その昔の暗号の話

JJ1SXA 池

太平洋戦争の開戦を告げる、かの有名な「ニイタカヤマノボレ 1208」は、実はこのようにそのまま平文のモールス信号で打電したのではありません。

「X 日(開戦日)を、12 月 8 日とする」というのを、「新」「高」「山」「登れ」「12」「08」と単語ごと一つ一つを暗号書により数字に変えて、更に乱数表を使って暗号化したものが打電されたそうです。

ちなみに、暗号書により数値符号化したものが 1 次暗号で、乱数表で更に変換したものが、2 次暗号です。

暗号手が、原文を 2 次暗号まで変換、通信手が、この 2 次暗号(数字の羅列)を送信し、相手方の通信手が、受信したものを、相手方の暗号手が、逆手順で正規の電文に直します。

尚且つ、数字は軍隊独特の略数字(効率良くするため短い符号)で、送・受信です。

モールス符号を知らなければ、それだけでも暗号のようなもの、高速の和文なら、外国の通信兵には、生の平文でも暗号のようなものだったのでは無いかとも思いますが、乱数表を使って暗号化しているにもかかわらず、日本の暗号は、暗号強度が低く、ほとんど解読されていたとの話もあります。

暗号の例(原文は、ニイタカヤマノボレ 1208)

01234567890123456789012345…仮定の乱数表

41013010706094598311220088…仮定の暗号書による 1 次暗号

60221557194139968678892367…2 次暗号(乱数表と 1 次暗号による)

乱数表は短時間では解読されませんが、1 次暗号は直ぐに解読できます。

上記の 1 次暗号と、原文「ニイタカヤマノボレ 1208」で、ある法則を見つけてください。

仮定の乱数表は規則制(0から順番)がありますので、バレバレですが、不規則の数字の羅列で乱数表はできています。

1 次暗号の法則は解読できましたか?

法則を見つけたら、次の数字を解読して下さい→「741238916021300463383402」

240 グループの局で解読できた局は、連絡ください、正解者には…?? (何かがあります…お楽しみ)

7MHz などで、高速の数字のみの CW を良く聞きましたが、暗号での連絡でしょう…

現在では、乱数表使用の数字だけの暗号文を無線で送受することはほとんど無くなりましたし、このような乱数表方式暗号は過去の遺物?となりました。

インターネットが主流の現在、RSA 公開鍵暗号方式が良く使われているようですが、実際には数値化の基本は変わっていないようです。

素因数分解が基本のようで、素因数分解には、「楕円曲線法」「複数多項式二次ふる

い法」、更に最近では、桁数の多い素因数分解に有効な「数体ふるい法」等の高等数学が使われ暗号化が行われるようで、暗号理論はより高度になり、素人には難しくてとても理解できるのではありません、子供向けのこれが分かりやすい

「暗号の科学」(http://jvsc.jst.go.jp/live/angou/index.htm)

現在主流の、「RSA 公開鍵暗号方式」は Rivest、Shamir、Adleman の三人の名前の頭文字をとって RSA 公開鍵暗号方式と名付けられました。

また、「DES 暗号方式」は、アメリカ商務省標準局がデータ暗号化規格(Data Encryption Standard)として制定したものです。

ここまでの記事は、1 年位前から HP に載せてあるものを若干編集したものです。

脳のトレーニングに、単純な数字の加減乗除等が有効との話もあります、前記の乱数表使用の暗号では、乱数表の数字列の数字から、1 次暗号の数字列の数字を 1 桁単位で減算してできた数列が、2 次暗号です。

2 次暗号作成の逆手順で、乱数表の数字列の数字から、2 次暗号の数字列の数字を 1 桁単位で減算してできる数列が、1 次暗号です。

平文を 1 次暗号に変換したり、逆に 1 次暗号を平文に変換するのも、かなり脳を使うことでしょうが、数字列の数字を 1 桁単位で減算する作業は、かなりの脳トレだと思います、この作業は、当時の一流の暗号手は、分速 150～170 字位をこなしていたそうです(200 字超の猛者もいたようです)、とりあえず、0、1、2…9 の繰り返しで筆記を一寸やってみてください、多分最初は 1 分間 60 字位書くのが精一杯？の筈です、計算をしないでこれですから、計算をする作業を入れて、分速 150 字がいかに早いかがわかると思います…ここまでの、暗号の話については、元陸軍通信隊暗号手だったOMさん(コマーシャルがらみで知り合った個人タクシーの運転手さん)から教えてもらいました。

次は、元日本海軍の通信手だったOMさん(JM1△△△…私の縦振れキーの先生)から聞いた話、とにかく徹底的に鍛えられて、ある期間経つと試験があり、成績で半分にクラス分け、その後の試験ごとにどんどん成績順に細分化し、卒業時の 1 番目のクラスが大本営(古い言葉です)、2 番目のクラスが戦艦というように、以下順次、重要部門順に振り分けて配属されたとのこと、このOMさんも当時は、縦振れキーで、和文を分速 100 字以上、それも確実な送受信を求められ、クリアーしていたそうですが、ようやく 3 番目のクラスだったそうです、かなりの年配でしたが縦振れキーを達者に操っていました、それにしても上には上があり、人間離れした、神様みたいな人がごろごろいたのですね。

(戦争には負けたが、良し悪しは別にして、旧軍隊の教育恐るべし…)

年々急速に衰える脳に刺激を与えて、活性化といかないまでも、衰えの速度を鈍化させなければと思ってはいるが、有言実行ならぬ、有言不実行の日々、これではいけないとは思いつつも、「昨日かくてありけれ、今日もまたかくてありなん」…まっ、いいか hi