暗号について

大阪大学基礎工学部情報工学科　藤原　融

1. はじめに

近年、計算機、通信の発達に伴って、大量の個人情報などが計算機のファイルにおかれるようになってきた。また、銀行のオンライン化などにより、通信回線上を重要なデータが流れることも多い。そのため、暗号を用いてそれらの情報の保護を行なう研究がなされている。さらに、1976年に公開鍵暗号〔4〕という興味深い新概念が発表されて以来、暗号の研究は非常に盛んになった。本稿では、古典的な暗号と公開鍵暗号を紹介し、最後にACOS、UNIX*で提供されている暗号について述べる。

ところで、現在、多くのシステムでは、ファイルや通信回線上のデータの暗号化はあまり行なわれておらず、主としてアクセスコントロールにより情報の保護が行なわれているようである。アクセスコントロールとは、特定の許された利用者以外はその情報をアクセスできないようにする手法である。ACOSも含めて通常の計算機システムでは、パスワードを知らない限り、ログインできないようになっているが、これは、パスワードを知っている使用者だけにアクセスを許す一種のアクセスコントロールである。また、ACOSでは、ファイル(カタログ）単位でアクセスコントロールが可能であり、ACCESSサブシステムなどを用いて、ファイル（カタログ）に読み出し許可、書き込み許可、実行許可等を与えることも可能である。

しかし、アクセスコントロールでは、

(1) ディスク装置を盗み出せば、そのディスク上のファイルが読める。

(2) システムの管理者は、通常、システム内のすべてのファイルを読み書きできる。

(3) 通信回線などは一般には盗聴可能であり、そのようなものまでアクセスコントロールにより保護するのは実際上不可能である。

などという問題がある。

一方、ファイルを暗号化しておけは、(1)、(2)が、また、通信回線上を流れるデータを暗号化すれば、(3)も、基本的には防げる。

2. 古典的な暗号

この章では、古くから知られている有名な暗号のうちのいくつかを紹介する。ここで紹介するものも含めて、文献〔1、2〕に多くの古典的暗号が紹介されている。

2.1 換字暗号

まずは、暗号文

---

* UNIXは米国AT&Tが開発したオペレーティングシステムである。

Brx pdb xvh d Frpsxwhu lq wkh Frpsxwdwlrq Fhqwhu ri Fvdnd Xqlyhuvlwb. (1)

を解読してください。実は、

You may use a computer in the Computation Center of Osaka University. (2)

という文(このような暗号化する元の文を平文とよぶ)において、文字aをdに、bをeに、...、wをzに、...、zをcにというように、文字をアルファベット順に3文字づつずらすことによって、上の暗号文ができあがる。

この例のように、平文の各文字をアルファベット順に何文字かづつずらすことにより暗号文を得る暗号化法は、シーザー暗号と呼ばれる。また、これをさらに一般化した暗号、すなわち、平文の各文字を別の記号で置き換える暗号を総称して、換字暗号という。

有名なポーの小説"黄金虫"やドイルの"踊る人形"などにも換字暗号が登場する。また、映画"2001年宇宙の旅"(クラーク原作)に登場するコンピュータの名前HALは、IBMを1文字づつずらしたものであるといわれている。

尚、一般に、暗号化法において、例えば、換字暗号における

"平文の各文字を別の文字で置き換える"

というような変換の規則を、暗号アルゴリズムと呼び、

"3文字ずらす"

のように暗号化(平文から暗号文を作成すること)、復号(暗号文をもとの平文に戻すこと)のために必要な秘密の情報のことを鍵と呼ぶ、もちろん、暗号化法によっては、暗号アルゴリズムと鍵の区別が明白ではないこともあるが、通常この2つは区別されることが多い。

2.2 転置暗号

転置暗号は平文の各文字の順序を入れ換えるものである。例えば、平文中の各単語において、文字を逆順に並べかえることにより、先ほどの平文(2)から、

Uoy yam esu a retupmoc ni eht Noitatupmoc Retnec fo Akaso Ytisrevinu. (3)

という暗号文が得られる。このような簡単な転置の方法では容易に解読されるが、各種の複雑な転置法が知られている。例えば、転置の順序を指定するのにグリルを用いたもの〔1〕があり、井沢元彦の小説"猿丸幻視行"などにも登場する。

2.3 古典的暗号の解読

暗号の解読とは、暗号文から平文を復元することであるが、暗号化に用いた鍵を知らずに復元

するという点で、正当な受信者が行なう通常の復号とは異なる。

シーザー暗号では、26通りの鍵（ずらし方）をすべて調べれば、元の平文が得られる。

一般の換字式暗号については、シーザー暗号のように鍵の総当たり法では解読できない。鍵（換字）の種類は、使われる文字の集合（簡単のため、平文に使われ得る文字の集合と暗号文に現われ得る文字の集合は同一とし、その集合）の要素の数をnとすれば、n！通りある。従って、鍵を総当たりすることはnが26程度でも実際上不可能である。1ナノ秒（10億分の1秒）に1個の鍵を調べても（もちろんこんなことは不可能）、すべての鍵を調べるのには100億年以上かかる。

しかし、ポーの"黄金虫"にもあるように、換字暗号は平文の統計的性質（例えば、英語では文字eが最も多く出現することなど）を用いて解読される。解読法の詳細については、例えば、文献〔2〕を参照されたい。

ところで、暗号文を解読するには、与えられた暗号文が換字暗号により作られたものかどうかという問題もある。通常、暗号解読の問題では、より強い意味での安全性を考えるため、暗号アルゴリズムは既知という前提で議論され、その条件の下で解読される暗号はよくないとされる。ただし、暗号文が換字暗号で作られたかどうかについては、暗号文中の文字の出現頻度から大体の見当がつくことが多い。すなわち、暗号文中の各文字の出現率と、通常の文の各文字の出現率（元の平文がどの自然言語で書かれているかわかっているとする）に相関があれば、換字暗号の可能性が高いことがわかる。

また、転置暗号についても、与えられた暗号文が転置暗号を用いたものかどうかの判定は、換字暗号と同様に行えるし、その解読もそれほど困難ではない〔2〕。

3. 現代の暗号

この章では、近年用いられている暗号を紹介する。

3.1 慣用の暗号

前章で述べたように、古典的な簡単な暗号では容易に解読されてしまう。そこで、換字、転置など従来から知られている方法を複雑に組み合わせて解読の難しい暗号が作られている。その代表格として、DES暗号がある。

DESは、Data Encryption Standardの略で、米国商務省により標準の暗号化法として測定されたものである。商務省が暗号化法を公募し、IBMから提案されたものをもとにしている。暗号化の方法はかなり複雑なのでここでは省略する。詳細は文献〔2、3〕などに述べられている。

3.2 公開鍵暗号

これまでに述べた暗号ではいずれも暗号化、復号において、同一の鍵を用いてきた。ファイルの暗号化を行なう場合などで、暗号化と復号を一人で行なう場合はこれでもよい。しかし、暗号通信を行なう場合には、通信を行なう当事者間であらかじめ、鍵を共有するために何らかの方法が必要である。しかし、例えば、信頼できる使者が運ぶなどの方法では、多くの人と暗号通信したい場合をはじめとして、実用的でないことが多く、鍵配送の問題は難しい問題である。また、多くの相手と通信する場合、鍵を共有できたとしても、相手ごとに異なる多くの鍵をすべて秘密に保管しておかなければならない。このような問題の解決策として、公開鍵暗号とよばれる概念がW. DiffieとM. E. Hellmanにより1976年に提案された〔5〕。

公開鍵暗号では、

暗号化に用いる鍵と復号に用いる鍵は同一のものを使う必要がないのでは？

という発想に基づいている。すなわち、公開鍵鍵暗号は、

（性質）暗号化と復号で異なる鍵を用い、暗号化鍵を知っても、復号鍵を計算することはできない。

という性質を持つ暗号である。

公開鍵暗号を用いて、例えば、太郎から花子への秘密通信は、以下のように行なう。

(1) 花子は、暗号化鍵と復号鍵を作る。

(2) 暗号化鍵を太郎に送る。このとき、上の性質から暗号化鍵は誰に知られてもよいので、盗聴される恐れのある通信路を用いてもよい。

(3) 太郎は、送られてきた暗号化鍵を用いて、送りたい情報を暗号化し、花子に送る。

このように、この方式では、暗号化鍵は他人に知られてもよい（公開してもよい）ことから公開鍵暗号とよばれている。公開鍵暗号の概念を提案した論文〔5〕には、具体的な暗号化方法は示されなかった。最初に提案された具体的な方法は、R. Rivest, A. Shamir, L. Adlemanによるもので、1978年に提案され〔6〕、3人の頭文字をとって、RSA暗号と呼ばれている。以下で、RSA暗号を簡単に説明する。ここでは、平文は整数で表わされるとする。

平文（整数）Mと暗号化鍵（整数の対）e，nに対して、暗号文（整数）は、

$$M^e \mod n$$

で与えられる。また、暗号文cに対して、復号鍵dを用いて、

$$C^d \mod n$$

を求めることにより、元の平文が得られる。ここで、公開の暗号化鍵e，nと秘密の復号鍵dは以下のようにして作られる。

(1) 大きな2つの素数（例えば、それぞれ10進数150桁）pとqを選び、$n = pq$とする。

(2) $\phi = (p-1)(q-1)$を計算し、ϕと互いに素な正数dを、$d < \phi$を満たすように定める。

(3) $e \equiv d^{-1} \mod \phi$ を満たすようにeを選ぶ。

d，及びn（＝pq）から公開鍵eを作り得るのにもかかわらず、eとnからdを求めることが困難（実際上不可能）であるのは、nだけからでは素因数p，qを実際上計算できないことに基づいている。すなわち、大きな数（例えば、nは10進150桁）を実用的な時間で素因数分解できるようなアルゴリズムが（存在しないとは限らないが、少なくとも）一般には知られていない。ここ数年、RSA法の提案がきっかけとなって、素因数分解の研究も進展したが〔3、4〕、まだ、（実用的な素数のサイズの）RSA法が破られるほどには進展していない。

また、暗号文 $M^e \mod n$（eとnは既知）から、平文Mを求める問題も数学的に非常に難しい問題である。

3.3 公開鍵法の応用

(A) ディジタル署名

重要な通信では、次のような問題がある。

(1) 受け取ったメッセージが誰から送られてきたかわかるか？

メッセージに送信者の名前が書いてあったとしても、本当にその人が送ったとは限らず、第3者がその名前を使ったのかも知れない。通常の手紙等では、署名したり、捺印したりすることで、この問題はない。

(2) メッセージが契約書などの場合、送信者が実際に送ったにもかかわらず、後になってそのようなメッセージを送ったことがないと主張したとき、受信者は、送信者が嘘をついていることを証明できるか？

通常の契約書等では、この問題も署名、捺印で解決している。

手書きの署名や印影を（イメージスキャナ等で）電気信号に変換して、送ったとしても、これらの問題を解決できない。電気通信では、メッセージの切り貼りが容易であり、署名部分の情報だけを抽出しておき、後で別の通報にそれを付けることで署名を偽造できる。

この問題は、公開鍵暗号を用いれば、基本的には、以下のようにして解決できる。

(1) 送信者は、自分の復号用の秘密鍵を用いて、送りたい通報を（暗号文とみたてて）復号しそれを送る。

(2) 受信者は、公開された鍵で暗号化し、意味のあるメッセージが得られれば、正当な通報として受け取る。

このようにすれば、送信された情報は、送信者の秘密の鍵に基づいて作られているので、他人には偽造できない。また、秘密の鍵と対になる暗号化鍵が公開されているので、送信者は後になって、送信事実を否定できない。

ただし、公開された鍵は、印鑑登録のように、信頼できる機関に登録しておかなければならない。また、これは印鑑登録でも問題になるが登録をしようとする人が本人（または本人に依頼されて来た人）であるかどうかをどのように確認するかが重要である。

(B) その他の応用

通信回線を通じて、ポーカーゲームを行なったり、コイン投げ（コインを投げて表が出るか裏が出るかを当てるゲーム）を行なう方法、また、投票システムなどがたくさん提案されている。

4. 計算機で提供されている暗号

この章では、ACOS、およびUNIXで利用できる暗号について紹介する。

4.1 ACOSの暗号

ACOSシステムでは、ファイルの暗号化、復号のために、TSSコマンド

CODE, DECODE

が提供されている〔7〕。

CODEは、利用者から与えられた暗号化鍵（英字、数字、特殊文字の任意の組合せからなる1～11文字の文字列）を用いて、ファイルを暗号化する。

一方、DECODEは、CODEにより暗号化されたファイルを復号する。このとき、利用者は、CODEを実行するとき用いたのと同一の鍵を用いなければならない。

以上のことから、暗号アルゴリズムとして慣用のアルゴリズムを用いていることはわかるが、アルゴリズムの詳細については、筆者の知る限り公表されていない。

4.2 UNIXの暗号

UNIXでは、暗号化、復号のコマンドcryptoが提供されている。暗号アルゴリズムは、第2次世界大戦中、ドイツ軍などで使われたエニグマ暗号を用いている。ドイツ軍のエニグマ暗号はイギリスによって、解読されたが〔1〕、UNIXで用いているものは、ドイツ軍のものより、鍵の種類が非常に多い〔8〕。

また、UNIXでは、パスワードファイル（パスワードを登録しておくファイル）も暗号化されている。パスワードファイルの暗号化は通常のファイルの暗号化と少し異なる。

まず、利用者が登録したパスワードは暗号化されてパスワードファイルに入れておく。利用者がログインしたとき、利用者の入力したパスワードを暗号化し、パスワードファイル中の暗号化されたパスワードと比較して一致すればログインを許可する。

従って、暗号化されたパスワードの復号を行なう必要がないので、いわゆる一方向関数を用い

ることができる。詳細は文献〔2〕を参照されたい。

参考文献

1. 一松　信：暗号の数理，講談社ブルーバックス，B－421，1980．
2. D．E．Denning：Cryptography and Data Security，Addison－Wesley，1982．
3. 嵩　忠雄，藤原　融："暗号アルゴリズムと計算量の理論"，情報処理（情報セキュリティ特集号）Vol．25，，№6，1984．
4. 土井則久，小山謙二編：コンピュータセキュリティ，共立出版，1986．
5. W．Diffie and M．E．Hellman；"New Directions in Cryptography，" IEEE Trans，on IT，Vol．IT－22，№6，pp，397－427，1976．
6. R．Rivest，A．Shamir and L．Adleman；"A Method for Obtainng Digital Signatures and Public－Key Cryptosystems"，Comm．ACM Vol．21，№2，pp．120－126，1978．
7. 日本電気：ACOS TSS－AFシステム説明書，FEE 22－3．
8. Computer Science Division UCB：UNIX Programmer's Manual（4.2BSD），1983．