

Lab 2 report

Расшифровка шифротекста в данной лабораторной работе базировалась на идее, что если в ходе шифрования не использовать соль или нонс и использовать один и тот же ключ больше чем 1 раз - то уязвимость алгоритма состоит в следующем (опишу формулами)

$X1 (+) \text{key} = \text{cipherText1}$

$X2 (+) \text{key} = \text{cipherText2}$

$\text{cipherText1} (+) \text{cipherText2} = X1 (+) X2$

далее, зная, что у нас два проксоренных логических текста, мы можем попробовать подобрать слово, которое скорее всего будет в сообщении и пробовать проксорить строки с этим словом. В итоге, если слово таки присутствует в тексте, то сделав ксор с $X1 (+) X2$ мы получим часть логичного текста, который соответствует позиции слова, которое мы продобрали. В после долгих попыток перебирания самых и не самых популярных слов и выбора зазных строк в https://toolbox.lotusfa.com/crib_drag/ я смогла получить две строки, вбив которые в гугл можно получить произведение If Редьярда Киплинга

Ciphertext1 ([Hex]):
ad924af7a9cdf3a1bb0c3e71a27adf3
7fdf3a474dfef44914b17d8ea2cc86c8
9d4d72f9e93556a44d71dfb8980034
b3cea5c4d4

Ciphertext2 ([Hex]):
bd9b1ffcb598e62a5aaa8bf65b0ea7a1
7cde6e4e03f9a64315b07cd7b7ca8b8
6910863e1a8381ea21f38c7f183006df
6c2a5

Character Set: a-zA-Z0-9,?!,:

Click me to show the details

Output 1:
yours

Output 2:
if you.....

Crib words:
if you can take

Result:
• yours is the Bo output1 output2
• `3+e:<0"(&15Hf9#v=)&' output1 output2
• output1 output2

Ciphertext1 ([Hex]):
ad924af7a9cdf3a1bb0c3e71a27adf3
7fdf3a474dfef44914b17d8ea2cc86c8
9d4d72f9e93556a44d71dfb8980034
b3cea5c4d4

Ciphertext2 ([Hex]):
bd9b1ffcb598e62a5aaa8bf65b0ea7a1
7cde6e4e03f9a64315b07cd7b7ca8b8
6910863e1a8381ea21f38c7f183006df
6c2a5

Character Set: a-zA-Z0-9,?!,:

Click me to show the details

Output 1:
yours

Output 2:
if you.....

Crib words:
if you can talk with

Result:
• yours is the Earth an output1 output2
• `3+e:<0"(&15Hf9#v=)&' output1 output2
• h!#':or output1 output2
• bzu0 4:+p/ ~3ojt~'s:* output1 output2