

CSxxx_C3_12-P

本講義の課題問題

*必須

メールアドレス *

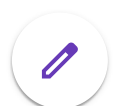
メールアドレス

氏名

回答を入力

学籍番号（例：20B123456, 半角で！）

回答を入力



(1) 以下の暗号解読プログラム cryptanalysis.rb を完成させよ。

```

# definition of subroutine dec(k, c)
def dec(k, c) # k = shift number, c = ciphertext
  # prepare
  code_a = 97
  leng = c.length
  # compute plaintext to m
  a = c.unpack("C*")
  b = Array.new(leng)
  for i in 0..(leng-1)
    dist = a[i] - code_a
    if 0 <= dist && dist <= 25
      (a) ← 小問2の答えを転記
          (変えてもよい)
    else
      b[i] = a[i]
    end
  end
  m = b.pack("C*")
  return m
end

##### program body #####
code_a = 97
ciphertext = gets.chomp
leng = ciphertext.length

# count frequency
aa = ciphertext.unpack("C*")
freq = Array.new(26, 0)
for i in 0..(leng-1)
  dist = aa[i] - code_a
  (b) ← freqの更新(複数行になるは)
end

# compute max_dist
max = 0
max_dist = 0 ← max_distの計算
(c)

# compute k from max_diff
(d) ← kの計算(複数行になってもよい)

# decrypt with the obtained ke
plaintext = dec(k, ciphertext)
puts(plaintext)

```



(a) 各 i 番目の文字（正確には文字コード） $b[i]$ に対しての k シフトの逆計算

回答を入力

(b) 各英小文字の出現頻度 freq の更新

回答を入力

(c) 最頻出文字の diff 値（ここでは, max_diff ）の計算

回答を入力

(d) max_diff から暗号鍵 k の計算

回答を入力

(2) 上記のプログラムに対して暗号鍵（シフト数）23 で作られた暗号文が与えられたとする。その際にプログラム中で変数 max_diff と変数 k に計算される値は、各々いくつになるか？また、 k の値が23だった場合には、 max_diff の値から $k = 23$ をどのように計算したかを説明せよ。一方、 k の値が23でない場合には、なぜその値でよいのかを説明せよ。なお、与えられる暗号文は英文で十分長い文であり、文字 e が最頻出文字種であると仮定しておい。

回答を入力

(3) シーザー暗号と似たような暗号方式（各英小文字を他の文字に変換する暗号方式）で、今回の解読法が通用しないような暗号方式を一つ提案せよ。（アイデアを数行で述べればよい。）

回答を入力



回答のコピーが指定したアドレスにメールで送信されます。

送信

Google フォームでパスワードを送信しないでください。

reCAPTCHA
[プライバシー利用規約](#)

このコンテンツは Google が作成または承認したものではありません。 [不正行為の報告](#) - [利用規約](#) - [プライバシーポリシー](#)

Google フォーム

