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:**

$$C = (P + k) \mathrm{mod}\ m$$

- **Формула расшифрования:**

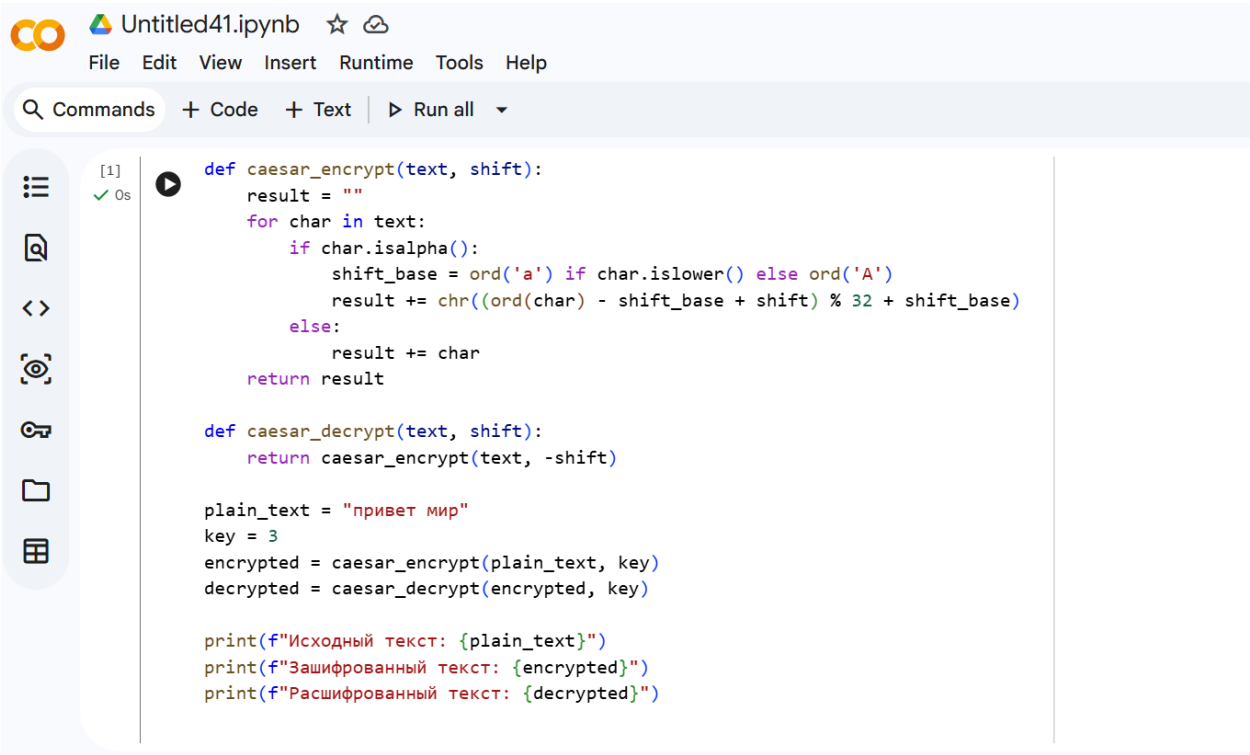
$$P = (C - k) \mathrm{mod}\ m$$

- 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

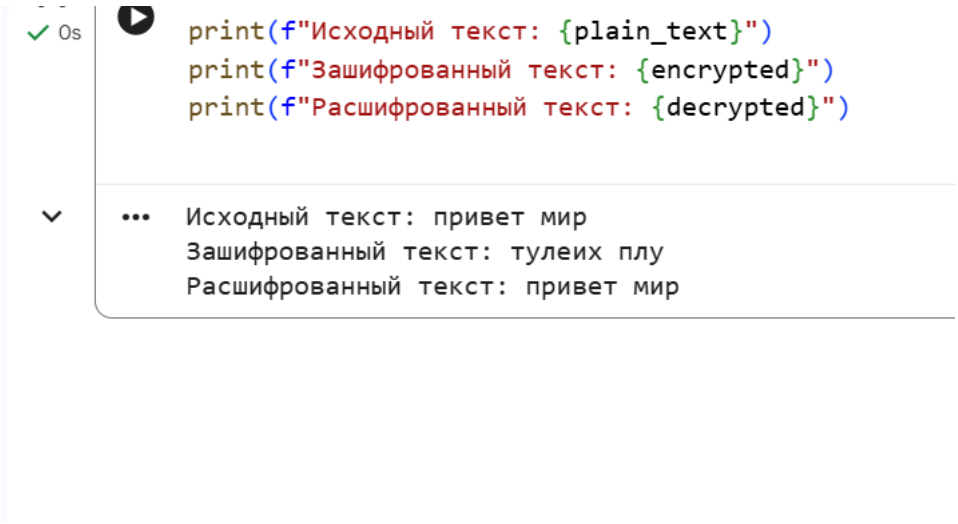
- Пример использования **пароля** для перемешивания алфавита:
    - Исходный алфавит: a b c d e f ...
    - Шифроалфавит: v g d e g z i ...
- Процесс: замена символа на соответствующий символ из второй строки

Слайд 5: Реализация на Python



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

Слайд 6: Результаты выполнения



- Практическая демонстрация корректности шифрования и расшифрования

Слайд 7: Преимущества и недостатки

Преимущества	Недостатки
- Простота понимания	- Слабая криптостойкость
- Быстрота выполнения	- Уязвимость к частотному анализу
- Основа для современных шифров	- Ограниченное число ключей (26 для латинского алф

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?