

# classicalcipher.sty (v0.1)

## サンプル

ワトソン

2015 年 10 月 21 日

いまここに、あなたの心情を表す英文があります。

I love TeX

ちょっと気恥ずかしいので、この文をシーザー暗号という最も古典的かつ単純な方法で暗号化してみましょう。

L oryh WhA

パッと見ただけでは意味がわからなくなりました。しかし元の文のスペースがそのまま反映されているため、単語の区切りが丸見えです。適当に 2 文字区切りにしてしまいましょう。

Lo ry hW hA

少しマシになりましたが、まだ平文の大文字・小文字の区別が残ってしまっています。全部大文字にしてしまった方が、少しは暗号強度が上がるでしょうか。

LO RY HW HA

次の文字列を見てください。

Lw lv qlfh zhdwkhu wrqdb.

意味不明ですね。でも、単純なシーザー暗号なので、すぐに復号化することができてしまいます。

It is nice weather today.

今度はこれです。あなたに解読できますか？

Gbeej Wotath

シーザー暗号よりは少し複雑になった、アフィン暗号です。しかし、これも頻度分析と簡単な方程式を解けばすぐに鍵が明らかとなります。暗号化に必要な鍵さえわかれば、復号化など朝飯前です。

Hello Brutus

せっかく暗号化するのであれば、やはり解読されたくはないものです。絶対に解読できない暗号も使ってみましょう。

eP1GRKLo;ANM3RWVR

この暗号を用いると、様々な記号がし得るので、タイプライタ体にした方が見やすいかもしれませんね。

eP1GRKLo;ANM3RWVR

このバーナム暗号は鍵を知らないかぎりは絶対に解読できません。逆に、鍵をもつ者であれば、暗号化とまったく同じ手順で復号化できます。

TeX\_is\_Wonderful!

暗号文からは読み取れませんでした。空白や感嘆符の情報も保持されていたようです。

e"1GRKLo;ANM3RWVR

バーナム暗号による暗号化の結果は、すべての文字が扱いやすい文字となるとは限りません。

>~9K,1G>`~<^->»m@

印字可能文字の範疇にあればまだいいですが、印字不能な文字に変換されてしまうケースもあるかもしれません。そこで、暗号化結果を「文字」に変換せず、2進数のまま出力してしまう方法を考えます。

0101110 0011101 0111010

7文字ずつに区切っていますが、ASCIIコードは7bitなので、それぞれが暗号化前の1文字と対応しています。復号化して、3文字になるか確かめてみましょう。

TeX