Crypto-Transposition I (Crypto, Trai...) 的解法

原创

滕青山YYDS 于 2021-03-02 12:07:00 发布 55 收藏
文章标签： java

本文链接：https://blog.csdn.net/qq_34626094/article/details/113120661

题目

解密下面的置换密码：

```
oWdnreuf.lY uoc nar ae dht eemssga eaw yebttrew eh nht eelttre sra enic roertco drre . Ihtni koy uowlu dile
```

思考

置换密码就是对明文重新排序以形成密文。

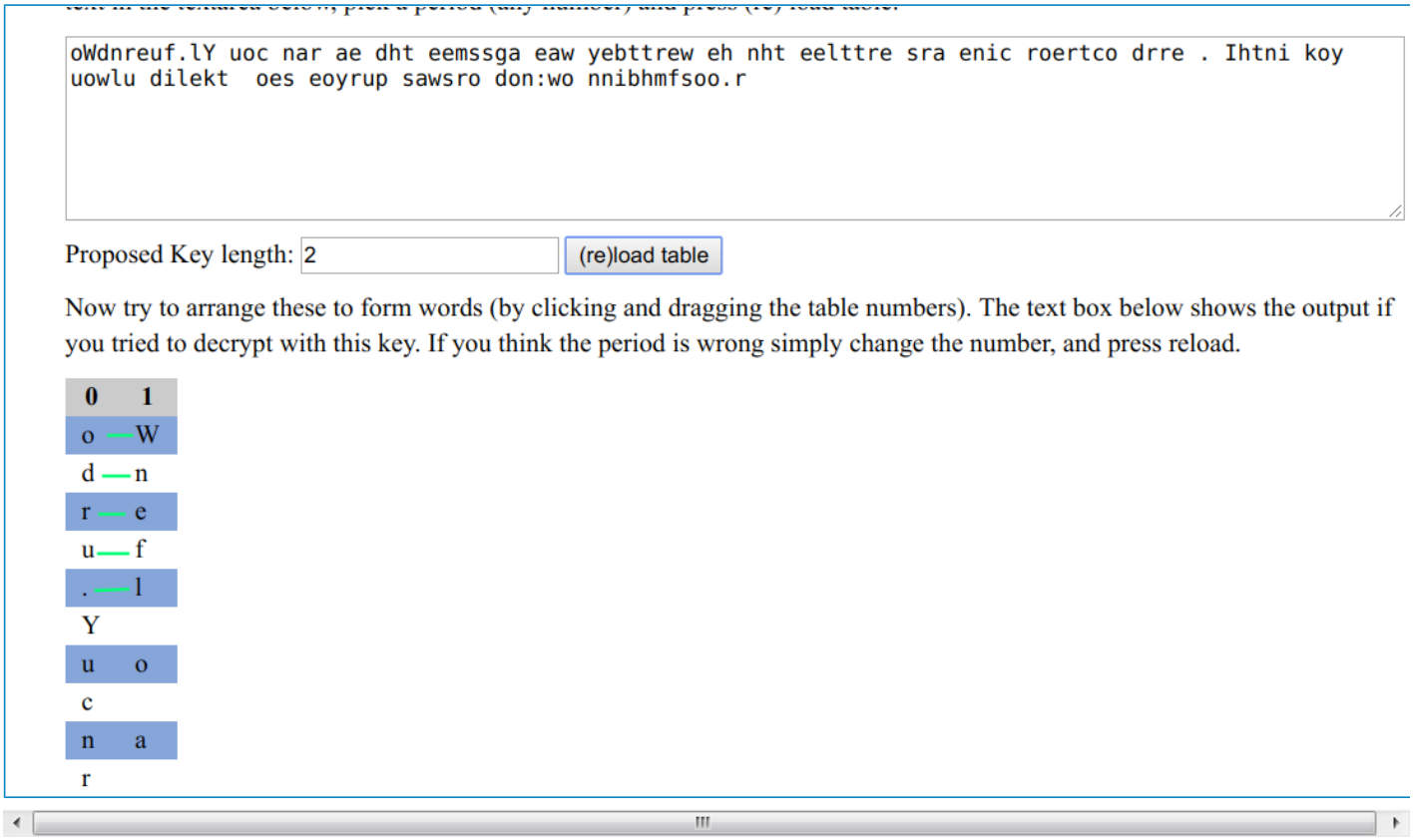
大致过程为：加密，先分组(最后不足补齐)；分别按组进行置换(置换矩阵)。

对待置换密码，首先需要根据其长度特征进行判断分组大小。分组大小是密文长度的因子。

解题

该文本的长度为148，对148求因数是2,2,37。 也就是说分组大小可能是2,2,37。就是说是有4 x 37, 37 x 4, 2 x 74, 74 x 2这么几种情况。

可以用Transposition Cipher Solver来将密码转成矩阵形式。



可以看到：将每两个字符(矩阵的每行)调换一下顺序，就可以还原成明文。例如`oWdnreuf.l`就是`Wonderful.`

用python3来写一下：

```
def decrypto(crypto):
    for i in range(0, len(crypto),2):
        print(crypto[i+1], end="")
        print(crypto[i], end="")
    print()
decrypto("oWdnreuf.lY uoc nar ae dht eemssga eaw yebttrew eh nht eelttre sra enic roertco drre . Ihtni koy
```

运行结果：

```
Wonderful. You can read the message way better when the letters are in correct order. I think you would lik
```

提交`onnbimhsfoor`即可。

更多

在线

到这里来https://www.dcode.fr/transposition-cipher

BY KNOWING THE KEY LENGTH => 选择 4

Bash

创建`ciphertext`文件，内容为

```
oWdnreuf.lY uoc nar ae dht eemssga eaw yebttrew eh nht eelttre sra enic roertco drre . Ihtni koy uowlu dile
```

接着在terminal输入下面命令

```
sed -r -e 's/(.{2})/\1\n/g' ciphertext | sed -r -e 's/(.)(.)/\2\1/g' | tr -d '\n'; echo
```

PHP

```php
<?php
function crypto_trans1_encrypt($pt)
{
    $len = strlen($pt);
    if (($len % 2) == 1) {
        $pt .= 'X';
        $len++;
    }
    $i = 0;
    $ct = '';
    while ($i < $len) {
        $ct .= $pt{$i + 1};
        $ct .= $pt{$i};
        $i += 2;
    }
    return $ct;
}
$ciphertext = "oWdnreuf.lY uoc nar ae dht eemssga eaw yebttrew eh nht eelttre sra enic roertco drre . Ihtni
$plaintext = crypto_trans1_encrypt($ciphertext);
print($plaintext);
?>
```

JavaScript

```javascript
var answer = "oWdnreuf.lY uoc nar ae dht eemssga eaw yebttrew eh nht eelttre sra enic roertco drre . Ihtni
.match(/[\s\S]{1,2}/g)
.map(function(val){
  return val[1]+val[0];
})
.join('');

console.log(answer)
```

C语言

如果用在其他地方，`malloc(200);`中的200可以改大点，以容纳更多字符。

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
char* decrypt(char cryptotext[]){
    int i = 0;
    char *value = malloc(200);
    while (i < strlen(cryptotext)){
        value[i] = cryptotext[i+1];
        value[i+1] = cryptotext[i];
        i += 2;
    }
    value[i] = '\0';
    return value;
}
int main(void)
{
    char cryptotext[] = "oWdnreuf.lY uoc nar ae dht eemssga eaw yebttrew eh nht eelttre sra enic roertco dr
    printf("%s\n", decrypt(cryptotext));
    return 0;
}
```

关于解密置换密码的思路参考了：

Wechall Challenges Writeup & 知识拓展 - 那酷小样的博客 - CSDN博客
Wechall刷题（三）Crypto - Transposition I//The Beginning//hi - leeham的博客 - CSDN博客
WeChall Journal | 陈文青

打