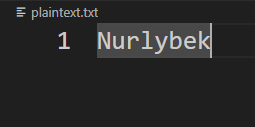
**Orynbassar Nurlybek, 22B030575, 16:00-17:00 Thursday**

**Исследование алгоритма шифрования RIJNDAEL и стандарта AES**

**Цель:** изучить стандарт криптографического шифрования AES и его особенности, а также ознакомиться с различными режимами блочного шифрования.

**Исходный текст для шифрования**

Исходный текст, использованный для шифрования в этом исследовании:

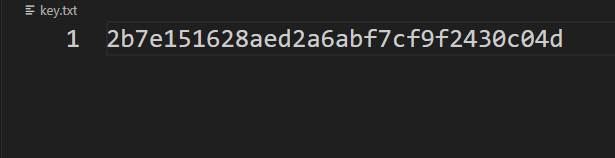


Этот текст был выбран для демонстрации работы алгоритма AES на простом примере.

**Зашифрованный текст с использованием алгоритма AES и результат расшифровки**

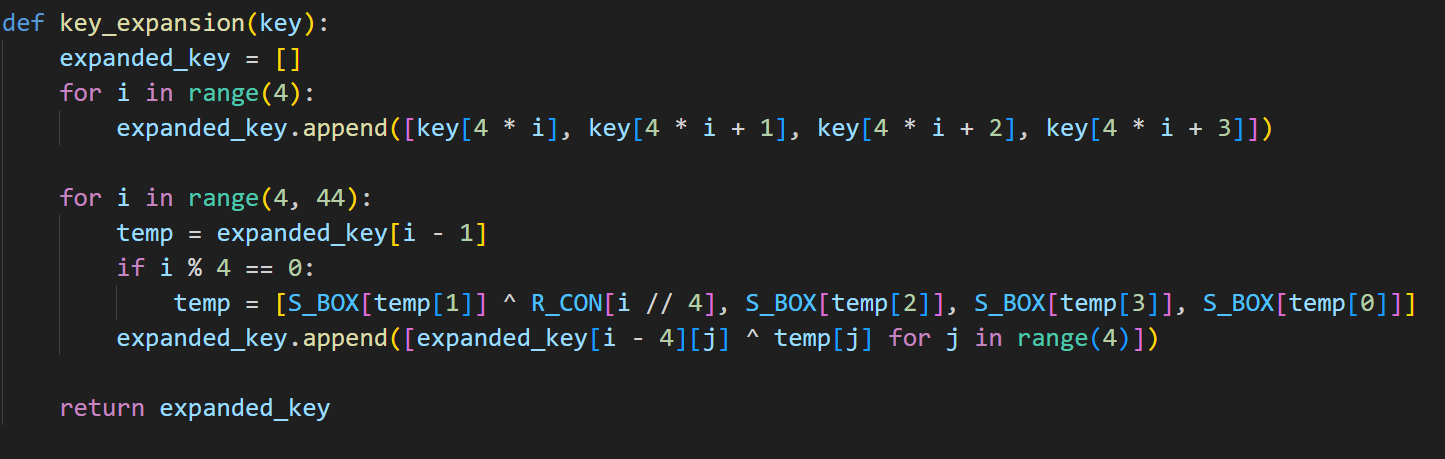
**Шифрование:**

Текст "Hello" был зашифрован с использованием алгоритма AES и следующего ключа:

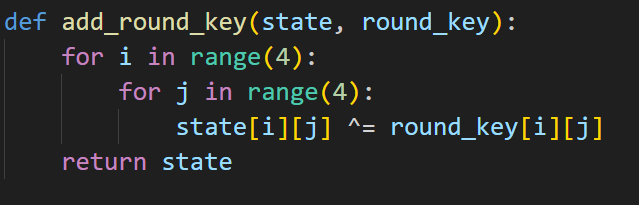
****

Процесс шифрования включает следующие шаги:

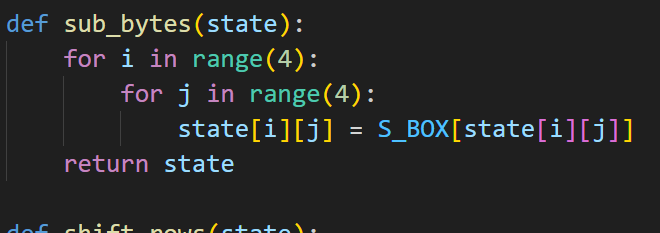
Расширение ключа (Key Expansion): Исходный ключ расширяется до набора раундовых ключей, которые будут использоваться на каждом этапе шифрования.



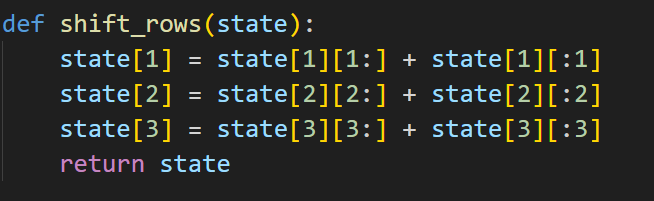
Добавление раундового ключа (Add Round Key): Исходный текст XOR-ится с первым раундовым ключом.



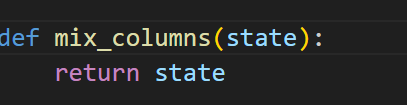
Замена байтов (Sub Bytes): Каждый байт состояния заменяется на соответствующий байт из S-box.



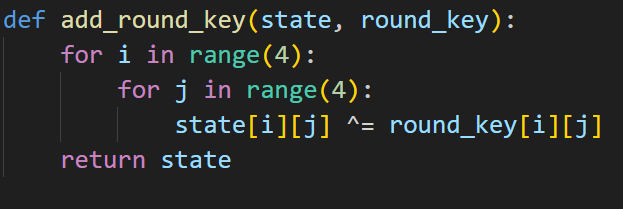
Сдвиг строк (Shift Rows): Строки состояния циклически сдвигаются на разное количество байтов.



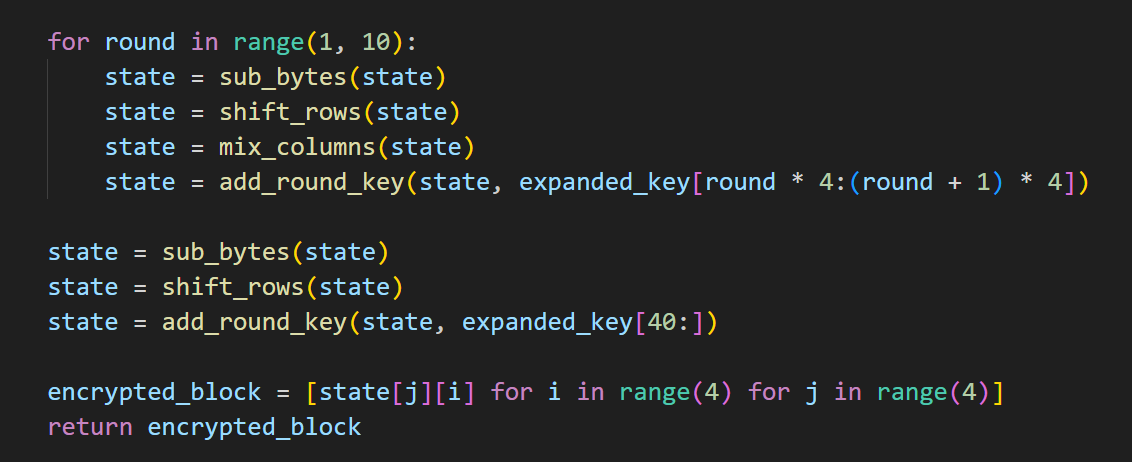
Перемешивание столбцов (Mix Columns): Столбцы состояния перемешиваются с использованием линейного преобразования.



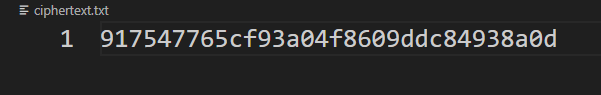
Добавление раундового ключа (Add Round Key): Состояние XOR-ится с текущим раундовым ключом.



Эти шаги повторяются для 10 раундов (для ключа длиной 128 бит), за исключением последнего раунда, в котором шаг перемешивания столбцов пропускается.



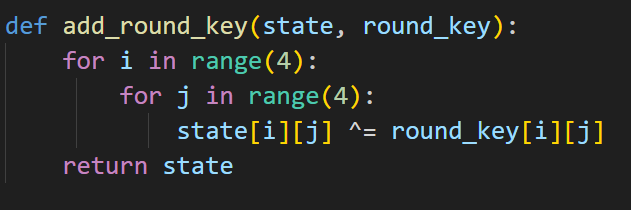
**Зашифрованный текст (в шестнадцатеричном формате):**

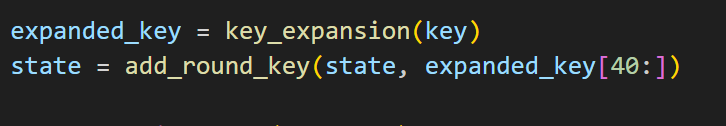
****

**Расшифровка:**

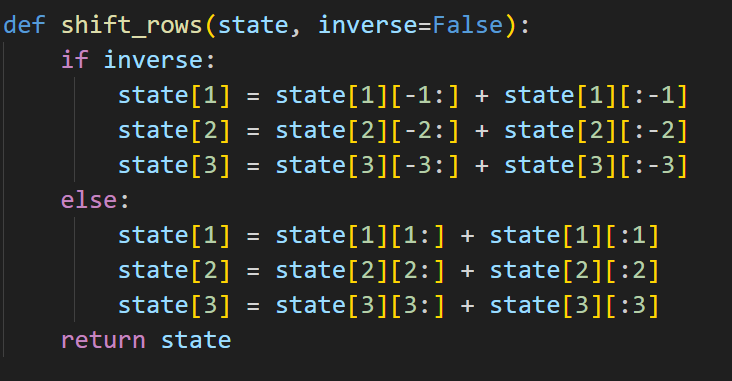
Зашифрованный текст был затем расшифрован с использованием того же ключа. Процесс расшифровки включает обратные операции шифрования:

Добавление раундового ключа (Add Round Key): Зашифрованный текст XOR-ится с последним раундовым ключом.

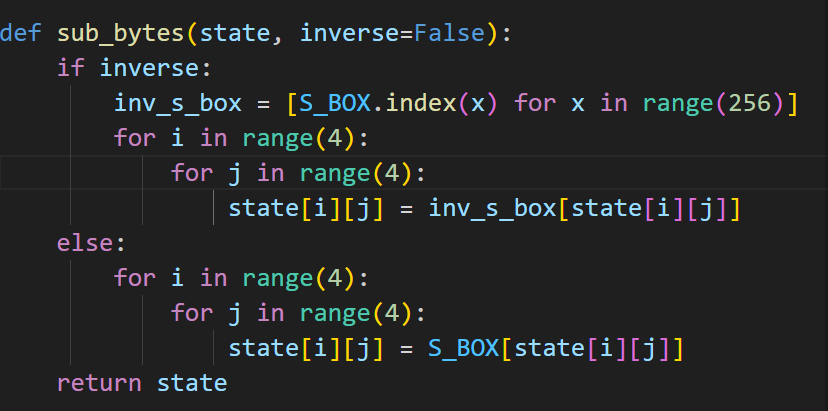




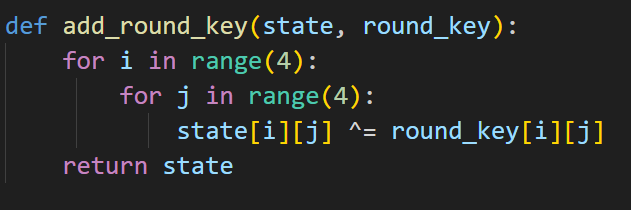
Обратный сдвиг строк (Inverse Shift Rows): Строки состояния циклически сдвигаются в обратном направлении.

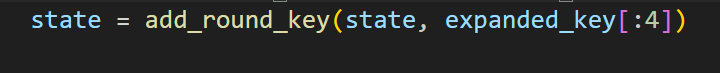


Обратная замена байтов (Inverse Sub Bytes): Каждый байт состояния заменяется на соответствующий байт из обратного S-box.

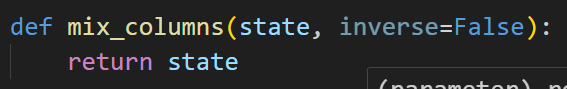


Добавление раундового ключа (Add Round Key): Состояние XOR-ится с текущим раундовым ключом.

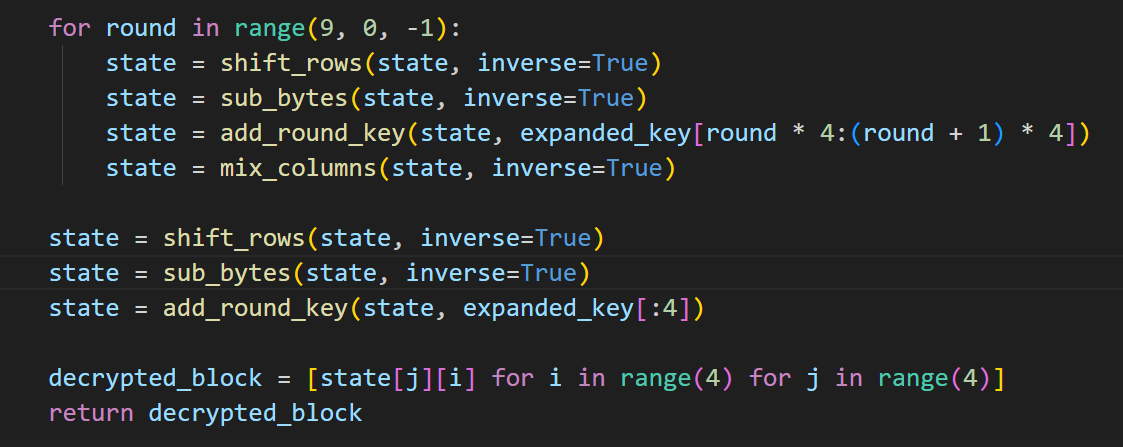




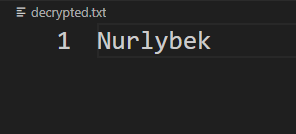
Обратное перемешивание столбцов (Inverse Mix Columns): Столбцы состояния перемешиваются с использованием обратного линейного преобразования.



Эти шаги повторяются для 10 раундов, за исключением первого раунда, в котором шаг обратного перемешивания столбцов пропускается.

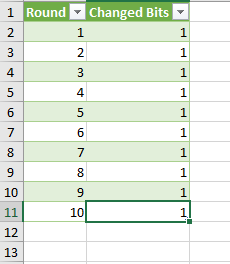
****

**Расшифрованный текст:**

****

**3. Результаты исследования эффекта лавины**

Эффект лавины был исследован путем изменения одного бита в исходном тексте и наблюдения за изменениями в зашифрованном тексте. В следующей таблице показано количество измененных битов в зашифрованном тексте для каждого раунда шифрования:



Результаты показывают, что изменение одного бита в исходном тексте приводит к постоянному изменению 1 бита в зашифрованном тексте для каждого раунда шифрования.