PHPゼミ～Caesar暗号解読~

佐々木研究室
06T4073R 三上健太

問題

Caesar暗号を解読するプログラムを作り，暗号を解読せよ

- 暗号鍵(何文字ずらすか)は不明
- 文字列に"person"が含まれていることがわかっている

-暗号文-

qdq-gi.q-a ziatmxxitmdqibtqi-ustbi ri.qmoqrcxi.qbubu
zir -ibtqi-qp-qaai ripmymsqkir -ibtqi-qy dmxi ri.cnxuoi
rruoumxakir -ibtqiqzmobyqzbkii-q.qmxi –imyqzpyqzbi
rixmeaki -puzmzoqai -i-qscxmbu zaimzpir -i btq-
iymbbq-a;iz -iatmxximzgi.q-a zinqiuzimzgiemgipuao-
uyuzmbqpimsmuzabir -ia. za -uzsiacotiimi.qbubu zj

Caesar暗号とは

- 単一換字式暗号の一種
- 平文の各文字を辞書順に何文字かシフトして暗号文をつくる暗号
- 文字のシフト数は固定

- 今回使用する文字は・・・
  "abcdefghijklmnopqrstuvwxyz .,-"の30文字

  ex. "grj"という暗号文を3文字シフト
  grj → fqi → eph → dog
  → これはdogという平文を暗号化したもの

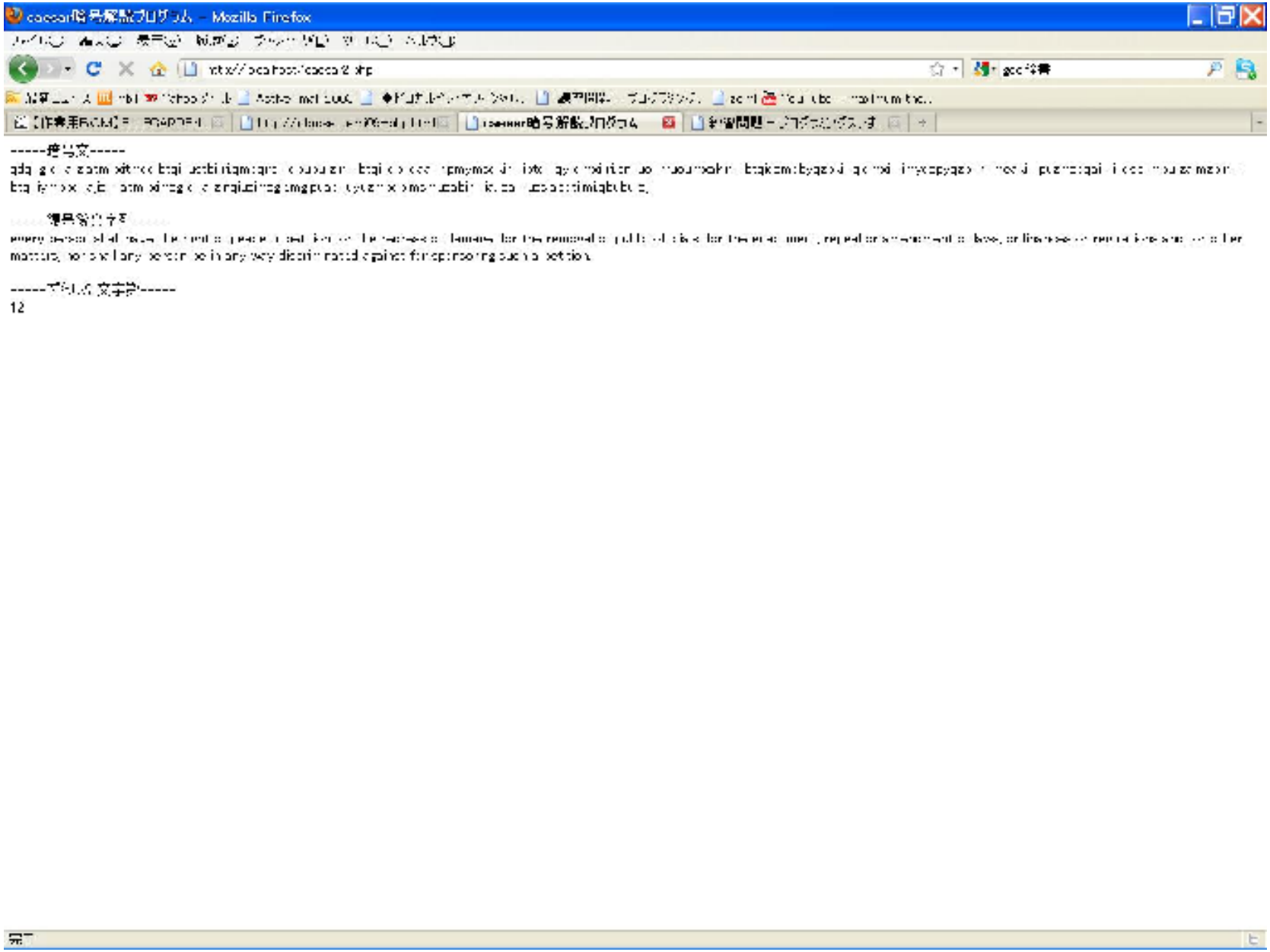
プログラム手順

1. 暗号文配列，置換対象文字配列，置換文字配列をそれぞれ用意する
2. 暗号文の文字列を最初の文字から順にみていく
3. もし暗号文中に置換対象文字が出てきたら置換文字で置き換える
4. 3の処理を暗号文中の全ての文字について行う
5. 2～4の処理を30文字シフトするまで繰り返す(元の暗号文に戻るまで)
6. もし処理途中に"person"という単語が出てきたらそこで処理終了
7. 復号後の文字列とシフト数を表示する

プログラム

```
$count = 0;          #シフト数をカウントする
for($i=0; $i<30; $i++){        #使用する文字分繰り返し
    for($j=0; $j<$length; $j++){         #暗号文の長さ分繰り返し
        for($k=0; $k<count($patterns); $k++){          #対象文字(30文字)分繰り返し
            if( strcmp($arr_word[$j],$patterns[$k])==0 ){  #文字比較
                $arr_word[$j] = $replacements[$k];  #置換を行う
                break;
            }
        }
    }
    $count++;
    $ans = implode("", $arr_word);   #配列要素を連結して文字列に変換
    if( preg_match("/person/", $ans) ){          #文字列に"person"が含まれているか
        echo "-----復号後文字列-----<br>",$ans,"<br><br>";
        echo "-----ずらした文字数-----<br>",$count;
        break;
    }
}
```

実行結果



実行結果(2)

-----暗号文-----

qdq-gi.q-a ziatmxxitmdqibtqi-ustbi ri.qmoqrcxi.qbubu zir -ibtqi-qp-qaai ripmymsqkir -ibtqi-qy dmxi ri.cnxuoi rruoumxakir -ibtqiqzmobyqzbkii-q.qmxi -imyqzpyqzbi rixmeaki -puzmzoqai -i-qscxmbu zaimzpir -i btq-iymbbq-a;iz -iatmxximzgi.q-a zinqiuzimzgiemgipuao-uyuzmbqpimsmuzabir -ia. za -uzsiacotiimi.qbubu zj

-----復号後文字列-----

every person shall have the right of peaceful petition for the redress of damage, for the removal of public officials, for the enactment, repeal or amendment of laws, ordinances or regulations and for other matters; nor shall any person be in any way discriminated against for sponsoring such a petition.

-----ずらした文字数-----

12