Crypto

Lab nr 2
due date 22 III 2015

Assignment 1 (10 pts.) Write a program which takes as an input an encrypted message c and returns a corresponding plaintext m. The message was encrypted with Vigenere's cipher.

For encryption the following piece of code was used:

Listing 1: encrypt.php

```
for ($i = 0; $i < strlen($plaintext); $i++)
        $ciphertext .= $plaintext[$i] ^ $key[$i % $key_length];

foreach (str_split($ciphertext) as $char)
    printf("%02X ", ord($char));
```

How good is your algorithm *i.e.,* what is the minimal length of the message that your program is able to decrypt? How its behaviour depends on the length of the key?