**Шифрование данных**  
  
  
  
  
  Колоев Ренат

Арутюнов Давид

Кудзиев Валерий

учащийся 7 класса,  Государственного

 бюджетного образовательного учреждения

республиканский физико – математический

 лицей – интернат, г. Владикавказ,

РСО- Алания

Научный руководитель:

 Зеньков Александр Игоревич,

 учитель информатики Государственное

 бюджетное образовательное учреждение

 республиканский физико - математический

лицей – интернат, г. Владикавказ,

РСО- Алания

**Аннотация**

В проекте изучены и реализованы основные алгоритмы шифрования: AES, RSA, DES, 3DES и ECC. Рассмотрены их принципы работы, преимущества и недостатки, а также области применения. В ходе работы создана программа для шифрования и дешифрования данных, позволяющая на практике протестировать выбранные методы. Проект демонстрирует, как работают современные криптографические алгоритмы и в чем их отличие, а также подчеркивает их значимость для защиты информации.

### Оглавление

1. **Введение**
   * Актуальность работы
   * Обоснование выбора темы
2. **Цель и задачи работы**
   * Цель проекта
   * Основные задачи
3. **Основная часть**
   * Методика выполнения работы
   * Выбор алгоритмов шифрования
   * Описание алгоритмов (AES, RSA, DES, 3DES, ECC)
   * Реализация алгоритмов
4. **Результаты, анализ и оценка**
5. **Выводы**
6. **Практическая значимость проекта**
7. **Список использованной литературы**

### Введение

Шифрование данных является одним из ключевых методов обеспечения информационной безопасности. В современном мире информация передается и хранится в цифровом виде, что делает ее уязвимой к атакам злоумышленников. Для защиты данных используются различные криптографические алгоритмы, такие как симметричное и асимметричное шифрование.

Целью данной работы является изучение, анализ и реализация популярных криптографических алгоритмов, что позволит глубже понять их принципы работы и определить наиболее подходящие методы защиты информации.

### Цель и задачи работы

**Цель:**

* Изучить и реализовать основные алгоритмы шифрования для понимания их механики и оценки их эффективности.

**Задачи:**

* Исследовать современные алгоритмы шифрования.
* Изучить понятие криптостойкости алгоритмов.
* Выделить и изучить наиболее распространенные алгоритмы: AES, RSA, DES, 3DES, ECC.
* Реализовать алгоритмы на Python и C++ для тестирования их работы.
* Провести анализ их эффективности и применимости в различных сферах.

### Основная часть

**Методика выполнения работы**  
Проект включает в себя теоретическое исследование криптографических алгоритмов, их классификацию и практическую реализацию на языках программирования Python и C++. В ходе работы использовались стандартные криптографические библиотеки и математические принципы, применяемые в шифровании.

**Выбор алгоритмов шифрования**  
В работе рассматриваются как симметричные, так и асимметричные алгоритмы:

* **AES (Advanced Encryption Standard)** – один из наиболее распространенных алгоритмов симметричного шифрования.
* **RSA (Rivest-Shamir-Adleman)** – асимметричный алгоритм, используемый для шифрования данных и цифровых подписей.
* **DES (Data Encryption Standard)** – устаревший, но значимый алгоритм симметричного шифрования.
* **3DES (Triple DES)** – усовершенствованный вариант DES с троекратным шифрованием.
* **ECC (Elliptic Curve Cryptography)** – криптографический метод, основанный на эллиптических кривых, обладающий высокой стойкостью при меньшей длине ключа.

**Описание алгоритмов**

1. **AES** – блочный симметричный алгоритм с ключами длиной 128, 192 или 256 бит, использует замену, перемешивание и раундовые преобразования.
2. **RSA** – основан на трудности разложения больших чисел на множители, использует пары открытых и закрытых ключей.
3. **DES** – блочный алгоритм с длиной ключа 56 бит, ныне признан недостаточно стойким.
4. **3DES** – усовершенствованная версия DES, применяющая тройное шифрование для повышения безопасности.
5. **ECC** – метод, использующий эллиптические кривые, обеспечивает высокий уровень защиты при меньших размерах ключей по сравнению с RSA.

### Результаты, анализ и оценка

В результате работы были реализованы все указанные алгоритмы, проведено их тестирование и анализ. Было установлено, что AES обеспечивает высокую скорость работы и безопасность, RSA удобен для передачи ключей, но требует значительных вычислительных ресурсов. DES и 3DES показали устаревшие характеристики, а ECC оказался перспективным благодаря высокой криптостойкости при небольших вычислительных затратах.

### Выводы

* Современные криптографические алгоритмы различаются по степени защиты, скорости работы и применимости.
* AES остается одним из самых надежных симметричных алгоритмов.
* RSA широко применяется в цифровых подписях, но требует больших ресурсов.
* DES и 3DES устарели и используются ограниченно.
* ECC показывает отличные результаты и перспективен в условиях ограниченных вычислительных мощностей.

### Практическая значимость проекта

Данный проект помогает лучше понять, как работают основные криптографические алгоритмы, и дает возможность применять их в реальных задачах. Реализованные решения могут использоваться в обучении, тестировании и разработке новых систем шифрования.

### Список использованной литературы

1. Menezes A., van Oorschot P., Vanstone S. **Handbook of Applied Cryptography**. CRC Press, 1996.
2. Stallings W. **Cryptography and Network Security: Principles and Practice**. Pearson, 2016.
3. Schneier B. **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. John Wiley & Sons, 1995.
4. FIPS PUB 197. **Advanced Encryption Standard (AES)**. National Institute of Standards and Technology (NIST), 2001.
5. Diffie W., Hellman M. **New Directions in Cryptography**. IEEE Transactions on Information Theory, 1976.
6. Koblitz N. **Elliptic Curve Cryptosystems**. Mathematics of Computation, 1987.
7. <https://habr.com/ru/articles/745820/>