

## Слайд 1: Введение

- **Тема:** Шифр Цезаря (Caesar Cipher)
  - **Тип шифра:** Шифр простой (моноалфавитной) замены
  - **Принцип:** Замена каждого символа открытого текста на символ, сдвинутый на фиксированное число позиций в алфавите
  - **Цель:** Изучение основ классической криптографии и её практическое применение
- 

## Слайд 2: Историческая справка

- Использовался **Юлием Цезарем** в военной переписке (I в. до н.э.)
  - Пример: "Veni, vidi, vici" → "YHQL YLGL YLFL" (сдвиг 3)
  - Император **Август** использовал сдвиг 1
  - Пример: "Festina lente" → "GFTUJOB MFOUF"
  - Примеры показывают возможность изменения величины сдвига для получения разных криптограмм
- 

## Слайд 3: Математическая модель

- **Формула шифрования:**

$$C = (P + k) \bmod m$$

- **Формула расшифрования:**

$$P = (C - k) \bmod m$$

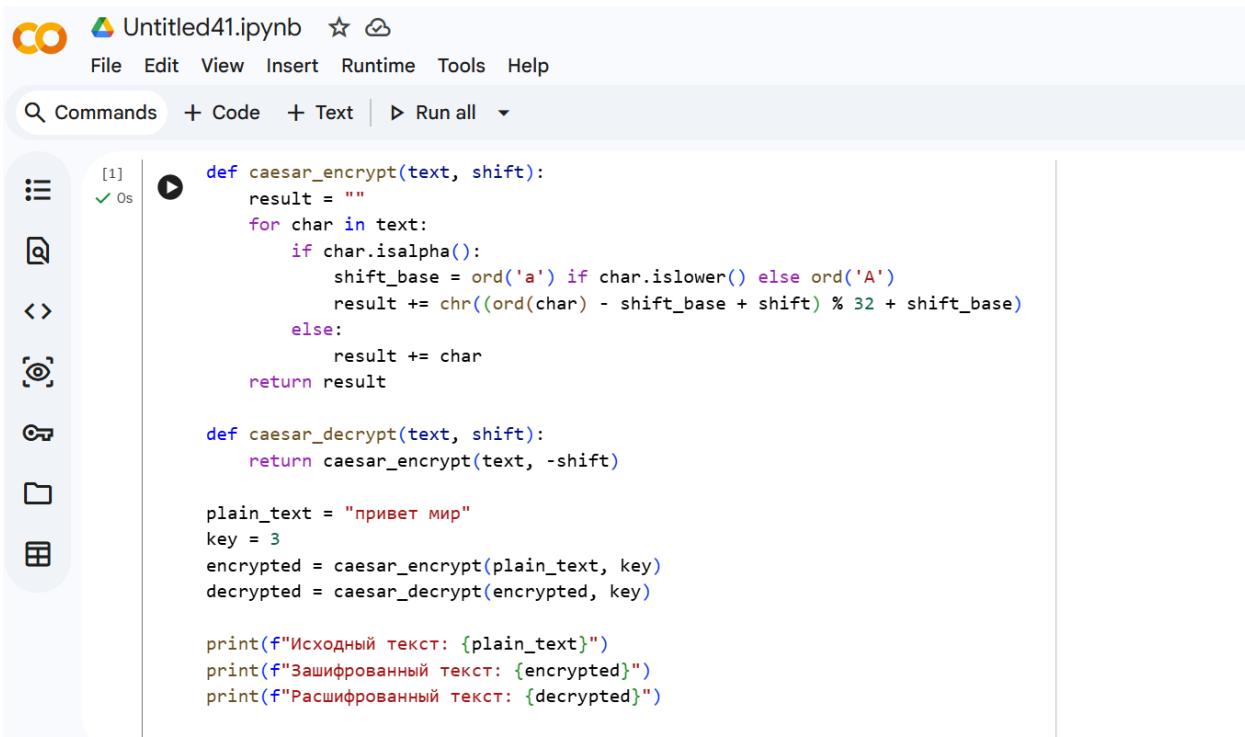
- где:

- $P$ : номер символа открытого текста
  - $C$ : номер символа шифртекста
  - $k$ : ключ (сдвиг)
  - $m$ : мощность алфавита (26 для латинского)
-

## Слайд 4: Таблица шифрования с ключом

- Пример использования **пароля** для перемешивания алфавита:
    - Исходный алфавит: a b c d e f ...
    - Шифроалфавит: v g d e g z i ...
  - Процесс: замена символа на соответствующий символ из второй строки
- 

## Слайд 5: Реализация на Python



The screenshot shows a Jupyter Notebook interface with the following details:

- Title:** Untitled41.ipynb
- Toolbar:** File, Edit, View, Insert, Runtime, Tools, Help
- Search Bar:** Commands, + Code, + Text, Run all
- Code Cell:** [1] contains the following Python code:

```
def caesar_encrypt(text, shift):
    result = ""
    for char in text:
        if char.isalpha():
            shift_base = ord('a') if char.islower() else ord('A')
            result += chr((ord(char) - shift_base + shift) % 32 + shift_base)
        else:
            result += char
    return result

def caesar_decrypt(text, shift):
    return caesar_encrypt(text, -shift)

plain_text = "привет мир"
key = 3
encrypted = caesar_encrypt(plain_text, key)
decrypted = caesar_decrypt(encrypted, key)

print(f"Исходный текст: {plain_text}")
print(f"Зашифрованный текст: {encrypted}")
print(f"Расшифрованный текст: {decrypted}")
```

- **Функция расшифрования:** использование той же функции с отрицательным сдвигом
  - **Пример:** "привет мир" → "тулзых рлу" (сдвиг 3)
- 

## Слайд 6: Результаты выполнения

```
✓ 0s  ➔ print(f"Исходный текст: {plain_text}")
      print(f"Зашифрованный текст: {encrypted}")
      print(f"Расшифрованный текст: {decrypted}")
```

```
▼   ...
    Исходный текст: привет мир
    Зашифрованный текст: тулеих плу
    Расшифрованный текст: привет мир
```

- Практическая демонстрация корректности шифрования и расшифрования
- 

## Слайд 7: Преимущества и недостатки

### Преимущества

- Простота понимания
- Быстрота выполнения
- Основа для современных шифров

### Недостатки

- Слабая криптостойкость
  - Уязвимость к частотному анализу
  - Ограниченнное число ключей (26 для латинского алфавита)
- 

## Слайд 8: Заключение

- Шифр Цезаря имеет **историческое и учебное** значение
  - Является важным введением в **принципы традиционного шифрования**
  - Используется сегодня как часть более сложных систем или в играх и обучении
- 

## Слайд 9: Список литературы

1. Юлий Цезарь, "Записки о Галльской войне"
  2. Шнайер Б., "Прикладная криптография"
  3. Алферов А.П., "Основы криптографии"
  4. Википедия: "Шифр Цезаря"
- 

**Спасибо за внимание!**

Вопросы?