

Звіт лабораторна №2

Для виконання другої лабораторної роботи використовувався Crib Drag Calculator.

Знаючи те, що для шифрування кожного рядку поеми використовувався один і той же ключ, без використання солі, ми можемо його дешифрувати за допомогою Crib Drag method навіть не знаючи ключа.

Це відбувається за наступним алгоритмом:

Для шифрування ми використовуємо One time pad, довжина якого дорівнює довжині ключа.

$\text{PlainText1 XOR RandomKey} = \text{CipherText1}$

$\text{PlainText2 XOR RandomKey} = \text{CipherText2}$

При існуванні тільки одного ключа ми можемо здійснити наступну операцію:

$\text{CipherText1 XOR CipherText2} = (\text{PlainText1 XOR RandomKey}) \text{ XOR } (\text{PlainText2 XOR RandomKey}) = \text{PlainText1 XOR PlainText2}$

Таким чином ми можемо відгадувати частини слів в першому повідомленні, ми автоматично відгадуємо частину, яка знаходиться на тій ж позиції в другому повідомленні.

За допомогою Crib Drag Calculator пробуємо підбирати слова, які можуть зустрітись в зашифрованому тексті. Для вибору слів можна використати список Сводеша для Англійської мови

https://geo.koltyrin.ru/spisok_svodesha.php?jazyk=english.

Після кількох невдалих спроб вдалося знайти частинку оригінального тексту. Для цього було використано слово you(з пробілами навколо)

Crib Drag Calculator

[One-Time Pad \(OTP\)](#) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key.

So what if we use same key to encrypt two message? The ans is we can decrypt them by using Crib Drag method without the shared key. You can read this [blogs](#) for more details.

Ciphertext1 ():

```
ad924af7a9cdaf3a1bb0c3fe1a20a3f36
7d82b0f05f8e75643ba688ea2ce8ec8
8f4762fbe93b50bf5138c7b699
```

Ciphertext2 ():

```
a59a0eaeb4d1fc325ab797b31425e6b
c66d36e5b18efe8060cb32edeaad681
80db4979ede43856a24c7d
```

Character Set:

Click me to show the details

Output 1:

```
..d ris.....
```

Output 2:

```
.. you .....
```

Crib words:

you



Open Grammarly

Result:

- (q+,=
- (=6h<

d ris

output1	output2
output1	output2
output1	output2

Далі перебором слів довжиною 3, що закінчуються на символ “d” було знайдено наступні частини поеми “if you” “and ris”. Продовжуючи такий ж перебір було знайдено “if you can” та “and risk it”, чого було вже достатньо для пошуку даної поеми.

Crib Drag Calculator

[One-Time Pad \(OTP\)](#) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key.

So what if we use same key to encrypt two message? The ans is we can decrypt them by using Crib Drag method without the shared key. You can read this [blogs](#) for more details.

Ciphertext1 ():

```
ad924af7a9cdaf3a1bb0c3fe1a20a3f36
7d82b0f05f8e75643ba688ea2ce8ec8
8f4762fbe93b50bf5138c7b699
```

Ciphertext2 ():

```
a59a0eaeb4d1fc325ab797b31425e6b
c66d36e5b18efe8060cb32edeaad681
80db4979ede43856a24c7d
```

Character Set:

Click me to show the details

Output 1:

and risk it.....

Output 2:

if you can

Crib words:

if you can

Result:

- and risk it

output1	output2
---------	---------
- a"yds&("f:m

output1	output2
---------	---------

Автор даної поеми - Редьярд Кіплінг та назва поеми "if".

Отже, навіть безпечний алгоритм такий як Salsa20 може бути зламаним, якщо використовувати один і той же ключ для шифрування різних повідомлень.