Ощепков Дмитрий Владимирович НКАбд-02-22

Дисциплина: Основы информационной безопасности

Презентация №7

Цель работы: освоить на практике применение режима однократного гаммирования

Порядок выполнения работы:

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.

2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

```python
import random

def encrypt(plaintext, key):
    ciphertext = ''
    for i in range(len(plaintext)):
        # Применяем операцию XOR к ASCII коду символа открытого текста и ключа
        encrypted_char = chr(ord(plaintext[i]) ^ key[i])
        ciphertext += encrypted_char
    return ciphertext

def decrypt(ciphertext, key):
    plaintext = ''
    for i in range(len(ciphertext)):
        # Применяем операцию XOR к ASCII коду символа шифротекста и ключа
        decrypted_char = chr(ord(ciphertext[i]) ^ key[i])
        plaintext += decrypted_char
    return plaintext


def generate_random_key(length):
    return [random.randint(0, 255) for _ in range(length)]  # генерация случайного ключа

# Пример использования:
plaintext = "С Новым Годом, друзья!"

# Генерация случайного ключа той же длины, что и открытый текст
key = generate_random_key(len(plaintext))

# Шифрование
ciphertext = encrypt(plaintext, key)
print("Шифротекст:", ciphertext)

# Дешифрование
decrypted_text = decrypt(ciphertext, key)
print("Дешифрованный текст:", decrypted_text)
```

```
Шифротекст: ѡ)ЄҢIъЧ□ҭӂӓҒC□.æйҸçеЙû
Дешифрованный текст: С Новым Годом, друзья!
```

Вывод: освоил на практике применение режима однократного гаммирования