INCLUDEの第四回
公開日:04/7/3

第四回:暗号技術に触れる！

皆さん、こんにちは。地球の引力圏を脱出した「INCLUDE」第四回です。今回は、「暗号」に挑戦してみましょう！　ところで皆さん。自分の家に入るとき、当然、玄関口から入るでしょう。(そうでない人は玄関から入ると思ってください。)そのとき、玄関のドアに当然ついているものが、そう、「カギ」ですね。皆さんはカギを開けて、中に入るわけです。

しかし、よく考えたら、おかしくありません？カギを使ってカギを開ける、じゃあ、カギは玄関にくっついているのか？そういえばそうです。「カギ」を使って、「カギ」をあけるんですよ。こんなことありえません。

つまり、カギを開けるのではありません。「錠前」を、「鍵」を使って開けるのです。錠前とは、扉を開けなくしているいつもの「カギ」です。それを、例のギザギザのついた「鍵」であけるのです。そうすれば、中に入れるわけです。

今回から、この区別をつけておくことをお勧めします。もはや、当たり前のように「カギカギ」がはやってしまいましたが・・・。

さて本題。皆さんは「暗号」と言う言葉を聞いたことがあるでしょうか？ばかにするな？まぁ、そう言わずに。

では、暗号を解いたことはありますか？おやっ？半分以上の人は黙り込んでいます。

最後に。暗号を作ったことはありますか？あ、一人いますね～。では、君の名前を聞いておきましょう。僕ちゃん、お名前は？「田淵です！」ばんざ～い　な・し・よ。

くだらないしゃれに付き合ってもらってありがたくございます。(笑)

暗号と言う言葉は、もはや、現代の必須アミノ酸のような言葉になってきているので、いろんな場面で使われています。そう。スパイ映画や、ミステリー小説や戦争アニメだけの話ではなく・・・。

たとえば、生活に欠かせない、銀行の暗証番号や、「パスワード」なんていうのも、インターネット上で聞くことがあるでしょう。

一昔前までは、主に軍事や企業秘密の保持に、独自の暗号を作って情報を守っていました。これはこれでよろしいのかと思います。つまり、錠前の形がいびつだと言うこと。錠前の製造メーカーがわからず、全日本錠前協会(フィクションかもしれません)の定める錠前規格からはずれた、不思議な錠前を使っている感じです。だから、泥棒だってあけられません。これは、安全。

しかし、今のようなインターネット時代では、そうはいきません。あったことも、聞いたことも無い、見ず知らずの人の人のホームページなどで、「パスワード」などをつかって、会員情報などを保護しています。そして、「誰でも」ホームページに訪れることができます。ここが味噌。そのなかで、会う人ごとに錠前を用意するのは、無理があるでしょう。

ですので、こう言った場合、錠前の形はみんなに教えておきます。そして、カギをとても精巧に作っておけば、泥棒だってカギを複製したり、作ることはできません。これは、後でふれますが、「公開鍵暗号」などといわれます。

たとえば、錠前の形が全世界で共通だとして、鍵を誰でももっているとします。さて、皆さんがお持ちの家の鍵、ギザギザがついていますが、もし、ギザギザがたった1つしか無かったらどうしますか？泥棒だけでなく、どんな人だって2通りの鍵を手作りすれば、開けられてしまいますね。

しかし、ギザギザが
1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000個あったらどうです？同じものなどまず作れません。これは「実質」安全。(いずれ、合鍵を作る人が出てくるでしょうが)ですから、基本的に、「錠前」を屈強にするのでなく、「鍵」を精巧につくることが大事と言うわけ。

また、インターネットでは、いつどこで情報の改ざんなどが行われているのか、わかったものではありません。匿名性の裏には、メリットとデメリットが同じだけ潜んでいるのです。つまり、周りを見たら悪い人が半分いるわけ。

まあ、こんな短絡的な考えはありませんが。でも、本当にそれだけのことを「秘密に」できる時代になったのです。うかうかしていると、どこの馬の骨かもわからない、悪い人によって、インターネット上で、利用されてしまいます。それには、主に2つの理由があるのでしょう。

まずひとつに、自己防衛の仕方を知らない人がいること。これは、結構多いです。たとえば、インターネットにつなぎっぱなしのまま、ウイルスに感染されたり、情報を奪われたりする、これは、本来、完全に防ぐことはできません。悪い人はいるものです。年がら年中、ウイルスを作ったり、ハッキングしたり。しかし、ある程度なら、某社のセキュリティソフトなどを使って防げます。

自分のみは自分で守る、これが大切です。現実の社会と違い、被害にあっても相談に乗るくらいしかできません。法律も甘いものばかり、犯人も見つからない。そして、結局泣き寝入り。

よくあることです。まずは、常に危険が潜んでいると言う意識を、きちんともちましょう。

さて、2つ目は安全と言われるセキュリティに頼りすぎる人がいること。「安全な」と聞くとすっかり信頼しきってしまう、しかし実は、抜け道があった。結果ハッカーに情報を奪われる、これも良くあることです。ですが、結局、対策をしてもいずれ悪い人は「新しいスキ」を狙ってきます。そうやって、今まで「イタチゴッコ」を繰り返してきました。

これに付随して、メールなどで簡単にパスワードをやり取りしたり、パスワードがかかっているからって、そのままメールでデータを送ったり。こんなことをすると、いつなんどき、被害にあってもわかりません。「いつのまにか」が命取りなのです。

完全なセキュリティなど、存在しないのです。ですから、いつであっても、新しいセキュリティなどに目を光らせておきましょう。

また、「理論的な」錠前とカギを用意しましょう。昔から、悪い人はいるのです。100年単位の昔から、暗号は「情報の錠前」として使われてきました。それは今も同じ。しっかりとした暗号を学ぶとよろしいです。

書いてる手前、こんなことをかきたくはありませんが、

このページの解説にも、落とし穴があるでしょう。

10人いれば10人の頭があるので、だれが悪いことを思いつくかはわかりません。無責任といえばそれまでですが。ですので、インターネットの常識にのっとり、「複数の人の解説を見比べる」ことを行ってくださいね。

さて、暗号の必要性をかいてきましたが、(と言うより、セキュリティの話にずれてきたような・・・)いよいよ本題の本題。暗号の理論を紹介します。

皆さんが読んだことのある「シャーロックホームズ」シリーズ、中に暗号として「踊る人形」と言うものがありました。これは、純粋に暗号です。人形の踊りかたの中にある「法則」という「鍵」が無ければ、解けない(あけられない)ものでした。

また、「江戸川乱歩」にも暗号が登場します。

これらの「暗号」は、共通して、「法則性」と言う「鍵」があります。これは、法則を知らない人にしてみれば、意味のわからないものです。だって、突然棒人間が踊ってるんですよ!誰がわかりますか?

しかし、これらの暗号はあまり優秀な暗号ではありません。法則性を見破られたら、全てがおしまいです。つまり、「元の文」さえ手にはいれば、「いずれ」中身がわかってしまうのです。ですので、ボーイスカウトや、忍者の情報のやり取りなど、単純なことに使われます。

パズル(ミステリー小説などでも一緒)みたいにぽんと出てくるような暗号では駄目なのです。パズルは、「作った人」が必ずいますから、そうすると、「解く人」だっています。

それでは、優秀な暗号とは何なのでしょうか?

優秀な暗号は、どんな場面でも優秀、つまり、「数学的に」優秀でなければいけません。これは、つまり「数学」を利用するもの。これまた、つまりは「数字」を利用するもの。数字の区別がつまりは鍵です。数字を「鍵」として持つと、メリットがあるのです。

法則性を知らなくても、「数字」さえわかれば錠前をはずせます。「知らなくても」です。コンピュータを使って、情報を保護する場合(というか、現代でこれ以外の場合があるでしょうか?)、決められた法則にのっとって情報を暗号化します。暗号化とは、つまり、金庫にしまうと言うこと。そして、ぺっと鍵を吐き出してくれます。皆さんは金庫にしまいたいものをしまうだけでいい。これほどわかりやすいものはありません。

しかも、鍵さえわからなければ(鍵の保護は必要ですが・・・)、法則を知っていても錠前をはずせないのです。なので、悪い人たちは「鍵」を自動で作る装置を開発します。つまり、鍵自体は単「ならない」数字、意味のある数字ですので、1から順に鍵のギザギザ(数字)を作っては、錠前に差し込んでみるのです。これの繰り返しをすれば、「いつか」あきます。これは「絶対」です。「全数検索」などといったりします。

しかし、皆さんがよく言う「いつかわかるでしょう」と言う言葉は、正確さに欠けます。いつかとは、いつですか?それが大事です。そして、現在最強の部類に入る暗号は、この世の中にある「全ての」・「最強の」コンピュータを使っても、150億年かかったって、たかだかひとつの鍵を作ることはできないのです。どんな天才泥棒であろうとも、無理です。コンピュータの性能が上がらない限り、この天才は

「役立たず」です。いても無駄です。

そして、すごいことは、なんと！

その法則性を皆さんに見せているのです。暗号の世界では、見せるものは少ないほど良かったのです。つまりは、鍵以外全てを非公開にするのが一番良かった。

しかし！今の世の中、先ほども言ったように、錠前を個人個人に用意するのは無理があります。それに、そんなに錠前を手作り(つまり、開発する)するのは無理でしょう。だったら、鍵を精巧に、緻密に作ればいい。そういった考えに基づいて、現代の暗号は作られています。これはわかりやすいです。だって、使う人はぽんと金庫にしまうだけでよい。泥棒は役立たず。

こんなに「最強の」暗号の「作り方」はありません。しかし、それは「最強」ではありません。問題なのは、「錠前」のほうです。

先ほども言ったとおり、鍵を1から作る泥棒がいるのは事実です。そうして、実際にいくつもの暗号が破られています。これは、「鍵」が精巧で、錠前が「ぼろい」せいです。

「共通な錠前」であっても、鍵を簡単に「次々と」作れるような錠前では駄目なのです。つまり、簡単にコンピュータで鍵を作れること。つまり、「高速に」鍵を作れると言うこと。つまりは、「安全でない」錠前なのです。

錠前の形は共通でも、それ自体の形は違います。より安全にするには、「錠前」も、精巧に作らなければならないのです。そして、それは皆さんに見せてしまうわけです。でないと、皆さんの鍵だって作れません。だから、こういうのを「公開」鍵暗号、と呼ぶのです。現在は、これ以外に皆さんの使える暗号はありませんね。自分だけで使う秘密の暗号なら別ですけど。

ただ、先ほども言ったように、これ自体は暗号の「形式」なだけで、中身が良くないと優秀とはいえません。やはり、中身が大事なのです。そして、専門的に言えば、「数学的に安全」であることを「証明」しなければなりません。この証明の基本はコンピュータです。

「理想的な」テストを述べましょう。

この世で「もっとも最強＝超最強」の、たった1台のコンピュータを使って、鍵を作っていく実験をしましょう。難しくなりますが、CPUがひとつあって、一回の鍵を作って、錠前がはずせるかどうかを1秒で行えるとします。つまり、開いたか開かなかったか。

さて、このコンピュータを、全世界になぜか、一人10台持ってるとしましょう。そして、全人類が同時に、鍵のテストをします。

つまり、一秒間に1＊人口(60億人としましょうか)＊10回＝600億回のテストができるわけですね。

さて、鍵のほう。鍵は、1000兆個に一個だけ、錠前をはずせる鍵があるとしましょう。先ほどの、「一秒間に600億回」のテストを行うと、1667秒で、誰かのパソコンで「開いた！」との結果になるでしょうね。これは「絶対」です。

こういったテストをします。「数学的に」と言うのは、暗号に使う数学の理論、つまりは、「コンピュータで扱う命令」をどれだけのスピードで実行できるかと言うことを考え、あとは、クロック周波数と、世界でパソコンが何台あるか、ぐらいのテストをして、「いつかわかる」の「いつか」がどれくらいなのかということで、安全かどうかを判断します。

理想的には、1命令で鍵テスト一回だとすれば(これ以上早いのはありません。クロックに同期しているCPUは、一回のクロックで「原則」ひとつのことしかできませんから。もしあるのなら、それを1命令としましょう。)、クロック周波数が爆発的にあがるとは考えにくい(ムーアの法則を凌駕するパソコンは、この先、光コンピュータが現在の100倍程度、超伝導コンピュータが200000倍程度、量子コンピュータが未知数、などがあげられています)。だから、ワーストケースを考え、安全と言えるくらいの

(200000倍の性能が来年実現できても、解析に1000年かかるくらいの安全さ、などと考えてください。)
暗号だったら、晴れて世の中に羽ばたいていくのです。

公開鍵で、現実てきだなぁ、と思う暗号は、「最強の」乱数発生装置を使って、1バイトずつ乱数との和をとったあと、その乱数を保持すると言うもの。データサイズが増えるごとに安全になるし、乱数データを捨てたら絶対にわかりません。だって、「法則が無い」んですから。

ですけど、考えてみれば、たとえばテキストデータで、部分部分で単語がわかるなどすれば、部分部分でわかってしまい、全部を推測できそうなので、だめですかねぇ。

でも、解析したものが真の文章かどうかは、本人以外、「絶対に」知りえません。

「明日また新宿で会おう」と言う文が「ぐはいrlsごjgそrぱ」と暗号化されたとしましょう。解析した結果、「7月」と、「ニュージーランド」と言う単語が出てきた。推測してみた結果として、「7月にニュージーランドで会おう」となったとしましょう。

しかし、明らかにもとの文とは違います。「意味が通」っても、「あってる」かどうかは、本人しかわからないでしょう。この暗号、実際、「バーナム暗号」として、電信用にフランス軍が使ってたらしいです。今でも、強力な暗号です。

もっと最強(超超最強)にするには、間違った鍵でも、錠前が開いてしまうというもの。一見意味が無いように思われますが、きちんと意味があります。錠前をあけた先が、「パラレルワールド」なのです。つまり、間違った鍵データを入れても、データを出力してしまうのです。(もちろん、ランダムデータの通りに。)こうすると、あっているのか間違っているのかもわかりません。もちろん、本人が鍵を間違っても区別なしにです。ある意味、「究極の暗号」といえませんかね?

しかし、実際には「最強の」暗号なんてありません。乱数には「法則」がつき物です。だって、コンピュータで出すんですから。それこそ、最強の暗号を思いついたらノーベル賞ものです(つまり、法則の無い法則を見つけることに値します。これは意味がわかりません)。あるとすれば、さっきのバーナム暗号を使えばいいんですからね。乱数については、暗号と同じくらい、研究対象になってますので、これを暗号に利用するのは、乱数自体の安全性の証明が難しいので、理想にはなりえません。(いやぁ、暗号って奥が深いですねぇ!)

そこで、今の暗号では「数学的に」証明できる暗号が使われます。

ここら辺は、特許がうずめいているので詳しくは説明しません。

強力な暗号のひとつに、「素数」を使うものがあります。

素数とは、「1とそれ以外に、割り切れる数が無い」数字です。つまり、それらの組み合わせも、それ以外に割り切れる数をもっていないのです。

しかも、この素数を求める「一般式」は、現在の数学で証明されたものがありません。ここが重要です。つまり、複雑な素数があったとして、その数がどの素数との組み合わせかを見つけるのは至難の業なのです。しかも、解析する場合、「全数検索」しか方法が無いので、数学的に安全と言えるでしょうね。(素数表みたいなものがあれば、多少はぼろくなるでしょうけど。)

しかし、問題もあります。この素数の一般式がわかったとたん、泥棒が今までに手に入れた、暗号化されたデータが全て本当のデータになってしまうのです。そうなると、いつの時代にも価値のある情報(芸能人のこととか)などは、暗号化データの漏れすら防がねばなりません。防げるくらいなら、暗号化しなくてもいいでしょうね。しかし、DVDなど、暗号化してでも配信したい場合などは、暗号が重要になってくるでしょう。

重要なのは、「証明できない問題はない」と言うこと。ただし、それが本当かはまさに「神のみぞ知る」ですけど。

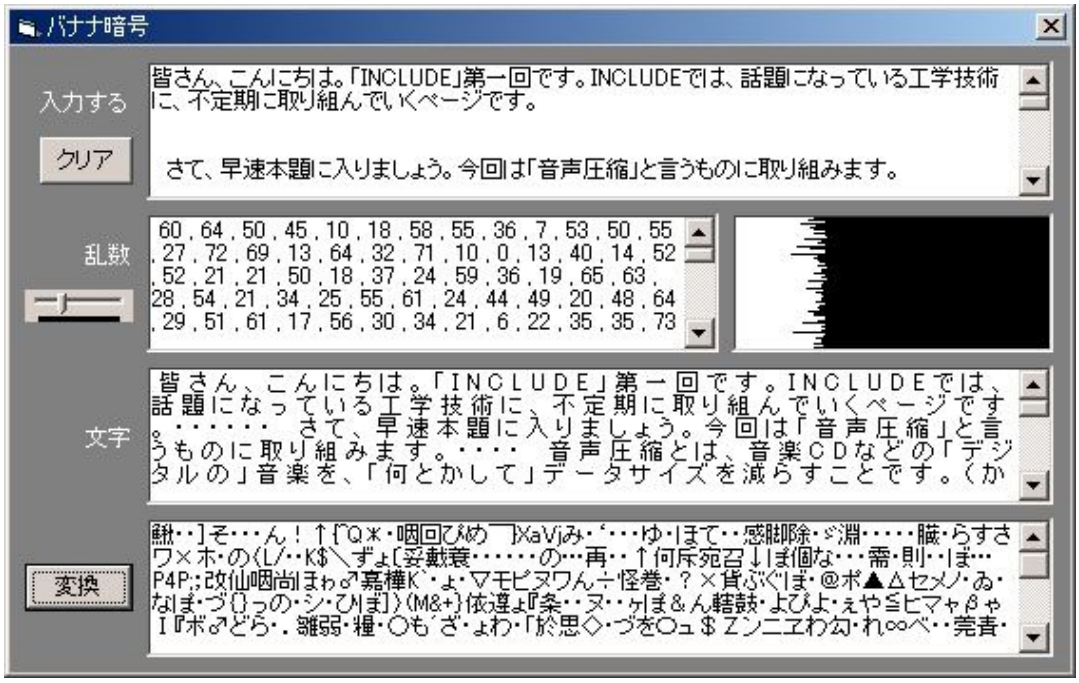
さて、こういった、かたっぽのことは簡単にできるのに、もうかたっぽは難しい、と言う性質を持つ関数を、「一方向関数」と言います。暗号の基礎です。さらに、意図的に落とし穴を空けておいたものを「落とし戸つき一方向関数」と呼ぶらしいです。これは、暗号化のときに、キーワードを入れると簡単に暗号化できるといったもの。暗号化を早くするキーポイントです。(たとえば、乱数よりも安全な?「人の入力」を利用します。といっても、人のほうが「癖」がでるので、乱数にはなりませんけど、意味のなさそうで癖のあるキーワードなら、全数検索してもヒットしにくいですし、なにより暗号化が早くなるので、メリットがあります。)

他にも、「離散対数問題」や、「楕円曲線暗号」といった技術用語があるので、興味のある方はごらんあれ。

さて、長々と話してきましたが、僕は乱数が好きです。なので、バーナム暗号に似た「バナナ暗号」というものを作ってみましょう。

例によって、オリジナルです。例によって、たいしたこと無いです。例によって、だれも盗みません。だから例になるのです。これが僕の理論。

以下の図をご覧下さい。



これは、バナナ暗号をVBで作った図です。文字列を入力して、乱数の幅を指定すると、乱数との和が出力されます。黒抜きの部分は、乱数をグラフにしたものです。

バナナ暗号のメリットは、暗号化が高速なのと、法則性が存在しないことです。デメリットは、鍵が長すぎることと、乱数の法則性が存在し、それが最強とは呼べないことです。

メリットのほうを詳しく説明すると、(「VBだから」と言うのは言い訳ですけど、何をやるにもVBじゃ遅いわけで、あまりメリットを感じれないかもしれませんが)とにかく和をとるだけのシンプル構造なので、暗号化に必要な時間が少なくてすむわけです。

また、和をとる法則はあっても、全数検索すらできないので(先ほど述べたように、真の文は貴方にしかわかりません)、つよいつよい暗号なのです。

デメリットのほう。鍵が長いと言うのは、つまり、他の人に渡しにくいと言うことです。たとえば、5人の人に暗号データの鍵を渡すとき、とても長い鍵データを渡さなければなりません。まぁ、今回は全ての値と乱数の和を取ったので、こんなに長くなりましたけどね。これは危険。

あと、乱数は、初期化が必要になります。なぜなら、乱数に法則があるから。だから、乱数をシステム時間で初期化します。そのため、初期化値＝システム時間を全数検索してヒットした（といっても、錠前があくかどうかはわからないのですけど）場合、まるっきりわかってしまうと言うことです。

しかも、初期化値はたいした精度はありません。たしか32ビットだったかな？これでは、4億2千万回初期化の検索をしたら、ヒットしてしまいます。これはすごく弱いですね～。

まあ、導入ですので。そう割り切ってください。

覚えておいて欲しいのは、鍵データの1ビットに、いかに多くの情報を詰め込むかと言うことです。これは、全数検索にはとてつもなく時間がかかり、正しいときだけ高速に錠前をあけられるような、理想的な暗号方法を考える際に、とても重要な意味を持ちます。

バナナのダウンロード

さて、ちょっと異端児な暗号方法？をご紹介。といっても、僕が作ったんですけど。暗号理論でもなんでもないですから、期待しないで下さい。あくまでも、「こういうこともありなのでは？」と言うことです。

名づけて「日常暗号鍵」！何かかっこいいでしょ！

さて、何をするのかと言うと、先ほどのバナナの初期化値などに使ったり、他の暗号における「落とし戸」を、何もキーボードで入力しなくてもいいじゃないの？という観点から、ゲームを利用して、与える事にするソフトです。

どういう意味かと言うと、普段キーボードを使ってデータを入力するでしょう。暗号化の「落とし戸」も同じで、ほとんどの場合、キーボードで文字列を入力します。

しかし、キーボードは、結局、頭の中に文字列が浮かんでいたり、めちゃくちゃに入力しても結構人間の癖と言うものは出てしまうものです。つまり、周りにいる人がパスワードのキーボードの指の動きをのぞいていて、もし9割くらいわかったのなら、たいていは全数検索してわかってしまいます。これは、隠しカメラで録画したりしても同じことです。

つまり、セキュアな入力方法など無いのです。これを打開するために、バーチャルめがねをつけて、でたらめにキーボードを配置して、めがねを通したときだけ、その位置がわかるような装置を企業など

が開発されています。

では、隠しカメラで撮ったり、覗いたりできないような、しかも、簡単にできるものは無いのでしょうか？あります。それがこのソフト！（誇大広告）

このゲームは、連打力と、もぐらたたきのタイミングなどをゲームとして入力して、その結果があらかじめ決まった値と似ているときに、照合可とするものです。今回は、プロジェクトをオープンにしますので、吐き出す部分はご自分でおつくり下さい。（なんて無責任な！）といっても、結果は内部でわかりますので、その値を実際の暗号に使ったりすれば普通に使えますので。

ただし、このプロジェクトははっきりいてごちゃごちゃです。わからない場合、同じようなソフトを作ってみるのがよろしいかと思います。

日常鍵のダウンロード

次こそは、といいつつも、やはり未定の「不定期プロジェクト」。次回も楽しい記事を書きますので、どうぞごらんあれ～。そして、お楽しみに～

おしまい。

ダウンロード

さて、記事に使ったプロジェクトを公開します。

日常鍵・・・VB用

バナナ・・・VB用

メール等の受付

当サイトの管理人は、MORIOです。

質問やご要望、ご感想、苦情などは、メールで受け付けております。以下のアドレス宛に送ってくださいませ。

master@morik.net

form 2006/1/9