



Title	現代暗号の数理
Author(s)	田中, 嘉浩; Tanaka, Yoshihiro
Description	暗号技術 (cryptography) は現代では、大量データの送受等本格的用途に使われる共通鍵暗号と、Diffie and Hellman (1976) に依る非対称鍵暗号を実用化した公開鍵暗号に大別される。前者は従来の暗号の延長ともいえ、近年迄永らく解読されなかったDES に引き続いて NIST が暗号を募集していたが、2000年に Rijndael が新たに連邦政府の正式暗号として採用された他、デジタル放送や携帯電話で使われる暗号も前者に属する。後者は「素因数分解の計算複雑度」に基いた Rivest, Shamir, and Adleman に依るRSA が電子商取引 (EC) に爆発的に利用されて以来、電子商取引や電子署名、来たる電子政府の実現等の社会基盤になっている。本稿では暗号の歴史や現状を調べ、後者の公開鍵暗号の内、特にRSA については、その原理、復号化の計算複雑度についてやや詳しく述べ、楕円曲線上の有理点のなす群上では離散対数問題が指数時間アルゴリズムしか知られていないので鍵長を大幅に短縮できる楕円 ElGamal 暗号等やその他の暗号の原理を述べた。これら社会基盤となる公開鍵暗号が数論や代数幾何学等の数学に基いていることは、最近実用化されつつある「絶対に解読できない」量子暗号や、原理的には素因数分解を多項式時間で解く量子コ 前田 周一
Citation	経済学研究, 54(3), 87-98
Issue Date	2004-12-09
Doc URL	<a href="https://hdl.handle.net/2115/5270">https://hdl.handle.net/2115/5270</a>
Type	departmental bulletin paper
File Information	ES_v54(3)_05.pdf



# 現代暗号の数理

田 中 嘉 浩

## 1. 序

暗号<sup>1)</sup>の歴史は古く、少なくとも前5世紀のスパルタには既に太さを揃えた棒に紙を巻き付けて通信文を書きその紙を送受する、転置式の暗号<sup>2)</sup>が使われていたらしい。今でも知られているのが、G.-J. Caesar 自身の手による「ガリア戦記」(52 B.C.) に記されている Caesar 暗号で、その時はローマ字をギリシャ文字に書き換えたもの[22]だったが、後に以前から有り彼自身も使った単アルファベット換字式でも同じ言語で元の文(平文)を数文字ずつずらして(シフトして)暗号文を作る暗号を指す様になっている。例えば、

Alea jacta est  
(賽は投げられた)

はカエサル・シフト暗号(シフト値3)では、

DOHD MDFWD HVW

となる。しかしながら当時ですら暗号が軍事目的に使われたのは象徴的である。

単アルファベット換字式暗号は単なるシフトでなければ非常に多くの場合の数になり、暗号化・復号化の容易さからコード(単語の置き換

え)の技術を交えたノーメンクラター(Nomenclator)が千数百年の間用いられていた。[22]にはノーメンクラターが劇的に用いられ解読・利用された例として、Mary Stuart 元スコットランド女王と反乱を企んだカトリック教徒の A. Babington との暗号の送受が挙げられており、密かに入手され改竄・おとり捜査されて彼等が捕えられ処刑される経緯が臨場感高く書かれている。

単アルファベット換字式暗号は言語学的分析、特に頻度分析で、アルファベットが、

ETAONRISHDLFCMUGPYWBVKXJQZ

の順に E は 13%, T は 10.5%, A は 8.1%, O は 7.9%, … という対応を取ることにより簡単に解読されることが多く、より解読されにくい暗号の必要性がルネッサンス以降に増してきた。

16世紀にフランスの外交官だった Blaise de Vigenere は「鍵」を使って鍵の分だけ順次シフトを繰り返していく Vigenere 暗号を作成した。例えば「鍵」を white にすると、

Vigenere

は Vigenere 暗号では、

RPOXRAYM

となる。注意すべきことは平文の1文字から変換される文字はキー長の数だけの可能性があり、逆に暗号文のアルファベットの1文字に対応す

1) 情報を秘匿する方法は暗号技術(cryptography)、電子透かしの様な情報隠蔽(steganography)に大別されるが本稿では前者を扱う。  
2) ペロポネソス戦争(431 B.C.~404 B.C.)で使われていたとの記述が有る。

る平文の文字はキー長の数だけの可能性がありしかもその対応は一意的でないので、頻度分析では破れない、ということである。実際、Vigenere 暗号は 19 世紀中頃に電子計算機の祖のイギリスの C. Babbage とプロシアの F. Kasiski による解読法が考案される迄約 300 年の間解読不能の暗号とされてきた。

更に 20 世紀初頭に AT&T の G. Vernam や陸軍少佐の J. Mauborgne は平文の文字数分の鍵（乱数等を使う）を使って暗号化する Vernam 暗号を考案・改良した。

「Vernam 暗号は鍵が分らなければ解読不能である」

ことが、情報理論の生みの親の C. Shannon [19] によって証明されている。しかしながら、考えてみると、

「(同じ鍵を使うならば) 多数回使っている間に解読できる」

ことも分る。それは多くの平文を暗号化する間に平均を取ると鍵が浮き彫りになってくるからである。よって Vernam 暗号はワンタイムパッドと呼ばれる「一回限りの暗号」に使えば特別に機密を要する文書の暗号化に用いることが出来るが「鍵をどうやって渡すのか？」という問題は残る。ところが最新の技術による、W. K. Heisenberg の不確定性原理 (Uncertainty Principle), つまり、

$$\Delta x \cdot \Delta p \sim \hbar$$

という不確定性関係を利用して光子の振動方向に「0」, 「1」の値を与える量子暗号では盗聴を検知する方法でその共通鍵を送ることが出来るので、Vernam 暗号が再び見直されているのは興味深い。

ところで再び暗号発展の経緯に戻ると、Vigenere 暗号の解読以降は、特に軍事目的に機械式暗号が考案されてきており、例えば戦時

ドイツのエニグマとか日本の紫は有名である。

エニグマは機械式暗号であり、プラグボード・3枚のスクランブラー・レフレクターの3つの構成要素からなっていて、スクランブラーは5枚（海軍は8枚）から3枚が指定順に選ばれることや1枚毎に向きが決めること、1字毎にスクランブラーが回転すること等の特徴が有り、リフレクターで反射しているのでエニグマ本体が有り初期状態（月毎に渡されるコードブックの初期配置で暗号化されたメッセージ鍵を用いる）が分りさえすれば、暗号文を初期状態を合せて打ち込めば平文を得るとい著しい特徴がある。1字毎に換字が変わる換字法とも言えるが、計算可能の概念を生み出した A. Turing のブレッチレーでのエニグマ解読、更に複雑性を増した海軍のエニグマは映画にもなった U ボート撃沈でのコードブック奪取等のドラマが有り、暗号解読が戦況を大きく左右した例である。同じくウルトラと言われた日本の紫暗号（パープル）も機械式暗号であるが、既に 1940 年 9 月に解読されていたと見られている。

1952 年に NSA (National Security Agency; 国家安全保障局) が暗黙裡に設立され、犯罪防止目的で通信傍受やスパイ活動の役割を果たしてきたが、暗号解読も業務の一担となっている。

戦後の現代暗号は軍事目的ばかりでなく政府使用や情報通信時代の商取引等を目的に作られてきた。NBS (National Bureau of Standard; アメリカ商務省標準局) は暗号を募集していたが、IBM の暗号を改良して 1977 年に採用されたものが DES (Data Encryption Standard) と言われるものであり、仕様を公開されているものの約 20 年間も解読されなかったものとして価値が有る。

DES の解読に合せて NIST (National Institute of Standards and Technology; アメリカ商務省標準技術協会) は暗号を募集していたが、長年の審査過程の後にベルギーの J. Daemen と V. Rijmen によって応募された Rijndael を 2000 年に採用されたものが AES

(Advanced Encryption Standard) という新たな標準暗号として連邦政府に正式採用されている。

1976年にW. Diffie and M. Hellmanによって今迄の「共通鍵」(対称鍵)と違って、鍵Aで暗号化したものは鍵Bでなければ復号化できず、鍵Bで暗号化したものは鍵Aでなければ復号化できない「公開鍵」(非対称鍵)の考え方が発表された。その翌年の1977年に当事MITの所属だったR. Rivest, A. Shamir, L. Adleman<sup>3)</sup>等が「素因数分解の計算複雑度」を利用したRSA暗号による公開鍵暗号を発見し、それは電子商取引を中心に爆発的に利用され、現在迄用いられ続けている。1982年にT. ElGamalがW. Diffie and M. Hellmanの考えた「離散対数問題の計算複雑度」を用いるElGamal暗号と言われる公開鍵暗号を実用化している。

一方、1985年にN. KoblitzとV. Millerが同時期に楕円曲線上で離散対数問題を作れること、それをを用いてより鍵長が短くできる楕円曲線暗号を作れることを発見した。

最近ではP.W. Shor [20]によって量子コンピュータが実現すれば公開鍵暗号が高速に破られることが示され、現代物理学、特に量子力学を応用した量子計算への期待や不安が高まってきている。又Vernam暗号の所で出てきたが、1984年にC.H. BennetとG. BrassardによってBB84と呼ばれる盗聴を防ぐ量子暗号も考案されているが、実験的には可能になってきている。

本稿では暗号の現状を概観し、電子社会や電子商取引の基盤になる公開鍵暗号の中心をなすRSAと楕円暗号を概観しながら、最近の話題や考察を加えていきたい。

## 2. 暗号の現状

計算機や情報通信の発展に伴って平和利用を

考えられ始めた意味でも、換字式でない意味でも、1970年代後半から出現してきた暗号法を現代暗号と定義していいであろう。

現代暗号は共通鍵暗号と公開鍵暗号に大別できる。

共通鍵暗号はブロック暗号とストリーム暗号が有る。

ブロック暗号はDESに代表される様に、平文を固定長(DESでは64ビット)毎に処理する。DESでは64ビットを上位32ビットと下位32ビットを鍵<sup>4)</sup>で攪拌しながらビット処理のXOR(排他的論理和 $\oplus$ ; 2回加算すると元に戻る)で下位を上位に上位を下位に加算する処理をしていく。それは何段になっていても同じ装置で処理方向を逆にすることで復号できる大きな特徴を持つ。

DESは1989年のE. Biham, A. Shamirによって考案された強力な差分読法<sup>5)</sup>ですら他の暗号と違って解読されなかったが、1993年に三菱電機の松井 充が発見した線形解読法によって遂に解読されることになった。

1990年代後半にはコンピュータの高速化によって鍵の全数探索すら可能になってきており、RSA Security社主催で「DES Challenge」と呼ばれる解読コンテストも何回も開かれることとなった。

この間、RC5と呼ばれる鍵長が可変な暗号や、日本でもBS-CS放送で使われるMULTI2や、次世代携帯電話で使われるKASUMI(MISTYの改良版)等のブロック暗号が考案されている。

米国政府は一時的に新たな政府暗号として80ビットの鍵を持つSKIPJACKと呼ばれる暗号を処理するClipper Chipの使用を義務付けるClipper構想が有ったが、NSA作成の暗号

3) 彼等はRSA暗号の発明で2002年ACM Turing賞を授与されている。

4) 鍵長が56ビットになった経緯やNSAとの確執については[13]に詳しい。

5) 平文 $X$ と平文 $Y$ に対して $X \oplus Y$ をその差分という。

に対する不安感と鍵預託 (Key escrow<sup>6)</sup>) を義務付ける制度に対する反発から実施に到らなかったことは興味深い。

AESの募集に際してNISTは1997年に、共通鍵ブロック暗号、可変な鍵長等4つの満たすべき要件と、安全性、コスト、単純性等の評価基準、ロイヤリティ・フリーの取扱いを公開した。2000年にAESに正式採用されたRijndaelはブロック長128ビット、鍵長は128, 192<sup>7)</sup>, 256ビットの選択可能な、8ビット空間の代数体上の演算 (byte 演算) で定義された簡明な暗号である。

アメリカのAESのみならず、欧州ではNESSIE (New European Schemes for Signatures, Integrity, and Encryption) プロジェクトが結成され、64ビット暗号にMISTY、128ビット暗号にCamellia、他にAESと合わせて標準暗号として定められており、日本でも情報処理推進機構 (IPA) と通信・放送機構 (TAO) が共同設置したCRYPTREC (CRYPTography Research & Evaluation Committee; 暗号技術評価委員会 (今井秀樹 (東京大学) 委員長)) が、2002年にそれらを含む29件の暗号を電子政府推奨暗号リストとして公開し、評価基準・試験基準の作成や調査・検討を続行している。

ストリーム暗号は高速に任意長の平文を暗号化するが、RC4やSEALとかが知られているものの発展途上の暗号法である。

公開鍵暗号はW. Diffie and M. Hellmanによる非対称鍵暗号の考え方を実現したもので、素因数分解の計算複雑度を用いたRSAと楕円曲線上の離散対数問題の計算複雑度を用いた楕円ElGamal法が主流になってきている。

RSAのRC4バージョン<sup>8)</sup>はTCPプロトコ

ル上で暗号処理し当初はNetscapeブラウザに組み込まれたSSL (Secure Sockets Layer) という規格で実用化され[13]、電子商取引等で爆発的に使われる様になった。SSLではX.509証明書をCAの秘密鍵で暗号化したものが、例えばアマゾンや書店等のサーバから利用者へ送られて利用者がCAの公開鍵で復号して署名を検証する手続きを最初に行う。その後、X.509証明書に記されたサーバの公開鍵を用いて利用者側のデータを暗号化し、サーバ側はそれをサーバの秘密鍵で復号化して暗号通信ができる。

上で出てきたCA (Certificate Authority; 認証機関) は電子商店が偽者でないことを保証するものであり、VeriSign等が有名だが、国内では後述の電子署名法に規定されており、電子政府に向けてCA同士の認証等の問題を考えられつつある。

一般に速度の面で公開鍵暗号は短い平文に共通鍵暗号は長い平文に適している。しかしながら、RSA暗号で共通鍵データ等短い平文を送る時に大部分はパディングと呼ばれる無意味なデータになるが、それを狙う攻撃法が知られている。そこでパディングに変化を付けて、最も強力な攻撃法の適応的選択文攻撃にも安全なRSA-OAEPが開発され、後述のPKCS#1に新たに盛り込まれている。

公開鍵暗号標準はRSA Security社によってPKCS (Public-Key Cryptography Standards) という標準化 (表1) がなされている。PKCSはインターネット関連の標準化IETF (RFC2459等) に取り入れられている。より一般的にはIEEE (IEEE P1363等)、ISO、ANSIでそれぞれの観点からの標準化がなされている。

6) アメリカ国内ではG. Orwellの「1984」に描かれたBig Brotherによる管理社会と対比され強く批判された。

7) 192ビット鍵長のAESをアメリカ政府は極秘 (TOP SECRET) 文書の伝送に使うと決定した。

8) NetscapeのSSLは当初はアメリカ国内では128ビット、輸出用では40ビットの鍵を使われていたが、1995年8月に解読され、最近では輸出用も128ビット対応になった。Internet Explorerにも組み込まれている。

表 1 公開鍵暗号標準（# 2 と # 4 は # 1 に含まれた）

PKCS # 1 :	RSA Cryptography Standard
PKCS # 3 :	Diffie-Hellman Key Agreement Standard
PKCS # 5 :	Password-Based Cryptography Standard
PKCS # 6 :	Extended-Certificate Syntax Standard
PKCS # 7 :	Cryptographic Message Syntax Standard
PKCS # 8 :	Private-Key Information Syntax Standard
PKCS # 9 :	Selected Attribute Types
PKCS # 10 :	Certification Request Syntax Standard
PKCS # 11 :	Cryptographic Token Interface Standard
PKCS # 12 :	Personal Information Exchange Syntax Standard
PKCS # 13 :	Elliptic Curve Cryptography Standard
PKCS # 15 :	Cryptography Token Information Format Standard

電子商取引（EC）の発展には公開鍵暗号の存在が必要不可欠だったと言える。実際、VISA International と Mastercard International が共同開発し、Microsoft、Netscape Communications、IBM 等と共同で標準化された SET（Secure Electric Transaction）という規格では、暗号化やデジタル署名に RSA（や DES）が使われている。SET では電子商店への発注関連情報とクレジット会社等の金融機関への決済関連情報が分離されており、電子商店でさえクレジットカード番号を知ることができない、等の大きな特徴が有る。

電子商取引に関しては国内では 2000 年 4 月に環境整備、標準制定、政府への提言目的に、電子商取引推進委員会（ECOM）が発足した。国内では、2003 年の事業者間（BtoB）及び事業者・消費者間（BtoC）取引はそれぞれ 77 兆 4,320 億円（前年比 67.2% 増加）、4 兆 4,200 億円（前年比 64.8% 増加）と大きな伸びを続けている重要分野である。

デジタル署名は SSL でも出てきたが、電子署名の一種で公開鍵暗号を使う時に言うが、ここでも公開鍵暗号が実生活に役立っている。電子署名は電子商取引の例では、電子商店側の秘密鍵で暗号化したものを公開鍵で復号して検証するので、客が発注データを公開鍵で暗号化して電子商店側が秘密鍵で復号するのと鍵の用い

られ方が逆であり、公開鍵暗号がそれを可能にすることに注意しよう。アメリカでは RSA の特許の問題が有り、DSA が標準の署名方式になっている。国内でも 2001 年 4 月から「電子署名及び認証業務に関する法律」（電子署名法）が施行され法的基盤は整備されてきている。

UNIX のパスワードは DES を複数回使ってハッシュ化する crypt によって /etc/passwd に暗号化されて収まっているが、そもそも telnet 等の通信プログラムが暗号化されていないのでは余り意味がない。まして途中の送信内容も勿論盗聴される訳に行かない。その目的には ssh と呼ばれる、公開鍵暗号で共通鍵を渡し認証しながら共通鍵暗号に切り替える通信プログラムが開発されている。

電子メールも暗号用途には、PGP<sup>9)</sup> や S/MIME と呼ばれる規格が浸透しつつある。

電子政府は e-Japan 戦略で国民の利便性の向上や行政運営の簡素化、効率化、信頼性及び速度の透明性の向上を目指して構築を宣言されたものであり、KWAN、LGWAN の構築化や住民基本台帳ネットワークの稼動に伴い、2003

9) 開発者の P. Zimmerman は 1993 年に武器輸出の観点で当局から警告されている。輸出問題、NSA との確執の面から興味深い。

年度から 2005 年度末の 3 年計画で計画されているものである。ここでも電子署名が非常に重要であるが、公開鍵暗号が大きな役割を果たしており、欧米の PKI (Public Key Infrastructure) を基に、GPKI や LGPKI 等の基盤が作られつつある。

### 3. RSA について

#### 3.1 RSA の原理

電子商取引や電子政府の基盤をなす公開鍵暗号の代表格である RSA 暗号系の原理を述べる。RSA 暗号は素因数分解問題の計算複雑度が桁数 (または  $\log n$ ) の多項式時間のアルゴリズムが知られていないことを応用して作られた暗号である。

#### 公開鍵の求め方

2 つの大きな素数  $p$  と  $q$  を乱数等を用いてランダムに選んで、その積  $N = pq$  を求める。一方、 $e \leq (p-1)(q-1) = \phi(N)$  ( $\phi(\cdot)$  は Euler の  $\phi$  関数) 且つ  $\gcd(e, (p-1)(q-1)) = 1$  を満たす  $e$  を求める。 $(e, N)$  が公開鍵である。

#### 秘密鍵の求め方

$\text{mod } \phi(N)$  に於ける  $e$  の逆元、即ち、

$$ed \equiv 1, \text{ mod } (p-1)(q-1) \quad (1)$$

を満たす整数  $d$  を求める。 $d$  が秘密鍵となる。

#### 暗号化と復号化

平文  $m$  を暗号化するには、次のようにする。

$$C = m^e, \text{ mod } N \quad (2)$$

暗号文  $C$  を復号化するには、次のようにする。

$$C = m^d, \text{ mod } N \quad (3)$$

つまり、Alice<sup>10)</sup> が Bob に平文  $m$  を送る時に、Bob から公開された公開鍵  $(e, N)$  を用いて上記の様に暗号化して暗号文  $C$  を送信し、Bob は持っている秘密鍵  $d$  で上記の様に復号化し

て平文  $m$  を得る。

尚、電子署名では逆に暗号化を  $C = m^d, \text{ mod } N$ 、復号化を  $C = m^e, \text{ mod } N$  で定める。

RSA 暗号は次の単純な定理に基づいている。

**定理 1 Euler (18 世紀)**  $\gcd(a, n) = 1$  ならば、

$$a^{\phi(n)} \equiv 1, \text{ mod } n \quad (4)$$

が成立する。

[証明]  $r = \phi(n)$  とし、 $b_1, \dots, b_r$  をどの 2 つも  $\text{mod } n$  で合同でない  $\gcd(b_i, n) = 1, i = 1, \dots, r$  なる整数とする。この時、 $\gcd(a, n) = 1$  であるから、 $\gcd(ab_i, n) = 1, i = 1, \dots, r$  となる。従って集合  $\{b_1, \dots, b_r\}$  と集合  $\{ab_1, \dots, ab_r\}$  は  $\text{mod } n$  で等しい。よって、

$$a^r \prod_{i=1}^r b_i \equiv \prod_{i=1}^r ab_i \equiv \prod_{i=1}^r b_i, \text{ mod } n$$

であるから、

$$(a^r - 1) \prod_{i=1}^r b_i \equiv 0, \text{ mod } n$$

よって

$$a^r \equiv 1, \text{ mod } n$$

Euler の定理から、

$C^d = m^{ed} = m^{1, \text{ mod } \phi(N)} = m, \text{ mod } N$  (電子署名では、 $C^e = m^{de} = m, \text{ mod } N$ ) となる。

Euler の定理は  $n = p$  (素数) の時を考える  $\phi(p) = p-1$  となるので、17 世紀に発表された Fermat の小定理の一般化になっていることに注意しよう。この様な単純な定理が現代暗号のかなりの割合を占める RSA 暗号系の基盤となっており、大量のマナーが動く電子商取引がその上に成り立っていることは驚くべきことである。

#### 3.2 復号化の計算複雑度

公開鍵  $(e, N)$  から秘密キー  $d$  を求めるため

10) [16] で Bob と共に出てくる。更なる参加者を Carol, Dave 等とし、他に特定の役割の Eve (傍受, 盗聴), Mallory (改変, 妨害), ... 等が暗号分野で良く用いられる。

には、 $N$  を素因数分解して  $p$  と  $q$  を求める必要がある。

素因数分解問題の計算複雑度を考えると，“yes”は素数の割り算で，“no”は素数判定の多項式時間アルゴリズム（例えば後述の AKS アルゴリズム）が有るので、

「素因数分解問題  $\in$  NP  $\cap$  co-NP」

と言える。実際には素因数分解問題にも離散対数問題にも準指数時間のアルゴリズムが知られている。しかしながら、P.W. Shor [21] は量子コンピュータでは原理的には素因数分解問題や離散対数問題を多項式時間で解けることを示しており、NP 完全問題を利用する欠陥の無い暗号系が中々作成されにくいことと併せて興味深い。

RSA では実際には  $p$  や  $q$  は数百 bit になるように決めるので、現在の RSA の解読は 10 年程度は少なくとも現実的な時間内には実行不可能である [5]。

### 素数の多項式時間判定

RSA と直接の関係はないが、2002 年 8 月にインド工科大学計算機科学工学部の M. Agrawal 教授と N. Kayal, N. Saxena によって “PRIMES in P” という素数判定アルゴリズムが発表された [2]。

彼等はまず、

「 $\gcd(a, n) = 1$  ならば、

$$(x-a)^n \equiv (x^n-a), \text{ mod } n$$

になる」

と Fermat の小定理を多項式環に拡張した。

ところがこのままでは  $(x-a)^n$  の評価に計算時間が掛かり過ぎる。そこで  $r$  を  $a$  と互いに素、且つ  $n$  に比べて十分小さな整数とし、

$$(x-a)^n \equiv (x^n-a), \text{ mod } (x^r-1, n) \quad (5)$$

ならば、 $n$  は素数だが、 $a$  を変えながら成立すれば逆も成立することを利用して作られたアルゴリズムである。

### 定理 2 Agrawal-Kayal-Saxena (2002)

$n \in \mathbb{N}$ ,  $s \leq n$  を仮定する。素数  $q, r$  を

(i)  $q \mid r-1$ ,  $n^{(r-1)/q} \not\equiv 0.1 \pmod{r}$ , 及び

$$(ii) \binom{q+s-1}{s} \geq n^{2\lfloor \sqrt{n} \rfloor}$$

(iii)  $n$  が  $s$  より小さい約数 ( $> 1$ ) を持たない。

(iv)  $(x-a)^n \equiv (x^n-a), \text{ mod } (x^n-1, n)$

が成立する様に選ばれていると仮定する。その時、 $n$  は素数である。 ■

更に (ii) の条件を満たす為には、

$$q > s \geq 2\lfloor \sqrt{r} \rfloor \log n$$

より進んで、

$$o_r(n) > 4 \log^2 n$$

但し、 $o_r(n) = n, \text{ mod } r$  の位数を満たす最小の  $r$ ,  $\gcd(r, n) = 1$  となることが分っている。

### AKS アルゴリズム

入力： 整数  $n > 1$

1.  $n = a^b$  ( $a, b > 1$ ) ならば  $n$  は合成数として終了。
2.  $o_r(n) > 4 \log^2 n$  を満たす最小の  $r$  を求める。
3. 或る  $a \leq r$  に対して  $a$  が  $n$  の約数になれば  $n$  は合成数として終了。
4.  $n \leq r$  ならば、 $n$  は素数として終了。
5.  $a = 1, \dots, \lfloor 2\sqrt{\phi(r)} \log n \rfloor$  に対して、

$$(x+a)^n \not\equiv x^n+a, \text{ mod } (x^r-1, n)$$

ならば合成数として終了。

$\phi(\cdot)$  は Euler の  $\phi$  関数。

6. 上述のどれでもなければ  $n$  は素数。

AKS アルゴリズムの計算時間は、Sophie Germain 素数に対する或る仮定の下で  $O(\log^{6+\epsilon} n)$ , そうでなくとも現在では  $O(\log^{7+\epsilon} n)$  となることが示されている。よって、

## 「素数判定問題 ∈ P」

であることが分る。但し未だ実用的でなく、実際は  $\text{co-RP}$  の高速な Miller-Rabin 判定法等を判定に用いるが、理論的意味は大きい。勿論、合成数判定も P に属する（というより最初から分っている）が、実際に素因数を求める素因数分解問題はずっと難しい。

## 4. 楕円暗号やその他の暗号

## 4.1 楕円曲線

$\mathbb{C}$  上に  $\omega_1, \omega_2 \in \mathbb{C}, \omega_1, \omega_2 \neq 0$  を取り、

$$L = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$$

と置くと  $\mathbb{C}/L$  はコンパクトリーマン面になる。 $L$  を周期とする Weierstrass の関数は、

$$\wp(z; L) = \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}$$

と定義されるが、

$$\wp'(z; L)^2 = 4\wp(z; L)^3 - 60a_4\wp(z; L) - 140a_6,$$

$$a_4, a_6 \in \mathbb{C}$$

となるので周期  $L$  を持つ任意の二重周期関数は  $\wp(z; L)$  と  $\wp'(z; L)$  の有理関数として書け、それは楕円関数になる。

楕円曲線  $E$  は特異点のない曲線であり、標準形は次の形になる。

$$y^2 = x^3 + ax + b \quad (6)$$

$$\text{但し, } 4a^3 + 27b^2 \neq 0$$

楕円曲線は種数 1 の曲線であり、次の定理が成立する。

**定理 3 (Siegel (1929))** 種数 1 以上の代数曲線は、有限個の整数点しか持たない。 ■

$\mathbb{Q}$  上（即ち係数、変数は有理数）の楕円曲線ならば次の定理が成立する。

**定理 4 (谷山-志村予想(1955); Wiles の定理(1994))**

$\mathbb{Q}$  上の楕円関数はすべてモジュラー関数である。 ■

定理 4 は G. Frey 等に Fermat 予想への帰着性を示され、A.J. Wiles によって 1995 年 2 月に Fermat の大定理、即ち、

$$x^n + y^n = z^n, \quad n \geq 0,$$

を満たす  $x, y, z \in \mathbb{N}$  は存在しない、の肯定的解決の中心柱になった重要な結果である。

$E(\mathbb{Q})$  の群構造を次の様に定める。 $P_1$  と  $P_2$  を通る直線と楕円曲線  $E$  との  $P_1$  と  $P_2$  以外の交点を  $x$ -軸について反転してできる点を  $P_1 + P_2$  で定める。更に  $E(\mathbb{Q})$  の群構造の単位元（零元） $O$  は無限遠点である。

**定理 5 (Mordell-Weil (1922))** 楕円曲線の有理点のなす  $E(\mathbb{Q})$  は有限生成アーベル群である。 ■

これは  $E(\mathbb{Q}) \cong \mathbb{Z}^r \times (\text{有理解})$  と表現できることを示しており、階数  $r$  は楕円曲線から定義されるゼータ関数  $\zeta_E(s) = 1$  の  $s = 1$  での零点の位数と等しいと予想されている (Birch-Swinnerton-Dyer 予想)。

有限体  $GF(p)$  上（即ち等号は  $\text{mod } p$  で考える）で楕円曲線を考える。

ところで、 $x, y \in GF(p)$  の有理点（整数点）に  $O$  を加えた集合を  $E(F_p)$  で表す。 $E(F_p)$  の位数  $\# E(F_p)$  は次の定理で与えられる。

**定理 6** 楕円曲線上の  $E(F_p)$  の位数  $\# E(F_p)$  は、

$$p+1-2\sqrt{p} \leq \# E(F_p) \leq p+1+2\sqrt{p} \quad (7)$$

の範囲にある。 ■

**例 1.**  $GF(19)$  上の楕円曲線

$$y^2 = x^3 + 2x + 1, \quad \text{mod } 19$$

を考える。

$E(F_{19})$  は上式を満たすものは、

$\{(0,1), (0,18), (1,2), (1,17), (4,4), (4,15), (6,1), (6,18), (7,4), (7,15), (8,4), (8,15), (9,8), (9,11), (11,9), (11,10), (12,9), (12,10),$

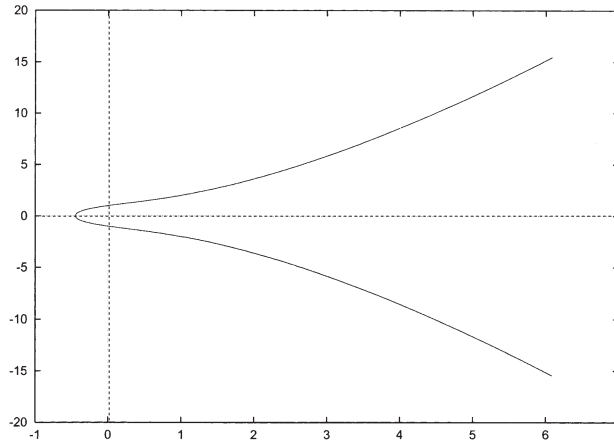


図1 楕円曲線  $y^2 = x^3 + 2x + 1$

(13,1), (13,18), (15,9), (15,10), (16,5), (16,14), (18,6), (18,13) となる。この26個に、無限遠点  $O$  を加えたものが  $E(F_{19})$  になるので、位数は  $\# E(F_{19}) = 27$  である。

$GF(p)$  上の楕円加算を次の様に定める。

$O$  以外の2点  $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$  に対して、 $x_1 = x_2, y_1 + y_2 = 0 \pmod p$  ならば  $P_1 + P_2 = O$  である (即ち直線上の3点の和は  $O$  である)。

さもなければ、

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, \pmod p & P_1 \neq P_2 \\ (3x_1^2 + a)(2y_1)^{-1}, \pmod p & P_1 = P_2 \end{cases} \quad (8)$$

$$x_3 = \lambda^2 - x_1 - x_2, \pmod p$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \pmod p$$

により、 $P_1 + P_2 = (x_3, y_3)$  である。

**例2.** 例1の  $E$  で、 $P=(4,4)$  として有限巡回群を計算すると、

$\{P=(4,4), 2P=(18,13), 3P=(1,2), 4P=(6,1), 5P=(16,14), 6P=(15,9), 7P=(9,11), 8P=(11,9), 9P=(8,4), 10P=(7,15), 11P=(13,1), 12P=(0,1), 13P=(12,9), 14P=(12,10), 15P=(0,18), 16P=(13,18), 17P=(7,4), 18P=(8,15), 19P=(11,10), 20P=(9,8), 21P=(15,10), 22P=(16,5), 23P=(6,18), 24P=(1,17), 25P=(18,6), 26P=(4,15), 27P=O\}$

である。(0,1) の離散対数は12等と考える。

#### 4.2 楕円 ElGamal 暗号

離散対数問題を利用した ElGamal 暗号は楕円曲線上の有理点のなす群を利用して問題の計算複雑度を上げれる。

##### 公開鍵, 秘密鍵の求め方

大きな素数  $p, GF(p)$  上の楕円曲線  $E(F_p)$  生成元として  $P_g \in E(F_p)$  を選び、その位数を  $q$  として  $x \in Z_q$  を任意に選び、

$$P_y = xP_g \quad (9)$$

を計算する。

$P_K = (E(F_p), P_g, P_y)$  が公開鍵であり、 $S_K = x$  が秘密鍵である。

##### 暗号化と復号化

送信者 Alice は、 $r \in Z_q$  を任意に選び、平文  $m$  に対して、

$$m + r(P_y) \quad (10)$$

で暗号化し、同時に  $rP_g$  も求める。

受信者 Bob は,

$$m + r(P_y) - x(rP_y) = m \quad (11)$$

によって復号化する。

基本的には有限体上の離散対数問題は指数計算法 (index-calculus method) で準指数時間<sup>11)</sup>になることが知られているが、楕円曲線上の有理点のなす群上では指数時間アルゴリズムしか考案されていないので、鍵長を大幅に小さくできる (元の ElGamal 暗号の  $p$  が 1024 ビットだが、楕円 ElGamal 暗号の  $p$  は 160 ビット程度) 所に大きな特徴がある。

#### 4.3 超楕円曲線と暗号

有限体  $F$  上の種数  $g$  の超楕円曲線  $C(g \geq 1)$  の標準形は次の形になる。

$$y^2 + h(x)y = f(x)$$

但し、 $h(x) \in F[x]$  は高々  $g$  次の多項式、 $f(x) \in F[x]$  は  $2g+1$  次のモニック多項式であり、 $C$  と偏微分して得られる  $2y + h(x) = 0$  と  $h'(x)y - f'(x) = 0$  を同時に満たす  $(x, y) \in \overline{F} \times \overline{F}$  (特異点) は無いものとする。

超楕円曲線  $C$  は種数  $g \geq 2$  の時に、次の定理が成立する。

**定理 7 (Mordell 予想(1922); Faltings の定理(1983))** 種数 2 以上の代数曲線は、有限個の有理点しか持たない。 ■

定理 7 は種数 2 以上の場合に関しては Siegel の有限性定理 (定理 3) の一般化になっているが、証明は予想の 60 年後になされたことに注意しよう。

11) 一般に  $c > 0$ ,  $0 < t < 1$  により、 $O(\exp(c(\log n)^t(\log \log n)^{1-t}))$  となる計算複雑度を  $(\log n)$  の準指数時間という。因みに  $t = 1$  では指数時間、 $t = 0$  では多項式時間になる。

超楕円曲線のヤコビ多様体は 2 点で表せそれらは群を為し、この群に属する  $P+Q$  も 2 点になる。有限体上でも同様に定義でき、それらが群を為すことから、離散対数問題等を考えられている。

超楕円曲線はより鍵長を少なく攻撃法のない方向性の為に模索されてきている。

#### 5. 今後の方向性

現代暗号の殆どが数学に少なからぬ関係を持ち、「意味の有る期間内に解読できない」という計算量的安全性に支えられているが、Vernam 暗号で出てきた様に「絶対に解読できない」という情報理論的安全性の方向も時には重要であり、現代物理学に基いた量子暗号がそれを可能にしてきていることは興味深い。2004 年 7 月には富士通と東京大学生産研が 100km の光ファイバーの距離で 100kbps の量子暗号通信を可能にする技術を開発したとの発表があった。

現代物理学、特に量子力学の応用であるが、量子コンピュータでは状態を、

$$|i_1, \dots, i_n\rangle, i_1, \dots, i_n = 0, 1$$

を用いて、

$$\phi = |x\rangle = \sum_{i_1, \dots, i_n = 0}^1 x_{i_1, \dots, i_n} |i_1, \dots, i_n\rangle \quad (12)$$

と量子  $n$  ビットで記述することができ、ユニタリ変換によって量子並列性を生かし  $2^n$  ステップの計算を 1 ステップで実行でき、結果を観測できる様に設計できる。Shor [21] の素因数分解アルゴリズムでは  $\gcd(a, N) = 1$  なるランダムな  $a$  に対して、

$$a^r \equiv 1, \pmod{N}$$

となる位数  $r$  を求める部分を量子コンピュータを用いれば多項式時間で実現できるので、その他の多項式時間の部分と併せて多項式時間計算可能であることが示されている。量子コンピュータは実験的には実現され始めており、デバイス

の実現に伴って、現在の鍵長の暗号は鍵長を増やす必要があり、長期的には別の原理による暗号の必要性も出てくるであろう。

盗聴を前提にして個々のプログラムで情報を暗号化することはそれ自体重要である。しかしながら、量子暗号の様に盗聴自体を防ぐ方向も非常に重要であろう。最近はサイドチャンネル攻撃と言われる電力解析を用いる攻撃法も出てきている。OECD のセキュリティガイドラインに示されている様に情報システムが C.I.A. (Confidentiality, Integrity, Availability) を満たす様に設計されるべきであり、最高の暗号が使われたとしても個々のセキュリティの甘さで結果をそのまま持って行かれたり、ハード的に簡単に解読される様では無意味である。

電子政府の実現は公開鍵暗号に変えられていても個々の WAN のセキュリティ向上が十分なされる必要があり、更には利用者個人のモラル向上も新技術と共に進められていくべきであろう。2004 年からは u-Japan 構想が公開されているが、来たるべきユビキタス (ubiquitous; 遍在) 時代を迎えて暗号の重要性は増す一方であり、人間と技術の有り方も問われている。

#### 参考文献

- [1] J.W.S. Cassels, *Lectures on elliptic curves*, Cambridge Univ. Press (1991), (徳永訳, 『楕円曲線入門』, 岩波書店, 1996).
- [2] F. Bornemann, "PRIMES is in P : A breakthrough for "Everyman"", *Notices of the AMS* 50 (2003), 545-552.
- [3] W. Diffe and M.H. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory* IT-22 (1976), 644-654.
- [4] L.K. Grover, "Quantum mechanics helps in searching for needle in a haystack", *Physical Review Letters* 79 (1997), 325-328.
- [5] 今井 浩, 「量子計算は暗号技術を破壊するか?」, *科学* 74 (2004), 226-230.
- [6] 情報処理振興事業協会, 通信・放送機構著, *CRYPTREC Report 2001*, (2002).
- [7] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation* 48 (1987), 203-209.
- [8] ———, *Algebraic Aspects of Cryptography*, Springer, Berlin, 1998, (林訳, 『暗号の代数理論』, シュプリンガー・フェアラーク東京, 1999).
- [9] M. Kraitchik, *Théorie des nombres, I*, Gauthier-Villars, Paris, 1922.
- [10] 黒川利明, 「暗号技術の現状と展望」, *科学* 74 (2004), 216-221.
- [11] 黒澤 馨, 尾形わかほか共著, 電子情報通信学会編, 『現代暗号の基礎数理』, コロナ社, 2004.
- [12] S. Landau (評者), "RSA and Public-Key Cryptography by R. Mollin; Introduction to Cryptography by H. Delfs and H. Knebl; Cryptography: Theory and Practice by D. Stinton; Algebraic Aspects of Cryptography, N. Koblitz; Elliptic Curves: Number Theory and Cryptography by L. Washington; Elliptic Curves in Cryptography by I. Blake, G. Seroussi, and N. Smart; Modern Cryptography, Probabilistic Proofs, and Pseudorandomness by O. Goldreich; Foundations of Cryptography: Basic Tools by O. Goldreich; The Design of Rijndael: AES – the Advanced Encryption Standard by J. Daemen and V. Rijmen; Handbook of Applied Cryptography by A. Menezes, P. van Oorschot, and S. Vanstone",
- [13] S. Levy, *Crypto : How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*, Viking Pr., 2001, (齊藤訳, 『暗号化』, 紀伊国屋書店, 2002).
- [14] 大山永昭, 「電子政府の現状と課題」, *情報処理* 44 (2003), 455-460.
- [15] R. Ribenboim, *The Little Book of Big Press*, Springer, 1991, (吾郷訳編, 『素数の世界 – その

- 探索と発達』, 共立出版, 1995).
- [16] R.L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and publickey cryptosystems”, *Communications of the ACM* 21 (1978), 120-126.
- [17] S. Robinson, “Still guarding secrets after years of attacks, RSA earns accolades for its founders”, *SIAM News* 36(5) (2003).
- [18] B. Schneier, *Applied Cryptography, 2nd Ed., Protocols, Algorithms, and Source Code in C*, Wiley, 1996, (山形訳, 『暗号技術大全』, ソフトバンク, 2003).
- [19] C. Shannon, “Communication theory of secrecy systems”, *Bell System Technical Journal* 28 (1949), 656-716.
- [20] P.W. Shor, “Algorithms for quantum computation: Discrete logarithms for factoring”, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, (1994), 124-134.
- [21] P.W. Shor, “Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM Journal on Computing* 26 (1997), 1484-1509.
- [22] S. Singh, *The Code Book : The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, 2001, (青木訳, 『暗号解説: ロゼッタストーンから量子暗号まで』, 新潮社, 2001).
- [23] 辻井重男, 岡本栄司共著, 『暗号のすべて—ユビキタス社会の暗号技術』, 電波新聞社 (2002).
- [24] Hal R. Varian, *Intermediate Microeconomics — A Modern Approach, 6th ed.*, Norton, 2002.