暗号について　情報リテラシー　C-28 塚本翔

・暗号とは

まず、暗号とは「当事者以外には意味がわからないように、当事者間でのみ理解できるように取り決めた、特殊な記号や文字、またはその手順や方式」のことである。

また、送信者が送りたい元の文章を「平文」、暗号文に変換する作業のことを「暗号化」、 受信者が暗号文を元の文章に戻すことを「復号（化）」と言い、暗号化や復号を行うための手順を「アルゴリズム」、暗号化に用いるパラメーターのことを「鍵またはキー」と呼ぶ。

図をいれる。

「暗号」と言うと「機密性」のみが重視されがちだが、「特定の相手」と「安全な通信」を行う場合には、下記の 4 つの条件が必要となる。

機密性　(2)完全性　(3)認証　(4)否認防止

それぞれを詳しくみていくと、

(1)機密性

文字通り第三者に「盗聴」されないようにする必要があると言うことです。

現代ではデジタルデータによる通信が当然になっており、万一盗聴された場合は、非常に大規模な漏えいが起こる可能性があります。大抵の場合、盗聴されている側は、何かしらの問題が発生するまで、盗聴されていることに気付きません。盗聴されたデータは、ログなどのファイルにより簡単に記録、保存することができ、その中から必要な情報を「検索」「抽出」することも簡単にできます。

(2)完全性

インターネットを流れるデータをインターセプトし、盗聴することは簡単にできます。それを利用してデータの内容を「改ざん」することも、また簡単です。もし「改ざん」が巧妙であれば、上記の盗聴以上に発見は難しいでしょう。

内容を「改ざん」されることなく、また「ミス」なく送ることは重要な課題です。

10 万円でパソコンを買ったはずなのに、100 万円引き落とされたら気付くと思いますが、引き落とされたのが 11 万円だったら、しばらく誰も気付かないかも知れません。

(3)認証

通信をインターセプトし、他人への「なりすまし」を行うことも可能です。

現代のデータ通信は、従来の声による電話などと違い、相手が「本人」かどうかが 非常に判り難くなっています。相手の顔が見えないまま、重要なデータをやり取りしていると言っても過言ではありません。「なりすまし」を防ぎ、相手が「本人」かどうかを確認するために「認証」という考え方が必要になって来ます。

懸命に口説いていた相手が男性だったと言うことは、怪しいチャットサイトでは良くあることです。

(4)否認防止

或る情報を送ったことを「否認」できないことを意味します。実際には送ったのに、「送っていない」または「知らない」と言うことを防止しようと言う考え方です。これは忘れられがちではありますが、通信上での「契約」を行う上で必須の条件です。

多くの人が「私はそんな注文していない」とトボケたら、インターネット上での商売は全く成り立たなくなりますし、逆に企業側が「そんな注文は受けていない」と言い張ったら、詐欺が横行することにもなりかねません。

・暗号の歴史

紀元前 19 世紀:暗号の起源としてヒエログリフ（象形文字）を用いた暗号が存在した。

紀元前 5 世紀：スパルタでスキュタレー（棒と布を使い棒の太さを鍵とした暗号）が発明される。

紀元前 2 世紀：ギリシャでポリュピオス暗号（表を使った暗号）が発明される。

紀元前 60 年:ローマでカエサル暗号(元の文章のアルファベットをある数だけずらす暗号)が発明される。

9 世紀：アラビア人が頻度分析（文章中の文字の出現頻度など、統計的特徴を使って暗号文を解読する手法）を考察する。

15 世紀：ヨーロッパで頻度分析の手法が確立される。

16 世紀：ヴィジュネル暗号（カエサル暗号を応用した暗号）が発明される。

1550 年代：イギリスで機密情報部という暗号解読の専門的な期間が設立される。

1854 年：ヴィジュネル暗号の解読法が発見される。

1895 年：無線通信が発明される。これにより情報を暗号化する必要性が高まり暗号の質が高まる。

1918 年：ドイツでエニグマ暗号機が発明される。

--第二次世界大戦後、電子計算機（コンピュータ）が発明されることにより暗号の重要性が増す--

～1975 年：共通鍵暗号方式（共通鍵暗号暗号化と復号に同じ鍵を使う手法）が主流だった。

1976 年：公開鍵暗号方式（暗号化に使う鍵と復号化に使う鍵が分けられている）が誕生する

1978 年：RSA 暗号（素因数分解の困難さを利用したもの）が誕生する。

1985 年：楕円曲線暗号（楕円曲線上の離散対数問題の困難さを利用したもの）が誕生する。

2000 年頃からは、楕円曲線暗号の新たな発展として双線形ペアリングを用いた暗号方式が注目される。

IDベース暗号：IDを用いた公開鍵暗号方式で、ペアリングが持つ双線形性を用いる手法。
タイムリリース暗号：IDの他に時間も指定することができる。
といったものが暗号の歴史となります。暗号の歴史は僕が想像していたものよりもずっと古く、驚きました。また、暗号はコンピュータの普及により急にレベルが高くなってきています。それは暗号解読がコンピュータを利用すれば従来の何倍も楽になるので、それを阻止、解読…といった、いたちごっこのようなものが続いたことが大きな原因だと思います。

コンピュータ・インターネットで使われる暗号

暗号の歴史で記載したように、暗号には色々な種類があります。

暗号の樹形図みたいなん書く

コンピュータ・インターネットで使われる暗号は現代暗号という。
現代鍵暗号は公開鍵暗号と秘密鍵暗号のふたつがある。
　そもそも、なぜコンピュータ・インターネットに暗号が必要なのかというと、インターネットの普及により誰でも簡単に情報のやりとりができるようになったことが大きいのです。現代は誰もが暗号を必要とする時代なのです。インターネットには危険が多く潜んでいます。
　例として、
盗聴・・・通信中のデータの覗き見する行為
　　個人情報（クレジットカード番号、住所、電話番号、住民基本台帳の登録者番号）
　　パスワード
改竄・・・通信中のデータを書き換える行為→送信者の意図と異なったデータに

なりすまし・・・他人の名前（番号）で注文したり、注文しておいて買ってないと言い張る

といったものがあります。これらの被害に遭うことはとても災難ですし、不快です。

　しかし、現代暗号の力は以下のことを可能にします。
盗聴・・・データを暗号化して守る
なりすまし・・・電子署名によって防ぐ（本人確認を可能にする）
改竄・・・暗号による改竄防止、原本証明（電子透かし）
　ネットワークで使う暗号（現代暗号）に必要な条件には以下のようなものがある。

・アルゴリズム（暗号の方式）の公開

鍵を秘密にすることだけで安全性を確保

世界中で安全性のチェック

暗号化に時間がかからない（コンピュータで数秒程度）

・暗号解読

暗号解読とは、正しい鍵を知らなくても、暗号化された通信を解読する技術です。暗号解読が成功すると、平文あるいは鍵のどちらかを解読するか、または暗号システムの弱点がわかるために、最終的に平文あるいは鍵のどちらかが解読されることになります。

暗号解読を試みることを攻撃とよび、暗号解読に成功すると暗号を「解く」ことになります。しかし、暗号を解くことによって、必ずしも暗号文から平文に回復させる実際的な方法を見つけたということにはなりません。総当たり攻撃（正しい鍵が見つかるまで可能性のある鍵をすべて試してみること）をしなくても解読することができるという、暗号の弱点が分かるということを意味しています。

暗号解読攻撃の基本的な方法

一般的に、暗号解読攻撃の方法は、攻撃を仕掛けるときに暗号解読者が持っている情報の種類によって分類されています。どの場合でも暗号解読者の目的は、追加情報なしで新しい暗号文を復号化することです。暗号解読者にとっての理想は、秘密鍵を抽出することです。

- 総当たり攻撃： しらみ潰しの鍵探索ともよばれ、正しいキーが識別されるまで順番に可能な鍵をすべて試してみる基本的な方法です。しらみ潰しの鍵探索はどの暗号でも展開することができ、暗号鍵に弱点があれば、しらみ潰しの鍵探索の効率を上げることができます。総当たり攻撃の成功と速度は、探索中の鍵の長さと、解読者が利用することができる計算能力によって決まります。
- 暗号文攻撃：解読者は平文のメッセージのコンテンツは全く知らず、暗号文だけで解読します。この攻撃は、解読者が使用している暗号化アルゴリズムに関する完全な知識を持っており、おそらくは同じアルゴリズムを使って暗号化したメッセージがいくつかあると仮定しています。解読者は平文を回復させるか、あるいはメッセージの暗号化に使われた鍵を導き出さなければなりません。
- 既知平文攻撃：解読者は暗号から平文のいくつかの部分を知るかあるいは推量したり、あるいは分析するために平文とそれに対応する暗号文の両方を与えられます。解読者の仕事は、この情報を使って暗号文のブロックの残りを解読することです。

・選択平文攻撃：解読者は平文および暗号文例にアクセスするだけでなく、未知の鍵を使って平文を暗号化することができます。解読者の仕事は、暗号化に使われた鍵を定義することです。
・差分選択平文攻撃：特殊な選択平文攻撃で、解読者は暗号化する平文を選択するだけでなく、以前の暗号化の結果と比較して選択を変えることもできます。
・選択暗号文攻撃：解読者が暗号文を選び、それに対応する解読した平文を与えられるか、または得ようとすることです。解読者の仕事は、鍵を導き出すことです。一般的に、攻撃の型は公開鍵暗号化システムに適用することができます。
・差分選択暗号文攻撃：選択暗号文攻撃の適応型です。暗号解読者は自由に使える解読ハードウェアを持っていますが、それから解読鍵を抽出することはできないという筋書きで、このタイプの攻撃をしかけることができます。

このように、暗号解読には多数の方法があり場合に応じて使うものが違うようです。多数の方法があるという事実が暗号解読の難しさを示唆しているのではないでしょうか。

・　RSA 暗号の解読の難しさ

RSA 暗号方式は「素因数分解の難しさを利用したもの」と暗号の歴史の部分で述べました。実際に素因数分解の難しさを見てみましょう。

素因数分解とは、ある数が与えられたら、その数と 1 でしか割りきることができない 2 以上の整数…すなわち素数を使った掛け算の式に分解することです。

例えば 33 という数があれば、3×11 というふうに分解できます。(3 も 11 も素数)

この素因数分解は簡単にわかります。しかしこれは人間の勘と長年の経験によるところが非常に大きいのです。 その証拠に、6887 はどう素因数分解されるでしょう。 これも２つの素数に分解できるのですが、解を求めるのは、なかなか難しいことだと思います。 それもそのはず、現在のところ巨大な 二つの素数を掛け合わせた数を素因数分解する 効率的な方法が見つかっていないのです。 つまり二つの素数 P=3 と Q=11 を掛けて P×Q = 3×11 = 33 を求めることは簡単にできますが、逆に掛けた結果の P×Q = 33 から P と Q（ 3 と 11 ）を知ることは極めて難しいのです。

先ほどは P=3, Q=11 で P×Q = 33 という小さな数で行ったために P×Q = 33 から P=3 と Q=11 を割り出せてしまいましたが、 これが巨大な素数を掛けたものとなると決して割り出せなくなってしまうのです。

ＲＳＡ暗号の安全性はこの素因数分解の難しさによって保証されているのです。