

CS第1 演習ガイド

本日の予定

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

1. Terminal を動かす
2. 講義のウェブページから プログラム をダウンロードする.
 - Downloads(ダウンロード)フォルダに day6.zip が展開される
3. Terminal で day6 をCS1 に移動
 - `cd Documents/CS1`
 - `mv ~/Downloads/day6 ./`
 - `cd day6`

2. 暗号化, 復号プログラムの作成

3. 作った angoo.py, hukugo.py の使い方

```
$ python angoo.py  
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
`python angoo.py < ファイル名`
- ・ 出力をファイルに書き出す
`python hukugo.py > ファイル名`

※ 読み込んで書き出すことも可能

`python angoo.py < hirabun.txt > angobun.txt`

```
$ python angoo.py <  
m.txt  
Hhoor, oryh brx!  
$
```



3. 解読プログラムのアイデア

解読



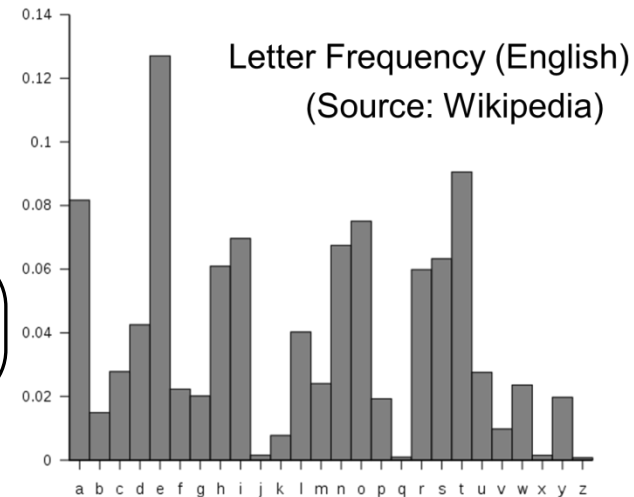
秘密鍵を知らない者が暗号文から平文を得ること

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！



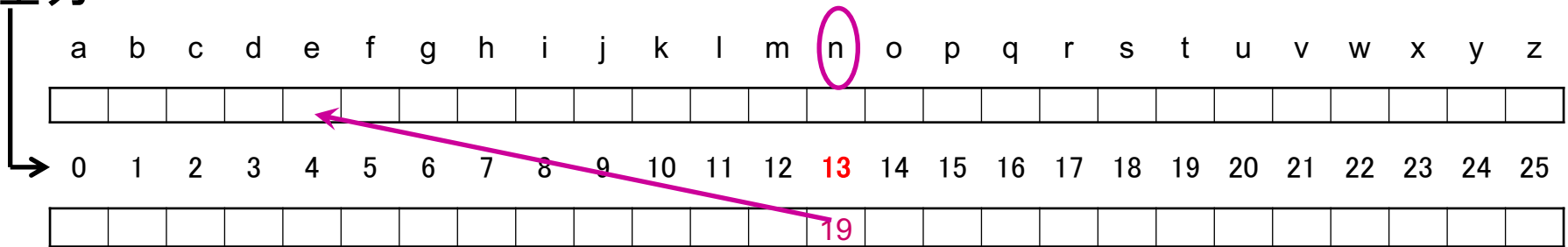
qxuv**n**b qjm k**nn**w b**n**jc**n**m oxa bxv**n** qxdab rw bru**n**w**n** frcq qrb
uxwp, cqrw kjlt ldae**n**m xe**n**a j lqnvrlju e**n**bb**n**u rw fqrlq q**n**
fjb ka**n**frwp j yjacrldujauh vjuxmxaxdb yaxmdlc. qrb q**n**jm
fjb bdwt dyxw qrb ka**n**jbc, jwm q**n** uxxt**n**m oaxv vh yxrwc xo ...

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 というフォルダを作る
cd	cd kadai2	kadai2 というフォルダに入る
	cd ..	上のフォルダに戻る
	cd ../..	上の上のフォルダに戻る
ls	ls	そのフォルダにあるファイルを表示する
rm	rm foo.py	foo.py を消す (戻らないので注意)
リダイレクト <	python xx.py < aa	xx.py を実行. 入力 は aa から取り込む
リダイレクト >	python xx.py > bb	xx.py を実行. 結果は bb へ出す