数値解析シンポジウム NAS 2001-05-23 での招待講演

情報社会を生きぬくための暗号技術

駒澤大学 経営学部　西村 和夫
検索キーワード：　ビー玉計算機

1. 暗号の定義

暗号とは，略式には“○○しないで □□する”技術の総称である．もっと厳密には：

暗号　特定の計算の実行が，特定の知識が利用できる場合には効率よく行え，利用できない場合には極めて困難であるように制御する情報処理技術の総称．特定の者だけに通信文の内容を伝える守秘機能や，通信文の作成または変更を行ったのが特定の者であるか否かを確認する認証機能などの，さまざまな情報セキュリティ機能を提供する（電子情報通信用語辞典）．

用語　内容を秘匿する通信の場合，発信者は（平文(ひらぶん)の）通信文を暗号化し，暗号文を作って送る．受信者は，暗号文を復号して元の通信文を得る．

暗号解読　暗号解読（攻撃）には，困難な順に少なくとも次の 3 段階がある．

(1)　暗号文だけによる攻撃 …… 攻撃する側はこれしかできないことがある．
(2)　既知の平文による攻撃 …… 攻撃される側はここまでは耐える設計をすべき．
(3)　任意の平文による攻撃

実際の暗号の応用はきわめて微妙であり，解読に成功してもその事実は隠そうとする．したがって，効果的な解読方法が発見されても，学会には発表されない可能性がある．

2. 公開鍵暗号系の概念

公開鍵暗号系は，暗号化と復号とで異なる鍵を用いる暗号系である（図１）．e を公開鍵と呼び第三者に知られてもかまわない．一方，d は秘密鍵と呼び，受信者だけが秘密に保持する．したがって，e と d の組は受信者が作成するか，信頼できる機関が作成する必要がある．

3. RSA 方式の概要

公開鍵暗号系を実現する方式の一つである RSA 方式は，非常に大きな 2 素数の積 n の因数分解が極めて困難なことを利用している．1977 年に MIT の Rivest, Shamir, Adleman の 3 人が考案した．

暗号化：　$C = M^e \mod n$
復号：　$M = C^d \mod n$

このとき暗号文の値は $C^d = (M^e)^d = M^{ed}$ であり，フェルマーの小定理によって $C^d \equiv M$ (modulo n) となる．

4. 認証

公開鍵方式の暗号化の関数と復号の関数とを逆に用いても通信文が元に戻るなら，通信

文の発信者を保証することができる．RSA 方式での認証は次のとおりである．

暗号化：　$S = M^d \mod n$ …… 署名文 S の作成
復号：　$M = S^e \mod n$

5. 暗号技術を使ってできること

(1) プライバシーの保護　通信内容を第三者に対して秘匿する．
(2) 認証　受信者に発信者の証明をする．
(3) 署名　第三者に発信者の証明をする．
(4) 個人識別　登録された本人であることを確認する．
(5) 同時交換　署名などを同時に交換する．

暗号プロトコルの例

(1) カードなしポーカー
(2) コイントス
(3) 電子投票
(4) 電子メールの受領証
(5) 秘密分散
(6) 電子現金

6. 量子暗号

基本的なアイデアは，Wiesner が 1970 年に考案した．しかし，掲載されたのは 1983 年であった. 具体的なシステムは, Bennett と Brassard が 1984 年に発表した（通称 BB84）.

量子コンピュータ　光量子 1 個ずつをデータ表現と演算に用いるコンピュータであり，演算速度が現在のコンピュータの 1 万倍以上になると予想されている．量子コンピュータの出現によって，RSA 方式は安全ではなくなったといわれている．

解読不可能な暗号　情報理論的に解読不可能な暗号方式がいくつかある．通信文と同じ長さのランダムな鍵を用いた多表式暗号は，暗号文だけによる攻撃では解読不可能である．Vernam 暗号（1917 年）は，通信文のビット列と同じ長さの乱数鍵ビット列との排他的論理和をとる共通鍵暗号方式であり，解読不可能である．（Vernam 暗号は，たった 2 行の表を用いた多表式暗号ともいえる.）

量子暗号　光量子による通信を行うと，不確定性原理によって，盗聴を確実に検出することができる．盗聴しようとする行為が外乱を与え，通信内容が乱れて（改ざんされて）しまうからである．

BB84 方式は，Vernam 暗号に基づいている．光量子による通信によって，送受信者の双方に乱数ビット列が秘密のうちに共有できる．この乱数ビット列を用いて解読不可能な暗号による通信ができる．

ただし，現在の技術では，光量子を 1 個だけで通信することができないので，まだ完全に解読不能とはいえない.