1 桁ごとに逐次暗号化・復号するストリーム暗号もある．

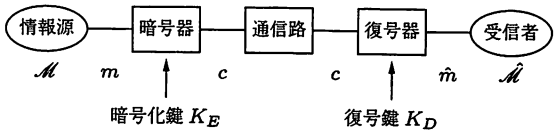


図 17.0.1: 暗号系のモデル

［例 **17.0.2**］ バーナム暗号の例

先ほど情報理論的に安全な暗号として述べたバーナム暗号の最も簡単なものは，2 元記号に対し 2 元乱数列 $\boldsymbol{k}$ を用いて

$$\text{暗号化 : } c_i = m_i + k_i \pmod 2 \tag{17.0.3}$$

$$\text{復　号 : } m_i = c_i + k_i \pmod 2 \tag{17.0.4}$$

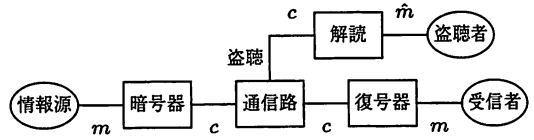
ただし，$\boldsymbol{m} = (m_1, m_2, \cdots, m_N), \boldsymbol{c} = (c_1, c_2, \cdots, c_N)$, $K_E = K_D = \boldsymbol{k} = (k_1, k_2, \cdots, k_N)$ と表わせる．すなわち 2 元乱数列を鍵 $K = K_E = K_D$ とするブロック暗号である． □

暗号の役割は大別して情報の秘匿と認証である．前章までの議論と違い暗号系では図 17.0.2(a) に示すように暗号文 c が不正な第三者 (**盗聴者**) により**盗聴**されること，(b) に示すように暗号文 c が不正な第三者により**改ざん**され c' となることの他，不正な第三者が正当な送信者になりすまし，あるいは送信者（受信者）が平文 m を送信（受信）しているにも拘らず送信（受信）していないと主張する**否認**などを考え対策を立てねばならない．**改ざん**，**なりすまし**，**否認**には認証機能が必要である．

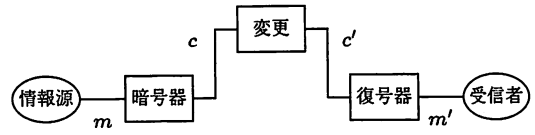
[1] 本章で用いる K は鍵を示し，前章まで用いた N, K, D, R などとは全く異なる．巻末記号表参照．

[2] 式 (17.0.2) は平文 m から暗号文 c を得たとき，c から一意に元の m に戻らなければならないことを示す．

[3] 平文，暗号文ともベクトル表現すべきであるが，通常数値として計算する場合はそのまま m, c などと表す．



(a) 盗聴



(b) 改ざん

図 17.0.2: 暗号系における不正

17.1 情報量からみた暗号系

まず，式 (17.0.1)，(17.0.2) において $K_E = K_D = K$ とする．すなわち，暗号化鍵と復号鍵は同一で共に K とする共通鍵暗号（秘密鍵暗号）を仮定する．ここで，鍵の集合を $\mathscr{K}$ で表わす．$K \in \mathscr{K} = \{K_1, K_2, \cdots, K_{\|\mathscr{K}\|}\}$ である．このとき，第 4 章のエントロピーの議論を思い出せば，鍵のエントロピー $H(\mathscr{K})$ は

$$H(\mathscr{K}) = -\sum_{i=1}^{\|\mathscr{K}\|} \Pr(K_i) \log \Pr(K_i) \tag{17.1.1}$$

である．同様に，長さ L の平文 $\boldsymbol{m}$ の集合を $\mathscr{M}^L$，長さ L の暗号文 $\boldsymbol{c}$ の集合を $\mathscr{C}^L$ とすると，平文のエントロピー $H(\mathscr{M}^L)$，暗号文のエントロピー $H(\mathscr{C}^L)$ はそれぞれ

$$H(\mathscr{M}^L) = -\sum_{\boldsymbol{m} \in \mathscr{M}^L} \Pr(\boldsymbol{m}) \log \Pr(\boldsymbol{m}) \tag{17.1.2}$$

$$H(\mathscr{C}^L) = -\sum_{\boldsymbol{c} \in \mathscr{C}^L} \Pr(\boldsymbol{c}) \log \Pr(\boldsymbol{c}) \tag{17.1.3}$$

で与えられる．$\boldsymbol{c}$ を知ったとき鍵 K_i を知っている正当な受信者は（もちろん盗聴者も K_i を知っていれば）暗号文 $\boldsymbol{c}$ から平文 $\boldsymbol{m}$ を復号できる．すなわち

$$\text{復号 } D \ : \ \boldsymbol{m} = D_{K_i}(\boldsymbol{c}) \tag{17.1.4}$$

である．いいかえれば

$$H(\mathscr{C}^L|\mathscr{K}) = H(\mathscr{M}^L) \tag{17.1.5}$$

である．一方，盗聴者は暗号文 $\boldsymbol{c} \in \mathscr{C}^L$ は知ることができるから，$\boldsymbol{c}$ を知ったときの鍵 $K_i \in \mathscr{K}$ のもつ平均情報量 $H(\mathscr{K}|\mathscr{C}^L)$ は

$$H(\mathscr{K}|\mathscr{C}^L) + H(\mathscr{C}^L) = H(\mathscr{C}^L|\mathscr{K}) + H(\mathscr{K}) \tag{17.1.6}$$

を満足する．式 (17.1.5) を代入し，$H(\mathscr{C}^L)$ を移項して

$$H(\mathscr{K}|\mathscr{C}^L) = H(\mathscr{M}^L) + H(\mathscr{K}) - H(\mathscr{C}^L) \tag{17.1.7}$$

が得られる．式 (17.1.7) は鍵のあいまいさを示しており，これが十分大きいことが解読されないために必要である．そのためには，当然右辺第 2 項 $H(\mathscr{K})$ が大きいほど，すなわち鍵が等確率で用いられるとすれば鍵の数 $\|\mathscr{K}\|$ が大きいほど安全である．また，$H(\mathscr{M}^L)$ は長さ L の平文のもつ情報量であり，長さ L の平文のもつ冗長度を $R(\mathscr{M}^L)$ とすると

$$R(\mathscr{M}^L) = L\log\|\mathscr{M}\| - H(\mathscr{M}^L) \tag{17.1.8}$$

と書ける．ここで，$\|\mathscr{M}\|$ は平文のアルファベットの大きさである．この式の意味は，平文のエントロピーは $H(\mathscr{M}^L)$ であったから平文の数はおおよそ $2^{H(\mathscr{M}^L)}$ 個であり，$\|\mathscr{M}\|^L$ 個のうち $2^{H(\mathscr{M}^L)}$ 個しか実際に用いられず残りが冗長であることを示している．平文は等確率で生起するとし，これを等確率で分布する $2^{H(\mathscr{K})} = \|\mathscr{K}\|$ 個の鍵で暗号化したとき，完全にランダムに暗号文 $\boldsymbol{c}$ が得られるとすれば，$H(\mathscr{C}^L)$ は最大の情報量をもつことになり

$$H(\mathscr{C}^L) = L\log\|\mathscr{C}\| \tag{17.1.9}$$

となる．ここでも，$\|\mathscr{C}\|$ は暗号文のアルファベットの大きさである．ここで，$\|\mathscr{C}\| = \|\mathscr{M}\|$ とし，式 (17.1.8)，(17.1.9) を式 (17.1.7) に代入すると

$$H(\mathscr{K}|\mathscr{C}^L) = H(\mathscr{K}) - R(\mathscr{M}^L) \tag{17.1.10}$$

が成り立つ．この式は，平文のもつ冗長性が小さくなければならないことを示している．さらに，式 (17.1.8) で $H(\mathscr{M}^L) \fallingdotseq LH(\mathscr{M})$，$R(\mathscr{M}^L) \fallingdotseq L\log\|\mathscr{M}\| - LH(\mathscr{M}) = LR(\mathscr{M})$ とおくと

$$H(\mathscr{K}|\mathscr{C}^L) \fallingdotseq H(\mathscr{K}) - LR(\mathscr{M}) \tag{17.1.11}$$

を満足し，これがゼロとなる系列長を L_1 とおくと

$$L_1 \fallingdotseq \frac{H(\mathscr{K})}{R(\mathscr{M})} \tag{17.1.12}$$

となる．L_1 を**一義長** (unicity length) といい，暗号文を一意に解読するために必要な系列長を示している．このことは，暗号文が長いほど元の平文に解読される可能性が高いことを示している．以上の結果，暗号文の長さ L が大きくなっても鍵のあいまいさ $H(\mathscr{K})$ が $H(\mathscr{K}) > LR(\mathscr{M})$ を満足するとき，情報理論的に安全な暗号系ということができる．

さらに別の見方をするために，平文 $\boldsymbol{m}$ と暗号文 $\boldsymbol{c}$ の (平均) 相互情報量 $I(\mathscr{M}^L;\mathscr{C}^L)$ を考える．

$$\begin{aligned} I(\mathscr{M}^L;\mathscr{C}^L) &= H(\mathscr{M}^L) - H(\mathscr{M}^L|\mathscr{C}^L) \\ &= H(\mathscr{C}^L) - H(\mathscr{C}^L|\mathscr{M}^L) \end{aligned} \tag{17.1.13}$$

であるから，暗号文ができるだけ平文についての情報を与えない方が良い．すなわち，$H(\mathscr{M}^L|\mathscr{C}^L) = H(\mathscr{M}^L)$ のとき両者は独立で，完全に安全な暗号系が得られることになる．バーナム暗号は長さ L の平文 $\boldsymbol{m}$ に対し長さ L の乱数列を加えて暗号文 $\boldsymbol{c}$ を作るから，$\boldsymbol{m}$ と $\boldsymbol{c}$ は独立となる．

［例 **17.1.1**］ 自然言語と単純置換暗号

英文の冗長性を 50% と仮定しよう．英文字アルファベットは 26 文字であるから $\|\mathscr{M}\| = 26$ である．このとき英文の冗長度 $R(\mathscr{M}) = 0.5\log_2 26 \fallingdotseq 2.35$［ビット/文字］である．**単純置換（換字）暗号** は A を A～Z の 26 通りに置換可能，次に B は A の置換したものを除いて 25 通りの置換可能，以下 C は 24 通り，D は 23 通り，$\cdots$ となり結局鍵の数 $\|\mathscr{K}\| = 26! \fallingdotseq 4.04 \times 10^{26}$ である．鍵を等確率で用いたとすると $H(\mathscr{K}) = \log\|\mathscr{K}\| \fallingdotseq 88.4$［ビット］となり一義長 $L_1 \fallingdotseq 37.6$［文字］となる．

17.2 秘密鍵暗号系

秘密鍵暗号は送信者（情報源）と受信者があらかじめ共通の秘密情報（秘密鍵 K）を共有し，この情報をもとに暗号化や認証を行う方式である．したがって，図 17.0.1 および式 (17.0.1)，(17.0.2) において $K_E = K_D = K$ である．基本的には鍵に基づいて**転字**（記号の順序を入れかえること），**換字**（記号を他の記号におきかえること）を繰返し適用する．記号はビット，バイト，英数字などを単位としている．アルゴリズムが簡単で高速処理が可能である．秘密鍵暗号で有名なのは，1977 年米国 NBS により標準暗号として制定された **DES** である．

DESは64［ビット］の平文mをランダム化した64［ビット］の暗号文cに変換する．鍵は64［ビット］（うち8［ビット］はパリティビットであるから正味56［ビット］）で，簡単な方法で16個の48［ビット］の部分鍵$K_1, K_2, \cdots, K_{16}$を作る．まず，2元記号を単位に転字（ビットの順序を入れかえることを通常，転置という）を実行し，次いで64［ビット］の2元情報（平文）を32［ビット］の2つのブロックに分割し，これに対し16段にわたりそれぞれ転字・換字を繰返す．最後に最初の転字の逆転字を行う．ここで，換字処理はSボックスと呼ばれる非線形変換である．そのため，平文とそれに対応する暗号文を入手したとしても鍵を割出すのが困難とされている．このように，暗号化アルゴリズムは完全に公開され，暗号の安全性は鍵に依存している．それゆえ，安全性を示す一つの指標として鍵の長さが問題となる．鍵の総当りによる解読が不可能な計算量的安全を確保するためには，現在少なくとも80［ビット］以上が必要とされている[4]．DESは，鍵の長さ$|K| = 56$［ビット］であり，トリプルDES（DESをさらに3段実行する方式）や新しい型の秘密鍵暗号方式（advanced encryption standard：AES）が検討されている．

秘密鍵暗号方式はアルゴリズムが簡単なため高速処理・小型化が可能で，現在データ暗号化を目的として実用化されているものの大半はこの方式である．しかし，暗号強度を鍵の管理により保持するため鍵の管理が重要である．また，N人で相互に通信するために必要な鍵の数が$\binom{N}{2} = \frac{N(N-1)}{2}$と多いのも欠点の1つである．

17.3 公開鍵暗号系

公開鍵暗号は，**暗号化鍵**K_Eと**復号鍵**K_Dを一対ずつ作り，暗号化鍵を公開，復号鍵を秘密にする暗号方式である．送信者Aは公開リスト（電話帳のようなもの）上の受信者Bの暗号化鍵を用いて暗号文を作成し，受信者Bは自分だけが知っている復号鍵（これは秘密とする）を用いて暗号文を復号し平文を得ることができる．したがって，秘密鍵暗号系のようにあらかじめ鍵を配送共有する必要はない．しかもこのとき，N人で相互に通信するために秘密に管理しなければならない鍵の数はNでよい．しかし，通常整数のべき乗演算と剰余演算を実行しなければならず，計算速度が落ちるという欠点をもっている．そのため，長い平文の暗号化に用いられることは少なく，パスワードや（秘密鍵暗号系の）共通鍵の暗号化に用いられることが多い．

[4]総当り攻撃法以外に差分攻撃法，線形攻撃法などがある．

公開鍵暗号系では暗号化鍵K_Eと復号鍵K_Dが異なり，公開されたK_Eから秘密にするK_Dが容易に求まらない．この仕組みを作るには**一方向性関数**が重要な役割をはたす．関数$f(\cdot)$が一方向性であるということは，順方向$f(\cdot)$の計算は容易（多項式時間で計算可能）であるが，逆方向$f^{-1}(\cdot)$の計算は（多項式時間では）困難であることをいう．例えば，2つの素数p, qが与えられてその積nを求める（$p \cdot q \to n$）のは容易であるが，nを与えて$p \cdot q$に素因数分解する（$n \to p \cdot q$）のは，積を求めるのに比べはるかに困難である．一方向性関数は，平文mから暗号文cを計算することは容易であるが，暗号文cを盗まれても平文mを割出すのは困難であるという暗号化の秘匿機能に活躍するのである．なお，公開鍵暗号方式は情報の秘匿だけでなく，**署名**を実現し情報の認証を可能とする方法としても有効である．

公開鍵暗号系には数多くの方式が提案されているが，次に**素因数分解問題**に基づく**RSA暗号**と**離散対数問題**に基づく**エルガマル**（T. ElGamal）**暗号**を紹介する．

17.3.1 RSA暗号

公開鍵暗号では，暗号解読の難しさは数論の難問を解く難しさに対応している．RSA暗号は，その安全性を大きな整数（例えば，10進数200桁）の**素因数分解問題**を解く困難さに根拠をおいている．すなわち，2つの素数p, qを与えたときその積$pq = n$を計算することは極めて容易であるが，整数nが与えられたとき$n = pq$となる素数p, qを求めるのは困難であるという一方向性を利用しているのである．ただし，素因数分解問題がnの桁数の多項式オーダで解けるやさしい問題かどうかは明らかではないが，現在知られている最良のアルゴリズムを用いても素数pの準指数的オーダ，例えば$O(e^{\sqrt{2 \ln p \ln \ln p}})$程度[5]である．このため，計算機の処理速度の向上と共にRSA暗号で用いる素数の積nの桁数を増さねばならない．次に，RSA暗号のアルゴリズムを示す．

[5]ln は $\log_e$ を示す．

[RSA 暗号のアルゴリズム]

準備

(1) 2つの大きな素数 p,q を選び，RSA 合成数 $n=pq$ を求める．p,q は秘密にしておく．

(2) オイラー関数 $\phi(n)=(p-1)(q-1)$ を計算し[4]

$$\mathrm{GCD}(d,\phi(n))=1 \tag{17.3.1}$$

$$ed=1 \pmod{\phi(n)} \tag{17.3.2}$$

を満たす対 (e,d) を求める．すなわち，$\phi(n)$ と互いに素な整数 d を求め[5]，$\phi(n)$ を法とする演算の下に d の逆数を e とする（これは，ユークリッド互除法を用いて求めることができる）．

(3) ここで

$$\begin{aligned} K_E(\text{暗号化鍵}) &: (e,n) \\ K_D(\text{復号鍵}) &: (d,n) \end{aligned} \tag{17.3.3}$$

とし，K_E を公開し，K_D を秘密に保つ[6]．

暗号化と復号

(1) 送信者 A はメッセージ（平文）m を $0\le m\le n-1$ の整数で表現し，受信者 B の公開鍵 K_E を用いて暗号文 c を

$$\text{暗号化:}\quad c=m^e \pmod{n} \tag{17.3.4}$$

とする．もちろん，暗号文 c は $0\le c\le n-1$ となる整数である．

(2) 受信者 B は自分だけが知っている秘密の鍵 K_D を用いて

$$\text{復　号:}\quad m=c^d \pmod{n} \tag{17.3.5}$$

を計算し，平文 m を得る．

ここで，式 (17.3.5) は，整数 $n=pq$ で割った余りの整数の集合 $\mathcal{Z}_n$ 上で任意の $m\in\mathcal{Z}_n$ に対し $m^{\phi(n)}=1 \pmod{n}$ であるというオイラーの定理を拡張した結果を用いて導かれる．すなわち，式 (17.3.2) を用いて，ある整数を a と

[4] 通常は $p-1$ と $q-1$ の最小公倍数を用いる．

[5] 実際には，$p-1$ と $q-1$ に対し互いに素であれば十分である．

[6] n を公開しているから，結局 d だけを秘密とする．もちろん，p,q は秘密である．

すると

$$c^d=m^{ed}=m^{a\phi(n)+1}=m \pmod{n} \tag{17.3.6}$$

である[7]．

次に，ごく簡単な例を示しておく．

[例 17.3.1] RSA 暗号の例

準備 (1) $p=11$, $q=5$ とする．$n=55$ である．

(2) $\phi(n)=10\times 4=40$ である．$\mathrm{GCD}(d,40)=1$ となる $d=7$ とする．ユークリッド互除法を用いて，$7e=1 \pmod{40}$ を解く．$e=23$ である．

(3) $K_E=(23,55)$, $K_D=(7,55)$ とする．

暗号化と復号 (1) **暗号化**：平文 $0\le m\le n-1=54$ となる $m=8$ とする．$c=m^e=8^{23}=8^{20}\cdot 8^3=17 \pmod{55}$[8]．

(2) **復号**：$m=c^d=17^7=18^2\cdot 17=8 \pmod{55}$[9] となり平文が復元される．□

17.3.2 エルガマル暗号

素因数分解と並んで数学的に効率良いアルゴリズムが知られていない（解き難い）問題として**離散対数問題**がある．エルガマル暗号はこの離散対数問題を解く困難さに安全性の根拠をおいている．

いま，p を素数とする．$p-1$ 以下の正整数 α（正確には $GF(p)$ の原始元[10]）に対し

$$y=\alpha^x \pmod{p} \tag{17.3.7}$$

とするとき，α と x が与えられて y を計算することは容易であるが，α と y が与えられて x を求めるのは困難であるという一方向性をもっている．これを離散対数問題という．例えば，$p=5,\alpha=3$ とすると表 17.3.1 が得られる．素数 p が小さいときは，あらかじめ対数表を作っておけばよいが，p が大きいとき（例えば，10 進数 300 桁）は離散対数表を作ることは事実上不可能である[11]．

[7] 式 (17.3.2) より $ed=a(p-1)(q-1)+1$ と表わせば，フェルマーの小定理 $m^{p-1}=1 \pmod{p}$ を用いてもよい．

[8] $8^{20}=1 \pmod{55}$ を用いた．

[9] $17^3=18 \pmod{55}$ を用いた．

[10] $\mathcal{Z}_p^*=\{1,2,\cdots,p-1\}$ とする．$\alpha\in\mathcal{Z}_p^*$ に対し，$\alpha^\gamma=1 \pmod{p}$ を満たす最小の自然数 γ を α の**位数**という．$\gamma=p-1$ ならば α を**原始元**という．$\mathrm{GCD}(\alpha,p-1)=1$ である．このとき $\mathcal{Z}_p^*$ の任意の元は $\alpha^x\ (0\le x<p-1)$ で表わすことができる．

[11] $\log y=x\log\alpha$ とすると，$\alpha^x>p$ となる x に対して (mod p) の操作により x と y の間には単純な大小関係が成り立たず，とびとびの値（離数値）について対数をとらねばならない．これが離散対数である．

表 17.3.1: 離散対数表

x	$y = 3^x \bmod 5$
1	3
2	4
3	2
4	1
5	3
6	4
7	2
8	1
9	3
10	4
⋮	⋮

次に，離散対数を用いたエルガマル暗号のアルゴリズムを示す．

［エルガマル暗号のアルゴリズム］

準備

(1) 素数 p と原始元 α を選ぶ．

(2) 適当な d を選び $e = \alpha^d \pmod p$ を計算する．

(3) ここで

$$\begin{aligned} K_E(\text{暗号化鍵}) &: (p, \alpha, e) \\ K_D(\text{復号鍵}) &: d \end{aligned} \tag{17.3.8}$$

とし，K_E を公開し，K_D を秘密に保つ（ただし，(p, α) はユーザごとではなくシステム共通に公開してよい）．

暗号化と復号

(1) 送信者 A は $c_1 = \alpha^r \pmod p$ を計算する．ただし，r はランダムに選ばれた数である．さらに送信者 A はメッセージ（平文）m を $1 \le m \le p-1$ となる整数とし，受信者 B の公開鍵 K_E を用いて $c_2 = me^r \pmod p$ を計算する．暗号文 c を

$$\text{暗号化} : c = (c_1, c_2) \tag{17.3.9}$$

とする．

(2) 受信者 B は自分だけが知っている秘密の鍵 K_D を用いて

$$\text{復　号} : m = c_2 / c_1^d \pmod p \tag{17.3.10}$$

と計算し平文 m を得る．

ここで，式 (17.3.10) は

$$\frac{me^r \pmod p}{\alpha^{rd} \pmod p} = \frac{me^r \pmod p}{e^r \pmod p} = m$$

から得られる．エルガマル暗号は c_1, c_2 の 2 項を送る必要があるが，受信側で秘密鍵 d を用いて打ち消される仕組みを用いている．しかも，秘密鍵 d から公開鍵 e ($= \alpha^d \pmod p$) を作っているから，r という秘密鍵暗号における共通鍵を離散対数の形 α^r で暗号化し送信するという大胆な方法をとることができる．したがって，r を共通鍵と考えると秘密鍵暗号方式を用いた公開鍵暗号ということもできる．

次に，ごく簡単な例を示す．

［例 **17.3.2**］ エルガマル暗号の例

準備 (1) $p = 7, \alpha = 5$ とする．

(2) $d = 2$ とし $e = 5^2 = 4 \pmod 7$ とする．

(3) $K_E = (7, 5, 4), K_D = 2$ とする．

暗号化と復号 (1) **暗号化**：乱数 $r = 4$ とすると，$c_1 = 5^4 = 2 \pmod 7$．平文 $m = 5$ とすると，$c_2 = 5 \cdot 4^4 = 6 \pmod 7$．よって暗号文 $c = (2, 6)$ である．

(2) **復号**：$m = \frac{6}{2^2} = \frac{6}{4} = 6 \times 2 = 5 \pmod 7$ となり[12] 平文が復元される． □

なお，エルガマル暗号はディフィー (W. Diffie) とヘルマン (M. E. Hellman) による**鍵配送方式**の変形と考えることができる．また，**楕円曲線暗号**も離散対数形暗号の一種である．

17.4 秘匿と認証

先に暗号の役割は情報の秘匿と認証にあることを述べた．秘匿は情報（暗号文）が盗聴露呈されても鍵がない限り情報の意味（平文）がわからないようにする仕組みで暗号の重要な役割である．しかし，秘匿だけでは改ざん，なりすまし，否認などに対しては不正を防止できない．ここでは，主として公開鍵暗号系を用いた認証方法について述べる．

図 17.0.2 に暗号系における不正行為を示す．**セキュリティアーキテクチャ**では (1) **相手認証**，(2) **アクセス管理**，(3) **秘匿**，(4) **情報の完全性**，(5) **否認防止**が規定され，それぞれに暗号技術が用いられる．

[12] 4 の逆数は $4 \times 2 = 1 \pmod 7$ から 2 であることを用いた．

まず，(1) は通信相手が本当に正当な者であるかを確認することで，正当な通信者以外のなりすましを防止すること，(2) は (1) を行った後，あらかじめ許可された範囲内の資源 (例えばファイル) へのアクセス制御であり，許可なく資源への不正アクセスを防止すること，(3) は盗聴などにより不正に情報が取られることを防止すること，(4) は通信路上での意図的な改ざんや誤りが生じた場合，それらを検出可能なこと，(5) は通信者が，通信に関して行った行為を後になって否認することを防止することである．これらは情報の秘匿の他に，その情報を誰が受信したか，それは正当な送信者であるかを証明する必要があるからである．そのために，**メッセージ認証**，**ユーザ認証**などの機能が必要である．これらは共通鍵暗号系でも実現することができるが，ここでは公開鍵暗号系を用いた**ディジタル署名**の方法を示す．

RSA 暗号を用いたディジタル署名を **RSA 署名**ともいう．署名や押印に相当する機能で，署名文を作ることができるのは**署名鍵** (RSA 暗号の復号鍵) $K_D = (d, n)$ を持っている者のみという公開鍵暗号系の特徴を生かしたものである．ここで，**検証鍵** (RSA 暗号の暗号化鍵) $K_E = (e, n)$ を公開している[13]．仕組みは簡単で平文を RSA 暗号の秘密鍵 K_D で暗号化し，公開鍵 K_E で復号しても元の平文に復元できることを用いる．すなわち，署名文を h，その暗号文を s とすると，署名者は

$$\text{署名：} \quad s = h^d \pmod{n} \tag{17.4.1}$$

とし，平文 m と署名の暗号文 s の対 (m, s) を送る．検証者は (m, s) より

$$\text{検証：} \quad h = s^e \pmod{n} \tag{17.4.2}$$

が成立するか否か検証し，成立すれば署名は正しいものとする[14]．同様に，**エルガマル署名**を作ることもできる (演習問題 [17.5] 参照)．なお，ディジタル署名はメッセージ認証のために用いられるがユーザ認証の機能を兼ね備えている．

[13] したがって，17.3 節の説明の K_E, K_D を用いると B が A に署名文を送ることになる．

[14] 実際には平文 m のハッシュ値を h とする．ハッシュ関数は送受信者両方であらかじめ共有しておく (ハッシュ関数とは衝突を起こしにくい圧縮関数である)．もちろん，平文に直接署名してもよい．

本章のまとめ

1° 暗号解読の安全性は (1) **情報理論的に安全** (無条件に安全)，(2) **計算量的に安全**に分けられる．前者には逐次鍵を変更する鍵の使い捨て法 (バーナム暗号など) がある．

2° 現代暗号には (1) **共通鍵暗号系** (DES など)，(2) **公開鍵暗号系** (RSA 暗号，エルガマル暗号など) がある．

3° 暗号系における不正は (1) **盗聴**，(2) **改ざん**，(3) **なりすまし**，(4) **否認**などがある．暗号技術は (1) に対し秘匿機能として，(2)~(4) に対し認証機能として有効に用いられる．すなわち，暗号の役割は情報の**秘匿**と**認証**である．

4° 暗号系に要求される主な条件は (1) 暗号化・復号の処理が高速に実行できること，(2) 盗聴者 (復号鍵をもたない不正者) が解読するのは困難であることである．

5° 情報理論的には鍵の数 $\|\mathscr{K}\|$ が大きい程，平文の冗長性が小さい程，また暗号文の長さが短い程解読されにくい．

6° 秘密鍵暗号方式はアルゴリズムが簡単で高速処理が可能であるが，公開鍵暗号方式は計算量が大きい．しかし，後者は管理しなければならない鍵の数は少なく，またディジタル署名が実現しやすい．

7° 公開鍵暗号の特徴は暗号化鍵を公開し復号鍵を秘密に保つ．その仕組みは**一方向性関数**にある．安全性は**素因数分解問題** (RSA 暗号)，**離散対数問題** (エルガマル暗号) など数論の難問を解く難しさに根拠をおいている．

演 習 問 題

[17.1] 片仮名 (50 文字あるとする) の文に対しシーザー暗号を用いる．シーザー暗号はブロック長 N に対し $\|\mathscr{M}\|$ 個の文字から成る文字列を各々 τ_i 文字 ($0 \le \tau_i \le \|\mathscr{M}\| - 1$, $i = 1, 2, \cdots, N$) ずらす暗号化法である．例えば，片仮名では $\tau_i = 2$ のときアはウにイはエにそれぞれ換字される．このとき，日本文のもつ冗長度を 70%，$N = 10$ としたとき，一義長 L_1 を求めよ．

[17.2] DES の暗号文を総当り攻撃法で解読しようとする．計算機の性能を，

(1) 1000 万分の 1 秒で 1 個の鍵をチェックできるとすれば，解読に要する時間はいくらか．

(2) これを 1000 台用いるとどうか．

(3) 3 重 DES を用いるとどうか．

(4) 鍵の長さを 80 [ビット] とし，1000 台用いるとすればどうか．

[17.3] RSA 暗号で $p = 7$, $q = 11$ とする．$d = 13$ とするとき

(1) e の値はいくらか．

(2) $m = 15$ のとき c を求めよ．

(3) c から d を用いて m に復元せよ．

[17.4] エルガマル暗号で $p = 37, \alpha = 17$, $d = 13$ とする．

(1) e の値はいくらか.
(2) $m = 15$ のとき, c を求めよ.
(3) c から d を用いて m を復元せよ.

[**17.5**] エルガマル暗号を用いたディジタル署名（エルガマル署名）の構成法を示せ.

VI まとめ

18 情報理論の体系とまとめ

本書では (I) 情報量の定義 (第 1,2 章), (II) 情報源符号化 (第 3〜8 章), (III) 通信路符号化 (第 9〜13 章), (IV) 誤り訂正符号 [符号理論] (第 14〜16 章), (V) 暗号と情報セキュリティ [暗号理論] (第 17 章), について述べた. 上記 (I)〜(III) は情報理論の主題である. (IV), (V) は基本的には情報理論に含まれるが, 情報理論とは若干異なる道具（有限体, 数論など）を用いるため, 別の体系として扱われることも多い. 本書では, 情報理論と密接に関連した部分の要点を述べた.

以上で, (I)〜(V) の個々の問題に関する話は終る. 最後の本章では情報理論が扱う枠組の中で, これらの相互関係と全体の体系を述べる. 通常は, まず全体の体系を示し, 次いで個々の問題に分解してゆくスタイルをとることが多いが, 敢えて 5 つの部分を独立に扱い, ここでそのまとめを行うことにした. その結果, 5 部構成のそれぞれをほぼ他の部を参照しないで読むことができるはずである.

18.1 情報理論の体系と数学的モデル

まず, (I) **情報量の定義**は後のすべての議論の出発点である. 情報のもつべき性質を公理として挙げ, その下で情報を測るために導いた簡潔で重要な結果である. これに疑問があれば, この後のすべての議論は全く意味をなさない.

(II) **情報源符号化**を考えるときの系のモデルが図 5.0.1 である. 同様に (III) **通信路符号化** ((IV) **誤り訂正符号**も全く同じ), (V) **暗号化**の系のモデルがそれぞれ図 11.0.1, 図 17.0.1 である. 個々の問題はこれで良いが, システムとしてこれらをつなぎ合わせるとどうなるのであろうか. 図 18.1.1 にそのモデルを示す.

ここで, 次のことは注意すべきことである.

(1) **情報源符号器は情報源の構造・性質（統計的モデル）をにらんで最適な符号化（情報圧縮）を行う.**