**Криптографические методы защиты информации**

[Ссылка на код](https://github.com/UsusCimex/NSU_SoftwareEngineering/tree/main/InformationProtection/Cryptographic)

# Поточный шифр RC4

Потоковый шифр: RC4 (Rivest Cipher 4) является симметричным потоковым шифром, который шифрует данные побайтно, генерируя псевдослучайный ключевой поток.

**Ключевое расписание (KSA):**

Инициализация вектора состояния S: Вектор S состоит из 256 элементов (от 0 до 255).

Перемешивание вектора S с использованием ключа:

Проход по всем 256 элементам S.

Вычисление индекса j, основанного на текущем значении S[i] и байтах ключа.

Обмен значениями S[i] и S[j] для создания перестановки элементов вектора S.

**Генерация псевдослучайной последовательности (PRGA):**

Побайтовая генерация ключевого потока:

На каждом шаге инкрементируются индексы i и j.

Выполняется обмен значениями S[i] и S[j].

Выбирается байт ключевого потока K из S[(S[i] + S[j]) % 256].

Длина ключевого потока соответствует длине открытого текста.

**Шифрование и расшифрование:**

Операция XOR: Каждый байт открытого текста шифруется путем выполнения операции исключающего ИЛИ (XOR) с соответствующим байтом ключевого потока.

Симметричность: Процедуры шифрования и расшифрования идентичны; для расшифровки достаточно снова выполнить XOR с тем же ключевым потоком.

**Управление ключами:**

Переменная длина ключа: RC4 поддерживает ключи длиной от 1 до 256 байт, что обеспечивает гибкость в использовании.

**Безопасность ключа:**

Слабости RC4 связаны с определенными шаблонами в выходном ключевом потоке при использовании слабых или предсказуемых ключей.

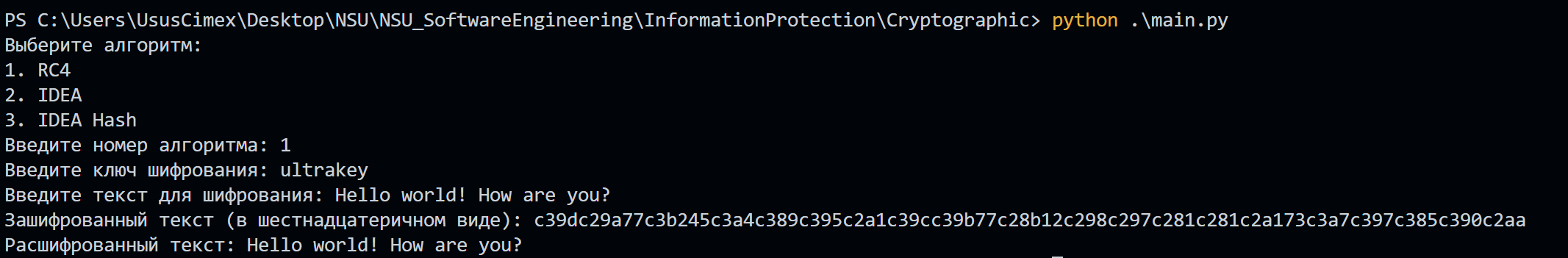
**Применение:**

Широкое использование в прошлом: RC4 был популярен благодаря своей простоте и скорости, использовался в таких протоколах, как WEP и SSL/TLS.

**Уязвимости:**

Известны различные атаки на RC4, особенно при неправильной реализации или использовании, что привело к постепенному отказу от его использования в современных системах безопасности.

**Скриншоты:**

****

# Блочный шифр IDEA

Блоковый шифр: IDEA (International Data Encryption Algorithm) является симметричным блоковым шифром, который оперирует с блоками данных размером 64 бита и использует ключ длиной 128 бит.

**Математические операции:**

Алгоритм основан на комбинации трех основных операций над 16-битными подблоками:

*Сложение по модулю 2^16*

*Побитовое исключающее ИЛИ (XOR)*

*Умножение по модулю 2^16 + 1*

**Структура алгоритма:**

8 основных раундов: Каждый раунд включает в себя серию вышеупомянутых операций, применяемых к подблокам данных и соответствующим субключам.

Выходное преобразование: После 8 раундов выполняется финальное преобразование с использованием оставшихся субключей.

**Генерация субключей:**

Расширение ключа: Исходный 128-битный ключ расширяется до 52 субключей по 16 бит каждый, которые используются в каждом раунде и выходном преобразовании.

Циклический сдвиг: Для генерации субключей используется операция циклического сдвига ключа.

**Шифрование и расшифрование:**

Симметричность операций: Процедуры шифрования и расшифрования очень похожи, различия заключаются в порядке применения субключей и использовании обратных операций (аддитивных и мультипликативных обратных элементов).

Обратные элементы: При расшифровании используются мультипликативные и аддитивные обратные значения субключей шифрования.

**Безопасность:**

Стойкость к криптоанализу: IDEA разработан для обеспечения высокой безопасности и устойчивости к различным видам криптоаналитических атак, включая дифференциальный и линейный криптоанализ.

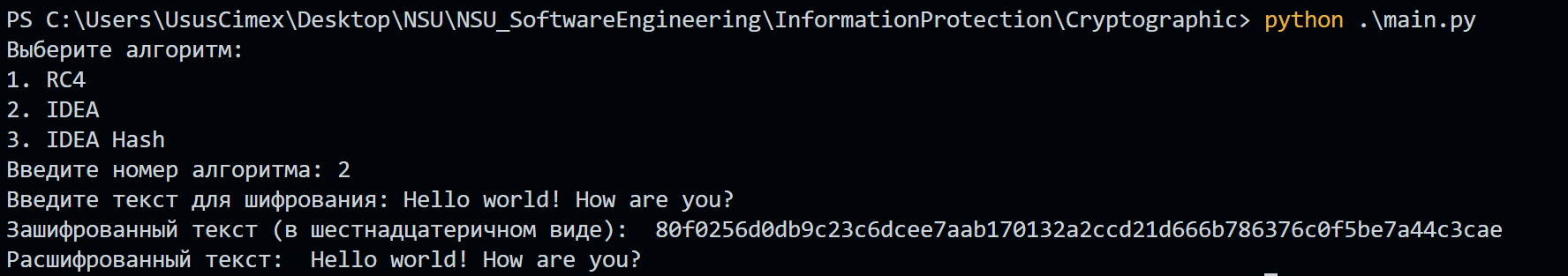
**Дополнение данных (padding):**

PKCS5 Padding: При шифровании данные дополняются до кратности 8 байтам, используя стандарт PKCS5.

**Применение:**

Широкое использование: IDEA использовался в различных криптографических приложениях, включая PGP (Pretty Good Privacy), благодаря своей надежности и эффективности.

**Скриншоты:**



# ХЭШ-функция, основанная на блочном шифре IDEA

Используется конструкция, аналогичная схеме Матьяса-Мейера-Осиаса (Matyas-Meyer-Oseas), где блочный шифр применяется для создания криптографической хэш-функции.

**Скриншоты:**