

CS第1 演習ガイド

本日の予定

1. 準備
2. ango.rb, hukugo.rb の作成
3. kaidoku.rb のアイデア
4. kaidoku.rb の作成など

1. 準備

1. ログインする.
2. **Terminal** を動かす (TSUBAME と直接対話する窓口).
 - 2.1. **cd** kadai3 課題3の部屋(フォルダ)へ移動.

2. 暗号化, 復号プログラムの作成

ango.rb, hukugo.rb の作成

1. まずは, コピーしてきた復習用の code.rb を実行してみよう.

```
code_a = 97          # 文字 a の文字コード
kosu = 26            # 英字アルファベットの数

bun = gets.chomp     # 入力文字列から改行を除去
cc = bun.unpack("C*") # 文字列懼口文字コードの配列
leng = bun.length     # 文字列の長さ

for i in 0..leng-1
  moji = bun[i]       # bun の i 文字目を得る (i は 0 から始まる)
  code = cc[i]        # その文字のコードを得る
  sa = code - code_a  # 文字 a との差分
  if 0 <= sa && sa < kosu
    print(moji, ": ", code, ", ", sa, "¥n") # 小文字アルファベットなら
                                              # 差分まで表示する
  else
    print(moji, ":", code, "¥n")           # そうでないときは
                                              # 差分は表示しない
  end
end
end
```

2. これを参考に, ango.rb, hukugo.rb を完成させよう.

2. 暗号化, 復号プログラムの作成

ango.rb, hukugo.rb の作成

2. これを参考に, ango.rb, hukugo.rb を完成させよう.

```
# enc(秘密鍵 k, 平文 m) = 暗号文 c
def enc(k, m)
  code_a = 97          # 文字 a の文字コード
  kosu = 26            # 英字アルファベットの数
  leng = m.length      # 文字列の長さ
  a = m.unpack("C*")   # 文字列から文字コードの配列へ変換
  b = Array.new(leng)   # 暗号文(のコード)格納用配列
  for i in 0..leng-1
    code = a[i]         # i 文字目のコードを得る
    sa = code - code_a  # 文字 a からの差分
    b[i] =
  end
  c = b.pack("C*")      # コードの配列を文字列に直す
  return(c)
end
# サブルーチン enc (終)
```

← ここを作る

使い方

```
k = 3
hirabun = gets.chomp      # 平文を入力
angobun = enc(k, hirabun) # 暗号文に変換
puts(angobun)             # 暗号文を出力
```

2. 暗号化, 復号プログラムの作成

3. 作った ango.rb, hukugo.rb の使い方

```
$ ruby ango.rb  
Hello, love you!  
Hhoor, oryh brx!  
$
```



m.txt

Hello, love you!

前もって安全なところで
作っておく

Terminal 上での使い方

- ・ 入力データをファイルから読み込む
`ruby ango.rb < ファイル名`
- ・ 出力をファイルに書き出す
`ruby hukugo.rb > ファイル名`

※ 読み込んで書き出すことも可能

`ruby ango.rb < hirabun.txt > angobun.txt`

```
$ ruby ango.rb < m.txt  
Hhoor, oryh brx!  
$
```



3. 解読プログラムのアイデア

解読



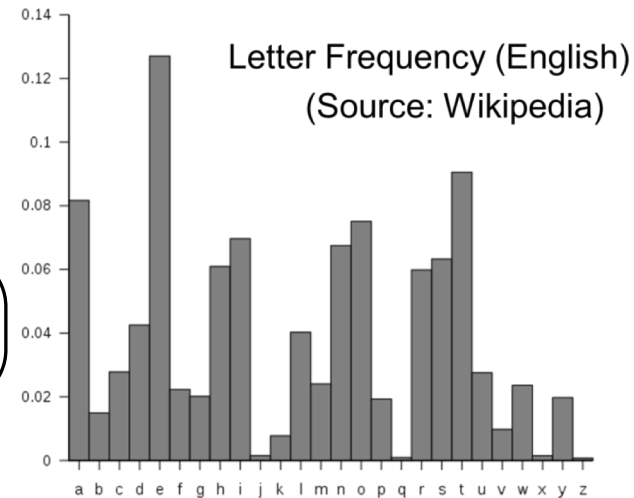
秘密鍵を知らない者が暗号文から平文を得ること

比較的長い英文を暗号化したものを解読したい
どうすればよいか？

明らかなだよ
ワトソン君

英語の場合

一番多く現れる文字が e のはず！



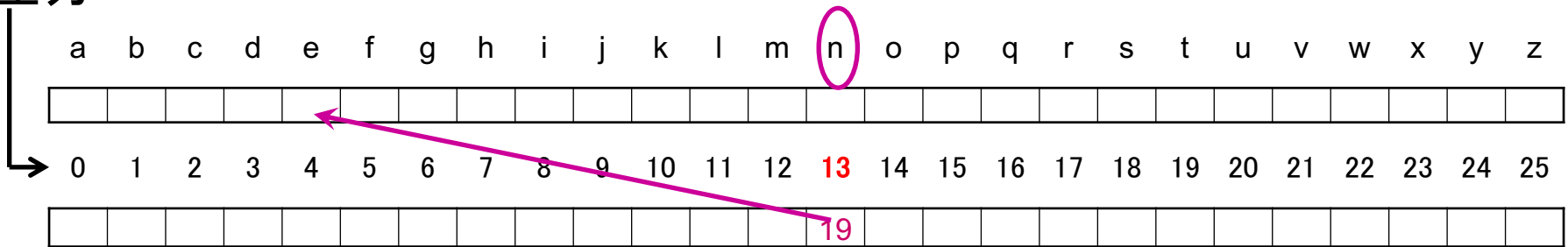
qxuv**n**b qjm k**nn**w b**n**jc**n**m oxa bxv**n** qxdab rw bru**n**wl**n** frcq qrb
uxwp, cqrw kjlt ldae**n**m xe**n**a j lqnvrlju e**n**bb**n**u rw fqrlq q**n**
fjb ka**n**frwp j yjacrldujauh vjuxmxaxdb yaxmdlc. qrb q**n**jm
fjb bdwt dyxw qrb ka**n**jbc, jwm q**n** uxxt**n**m oaxv vh yxrwc xo ...

n が19回出現で最多

qxuv**n**b qjm k**nn**w b**n**jc**n**m oxa bxv**n** qxdab rw bru**n**wl**n** frcq qrb
 uxwp, cqrw kjlt ldae**n**m xe**n**a j lqnvrlju e**n**bb**n**u rw fqrlq q**n**
 fjb ka**n**frwp j yjacrldujauh vjuxmxaxdb yaxmdlc. qrb q**n**jm
 fjb bdwt dyxw qrb ka**n**jbc, jwm q**n** uxxt**n**m oaxv vh yxrwc xo ...

n が19回出現で最多

差分



$$13 - 4 = 9 \text{ だけずれた} \Rightarrow k = 9$$

頻度配列と呼ぼう

アイデア

注意 ! $\max j < 4$ のときも
大丈夫 ! ?

1. 頻度配列 hindo を作る.
2. 最大頻度の場所 $\max j$ を見つける.
3. $k = \max j - 4$ で求め, $\text{dec}(k, \text{angobun})$ で平文を求める.

まとめ: Terminal command

命令	使用例	意味
mkdir	mkdir kadai2	kadai2 というフォルダ(部屋)を作る
cd	cd kadai2	kadai2 というお部屋に入る
	cd ..	上の(大きな)部屋に戻る
	cd ../..	上の上の部屋に戻る
ls	ls	その部屋にあるファイルを表示する
rm	rm foo.rb	foo.rb を消す(戻らないので注意)
リダイレクト <	ruby xx.rb < aa	xx.rb を実行. 入力 は aa から取り込む
リダイレクト >	ruby xx.rb > bb	xx.rb を実行. 結果は bb へ出す