とっても明るい「暗い」話

伊藤　洋

（工学部コンピュータメディア工学科教授／総合情報処理センター長）

「暗号」の話をしよう。暗号などと聞くと、とたんに暗い気分になる。夜陰にまみれて小舟で日本海に上陸した不審な黒い服の一団。これを海上保安庁の巡視船が拿捕してみたら男達のポケットの中から小さな「乱数表」が見つかった、などというニュースが冷戦時代にはしばしばあった。某国のスパイが侵入したらしいというのである。こういうとき「乱数表」は、「暗号」＝「スパイ」の代名詞みたいなものであった。そして、一見平和そうに見える日常生活の場も、実は国際的謀略が渦巻く暗黒の世界なのだと実感させられたりして、暗い気分になる。

映画「2001年宇宙の旅」に登場するコンピュータの名前はHAL。これをアルファベットで1文字ずらすとHはIに、AはBに、LはMになる。ここには有名なコンピュータメーカーの名前が隠されていたのだという。「Jbnbcpz」という暗号文は、「僕は男の子だ」という平文の暗号文に他ならない。このように、文字をいくつかずらすというような単純なやり方で暗号文を作っていた時代があった。あの最強のローマ皇帝ジュリアス・シーザーの時代だ。だからこういう暗号の作り方を「シーザー暗号」または「秘密鍵暗号」などという。こういうやり方では、アルファベットは26文字しかないから総当たりでしらみつぶしに調べれば簡単に暗号は解読されてしまう。現代ではコンピュータがあるからあっという間に解読されてしまうだろう。先の「乱数表」は、規則性の全く無い数で、何文字かの文章の組をずらすので簡単には解読されないが、それでも乱数表を沿岸警備隊に応酬されたのではもうおしまいだ。送られてくる暗号文はすべて解読されてしまう。

このような暗号の作り方・解読の仕方のことを総じて「暗号アルゴリズム」といい、暗号文を平文にもどす操作のことを「鍵」という。鍵を奪われるともはや暗号ではなくなる。だから、暗号の取り扱いは大変難しいのである。

インターネットの時代に暗号の必要性が叫ばれている。しかし、秘密鍵である暗号鍵を使うようなやり方では、鍵のやりとりに困ってしまう。いつ盗まれてしまうか分からない。だいいち一度誰かとの間で使った鍵を他の人と使うことになると盗まれなくても知れ渡ってしまう。それでは暗号の役には立たない。インターネットの時代には、必ずしもよく知っている信用できる人との間だけで通信するばかりではない。不特定多数のアカの他人、ネットワークの中で偶然遭った人とコミュニケーションを始めることなど枚挙にいとまが

無い。

そこで考え出されたのが公開鍵暗号だ。どうせ盗まれてしまうなら公開してしまおうというのである。暗号解読の鍵を公開して暗号になるのかと思われるだろうが、本当に公開するのだ。何なら名刺に刷ってもいい。もちろん鍵を全部見せてしまっては暗号にならないのは当然である。そこで、鍵を二つ作る。一つは公開用の鍵で誰にでも知らせておく。もう一つは恋人にも神様にも教えない秘密の鍵。二つの鍵の間には一対一の関係があるがその関係を見つけるにはスーパーコンピュータでしらみつぶしに調べてさえ1万年とか1億年とかかかるようにしておく。この原理は数学の素因数分解の知識があれば容易に分かるが、ここでは紙幅が無いので解説しない。

さて、いま私が、君にメールを送る場合を想定してみよう。先ず私は、君の公開鍵を使って私が書いたメール文（平文）を暗号化してネットワークに投げ込む。この暗号文はもはや私にも解読できない。君の公開鍵でひとたび暗号化してしまうと書いた本人の私にも解読できないのだ。これを解読できるのは、君が持っているあの秘密鍵だけである。だから安心して君は私のメールの中身を受け取ることができる。

これで、公開鍵によって不特定多数の誰とでも安心して通信ができそうだ。しかし、疑い出せばきりがない。君は、本当にこのメールが私からのものかどうか確信は持てないはずだ。誰かが嘘を言っているかもしれない。これを「なりすまし」という。（げんに、本学のサーバーから学生のパスワードを盗み出して、その学生になりすまして、アメリカの大学でいかがわしい行為をしていた者がいた。ログ記録からアメリカの学生らしいのだが、それもなりすましかもしれないのでその先は不明という事件が本学でもあった。被害のあったアメリカの大学から指摘されて陳謝したことがある。学生諸君はパスワード管理をしっかりして欲しい。）

それはともかく、こういう疑いが出ないように、先のメールには私が私の秘密鍵を使って署名しておいた。君はメールを受け取ったときメールの本文は君の秘密鍵で解読し、私の署名は私の公開鍵を使って開くと間違いなく私の名前や住所が出てくる。これで差出人が私であることが確認できる。こうしてなりすましは撲滅できそうだ。だが待てよ、この公開鍵そのものが嘘だったらどうなるか。そういう疑い深い人の為に、権威ある認証機関を構築しておく。私も君もその認証機関に公開鍵を預けるのだ。

さて、この権威ある認証機関も公開鍵を公開しておく。私は、君にメールを出すときに君の公開鍵をこの認証機関に尋ねることにする。すると認証機関は、私の公開鍵をも調べて君の公開鍵の番号を、私の公開鍵で暗号化して、しかも認証機関自身の秘密鍵で暗号化した機関自身の署名を添付して教えて呉れる。こうして教えられた君の公開鍵で、私は上の手順でメールを発送することにします。君は、私の暗号メールを受け取ったら直ちに認証機関に私がやったのと同じように私の公開鍵の番号を教えてもらって、これで私の署名を確認してください。これで万事大丈夫です。

いやいや、その権威ある認証機関とやらがなりすましだったらどうなるかって。それじ

ゃ、宮沢賢治の『注文の多い料理店』みたいなもので、そこまで疑っちゃどうにもならないよ。

どうだろう。これなら暗号のもつ暗さは無くなるではないか。鍵を公開するという明るさと、秘密鍵を持ち運ばないのだから盗まれることもない安全性。

公開鍵暗号方式は、人類1500年の暗号の歴史の中でも、あっと驚く発想の転換であった。インターネットの普及、そしてとどまるところを知らない情報化の進展。そういう時代の中で明るい暗号を使って、安全で確実な情報の受発信がなされようとしているのだ。

しかし、ここで言いたいのは明るいばかりではない。情報化時代に生きるということは、ただ情報化の便利さを享受するというのではなくて、「自律・分散・協調」という三つのキーワードを実行することだ。自分のことは自分でしろ、自分の安全は必ず自分で確保せよ、ということだ。ただなんとなく自分の身の回りの人々の中に群れて生きるのではなく、世界をまたにかけて分散して生きる力を持てという事も、このキーワードには入っている。そして第三に、世界の人々と協調して生きよ、ということも追加されているのだ。

いまや、君の膝の上のノートパソコンがそのまま世界につながっている。そこにはありとある知識や生きた世界の今が映し出せるのだ。しかもネットワークの進展は、日進月歩の速さで続いている。そしてその中には有害な情報や悪も入り込んでくる。人間社会の持つ矛盾もまたこの中にはたっぷりと入っている。それでいて、その中に、いささかでも人類の役に立つ何かができる可能性もそれこそ無数に用意されている。

インターネットは、ネットワークの帯域の広さ／狭さや回線品質などその基盤の地域間格差は如何ともし難く存在するものの、ネットワークの性格は人類の他に例を見ない民主的な構造と機能とを有している。

しかも、我が山梨大学の学内ネットワークＹＩＮＳは、他大学に比べて圧倒的に完備しているはずである。ここから、学習や研究はもちろんのこと、世界の今に棹差していく自由を十分に利用しない手はない。暗い暗号が、明るいそれになったように、受験時代の勉強の発想をきれいさっぱり転換して、ＹＩＮＳを駆使して学園生活を豊かなものにしない手はないのだ。