演習ガイド: Windows

1. 講義のウェブページから day6.zip をダウンロードする.
   - Downloads（ダウンロード）フォルダに day6.zip を置かれる
   - ファイルを開く → すべてを展開
   - 展開先として，Documents¥CS1 を指定して，展開
2. コマンドプロンプトを実行
3. day6 フォルダに移動
4. 内容を確認

OneDriveを使用している場合，zipファイルの展開先が
　OneDrive¥ドキュメント¥CS1
になるので下の最初のコマンドを変更

```
C:¥Users¥minamide>  cd  Documents¥CS1
C:¥Users¥minamide¥Documents¥CS1> cd day6
C:¥Users¥minamide¥Documents¥CS1¥day6> dir
...
...              a1.txt
...
```

演習ガイド: Mac

1. 講義のウェブページから day6.zip 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
2. Terminal を実行
3. Terminal で フォルダ day6 をCS1 に移動
4. day6 フォルダに移動
5. 内容を確認

```
$ cd Documents/CS1
$ mv ~/Downloads/day6 ./
$ cd day6
$ ls
a1.txt      angobunX.txt    h0.txt      kaidoku.py
ango.py     code.py         hukugo.py
```

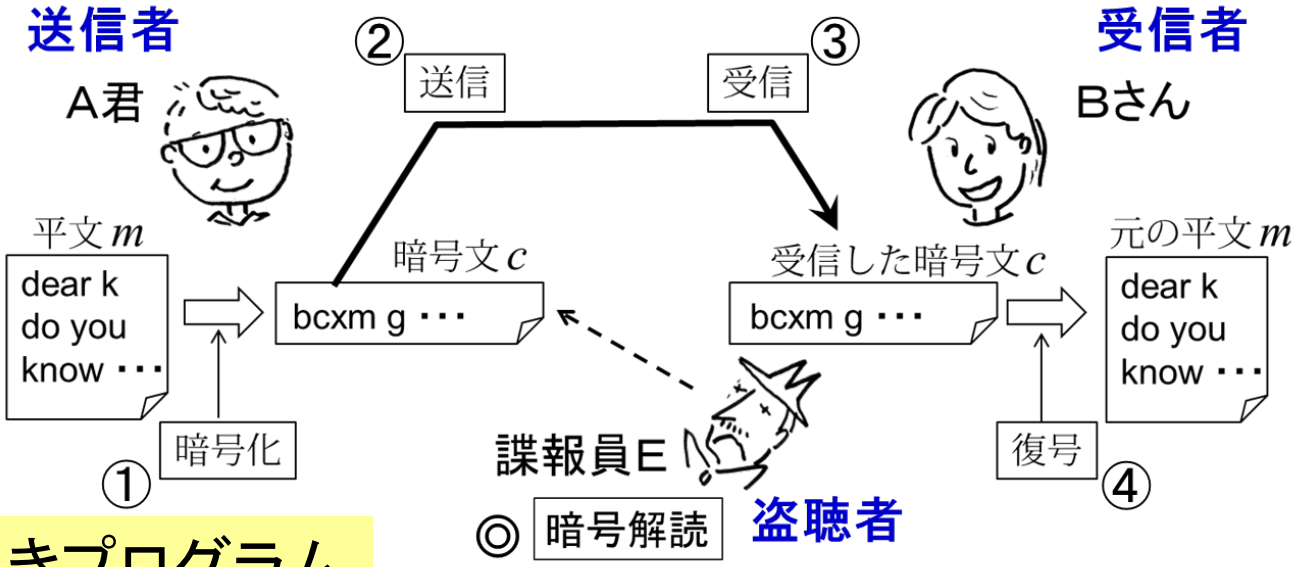
CS第1　レポート課題3

提出方法

- OCWi から提出：11月17日　レポート課題3
- 提出期限： 11月29日 22:00
- 提出物
  - レポート（PDFファイル）: kadai3.pdf
  - 作成したプログラム

CS第1　レポート課題3

課題　暗号解読に挑戦



作成すべきプログラム

1. 復号プログラム hukugo.py
2. 暗号解読プログラム kaidoku.py

（オプショナル）

3 (a) 自分流の暗号方式の myango.py, myhukugo.py
  (b) チャレンジ暗号を解読するための mykaidoku.py

CS第1　レポート課題3

レポートの内容と採点基準（満点 40）

1. 暗号解読プログラムの使い方の説明
2. a1.txt の解読文（最初の1文）
2. 暗号解読プログラムの仕組みの説明（20点，含むプログラム）
   工夫した点も書くこと
3. オプショナル（20点，含むプログラム）
   - 自分独自の暗号方式の提案と暗号化，復号プログラムの説明
   - チャレンジ暗号の解読（そのための補助のプログラムの説明）

採点者は，解読の考え方や計算法は
知らないと想定して説明すること

発展課題(オプショナル)について

(a) 自分流の暗号方式の myango.py, myhukugo.py

- 自分流の方式の提案(チャレンジ暗号とは，異なるもの)
- 暗号化や復号の方法の説明(工夫点など)
- プログラム

(b) チャレンジ暗号を解読するための mykaidoku.py

- チャレンジ暗号 angobunX.txt の解読文(最初の1文)
- どうやって解読したかの説明
  注)適切な説明があればプログラムを使わなくてもOK.
  また，プログラムを道具として使って解読したら点が高い.
- そのために使ったプログラム mykaidoku.py の説明
  (複数のプログラムを使っても良い)

2. 暗号化，復号プログラムの作成

3. 作った ango.py, hukugo.py の使い方

```
$ python ango.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 ango.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 ango.py **<** hirabun.txt **>** angobun.txt

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

3. 解読プログラムのアイデア

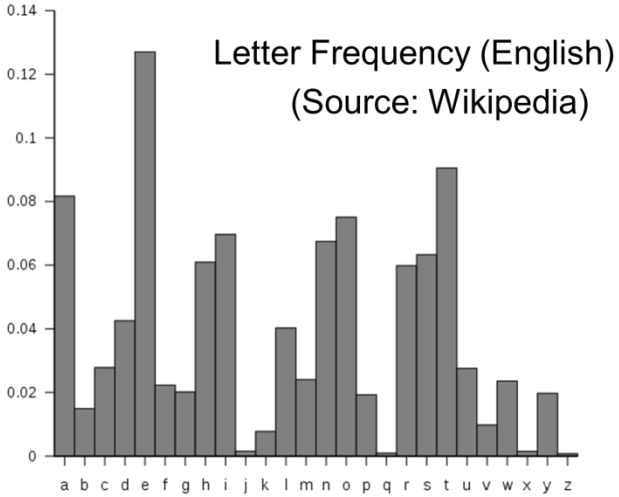
解読 ⟷ 秘密鍵を知らない者が暗号文から平文を得ること

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！



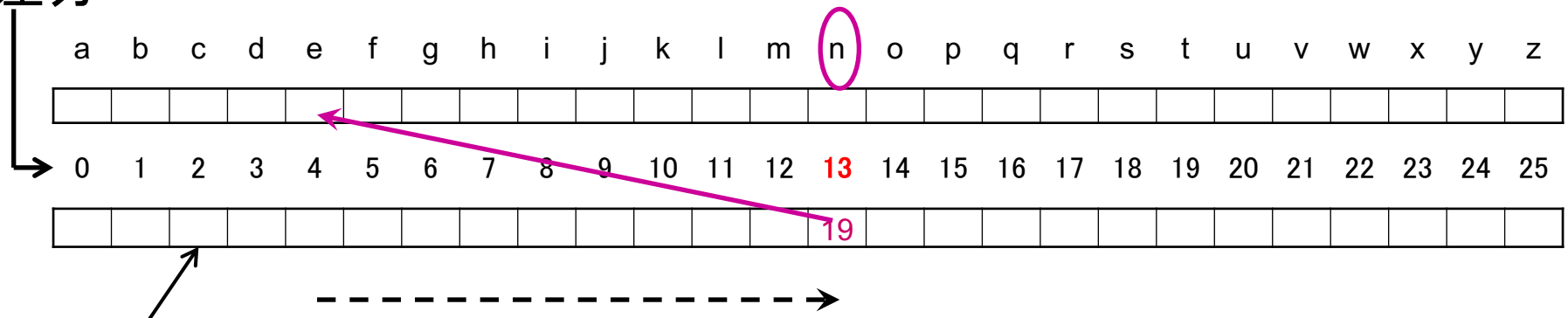
qxuv**n**b qjm k**nn**w b**n**jc**n**m oxa bxv**n** qxdab rw bru**n**wl**n** frcq qrb
uxwp, cqrw kjlt ldae**n**m xe**n**a j lqnvrlju e**n**bb**n**u rw fqrlq q**n**
fjb ka**n**frwp j yjacrldujauh vjuxmxaxdb yaxmdlc. qrb q**n**jm
fjb bdwt dyxw qrb ka**n**jbc, jwm q**n** uxxt**n**m oaxv vh yxrwc xo ...

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 ...

差分

n が19回出現で最多



13−4 = 9 だけずれた ⇒ k = 9

頻度配列と呼ぼう

アイデア

1. 頻度配列 hindo を作る.
2. 最大頻度の場所 maxj を見つける.
3. k = maxj − 4 で求め, dec(k, angobun) で平文を求める.

注意！ maxj < 4 のときも
大丈夫！？

まとめ： Terminal command

命令	使用例	windows	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 ../..	cd ..¥..	上の上のフォルダに戻る
ls	ls	dir	そのフォルダにあるファイルを表示する
rm	rm foo.py	del 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