УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КЛАССИЧЕСКИХ И КВАНТОВЫХ МЕТОДОВ ШИФРОВАНИЯ

А.Ю. Ефремова, А.Н. Морозова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В представленной статье проведен сравнительный анализ классических и квантовых методов шифрования, с указанием их индивидуальных особенностей. Классические методы, такие как симметричное и ассиметричное шифрование, широко используются в современных системах безопасности, однако они подвержены угрозам взлома, связанным с развитием вычислительных технологий. В то же время квантовые методы шифрования, основанные на принципах квантовой механики, предлагают новые уровни безопасности благодаря использованию кубитов и явлению квантовой запутанности. Сравнительный анализ проводился по следующим показателям: скорости шифрования, сложности реализации, возможности применения, уязвимости к атакам, стоимости реализации.
Ключевые слова: безопасность данных; шифрование; классические методы шифрования; симметричное шифрование; ассиметричное шифрование; квантовая криптография; параметры; сравнительный анализ.

COMPARATIVE ANALYSIS OF CLASSICAL ENCRYPTION AND QUANTUM ENCRYPTION METHODS

A.Y. Yafremava, A.N. Morozova
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In the presented article, a comparative analysis of classical and quantum encryption methods is conducted, highlighting their individual characteristics. Classical methods, such as AES and RSA, are widely used in modern security systems; however, they are susceptible to threats associated with the advancement of computational technologies. At the same time, quantum encryption methods, based on the principles of quantum mechanics, offer new levels of security through the use of qubits and the phenomenon of quantum entanglement. The comparative analysis is carried out based on the following criteria: encryption speed, implementation complexity, application possibilities, vulnerability to attacks, and implementation cost.
Keywords: encryption, data security; threat of hacking; comparative analysis, classical encryption methods, symmetric encryption; asymmetric encryption; quantum cryptography; quantum key distribution; quantum mechanics.

Введение

Вопрос безопасности в современном мире, где комфортную жизнь нельзя представить без обмена данными, занимает главенствующую роль. Большая часть этих данных содержит конфиденциальную информацию, распространение которой может нанести значительный ущерб. Для предотвращения распространения конфиденциальной информации используются специализированные системы

шифрования, гарантирующие, что доступ к этим данным смогут иметь только пользователям, обладающим ключами шифрования.

На протяжении многих лет использовались классические методы шифрования, так как они были в значительной степени эффективны, однако эти методы бессильны против квантовой угрозы. В таком случае наиболее верным решением станет использование квантовой криптографии.

В данной статье будут рассмотрены основные отличия классических методов шифрования от квантовых. В качестве сравниваемых параметров рассматриваются скорость шифрования, сложность реализации, возможности применения, уязвимость к атакам, а также стоимость реализации.

Основная часть

Под классическим шифрованием понимают совокупность методов шифрования, использующих простые алгоритмы и ключи для преобразования открытого текста в зашифрованный. В основе классического шифрования заложены методы, которые использовались еще до появления современных компьютерных алгоритмов. Среди таких шифров можно выделить шифр Цезаря (метод заключается в сдвиге алфавита на фиксированное число позиций), шифр Виженера (метод, в котором применяется ключевое слово для управления сдвигами), шифр *Playfair* (шифр, использующий квадрат символов 5×5 для шифрования биграмм), шифр транспозиции (шифр, использующий перестановку символов в тексте согласно определенной схеме, не изменяя сами символы), а также уже известное шифрование с использованием ключей.

Классические методы шифрования включают в том числе и симметричное и ассиметричное шифрование. Симметричное шифрование является фундаментальным методом, в котором для преобразования данных применяется один и тот же ключ. К наиболее известным алгоритмам симметричного шифрования обычно относят *DES* (относительно устаревший, использует ключ в 56 бит), *Triple DES* (улучшенная версия *DES*, использующая три итерации шифрования), *AES* (более безопасный по сравнению с *Triple DES*, поддерживающий ключи длинной в 128, 192 и 256 бит).

Симметричное шифрование позволяет быстро обрабатывать большие объемы данных, требуя при этом меньше вычислительных ресурсов. Несмотря на относительно невысокий уровень безопасности, симметричное шифрование широко используется для защиты файлов и данных на жестких дисках (*BitLocker*), передачи данных через защищенные каналы (*SSL/TLS*), а также для *VPN* соединений.

Асимметричное шифрование – это более сложный метод шифрования, который использует два ключа: открытый (публичный) и закрытый (приватный). Использование двух ключей обеспечивает высокий уровень безопасности, а также является основой многих современных систем. Открытый ключ используется для шифрования данных и находится в открытом доступе для пользователей, отправляющих зашифрованное сообщение. Закрытый ключ используется для расшифровки полученных данных и известен только владельцу.

Методы ассиметричного шифрования просты в реализации. Виду отсутствия необходимости передачи секретного ключа, риск его компрометации значительно снижен. В отличие от симметричного шифрования, асимметричное требует больше времени на обработку, что делает его менее подходящим для шифрования больших объемов данных. Высокий уровень безопасности позволяет применять ассиметричное шифрование во многих сферах, например, для создания и проверки цифровых подписей, подтверждающих подлинность сообщений, и в протоколах передачи, таких как SSL/TLS. Квантовое шифрование, также называемое квантовой криптографией, –

это метод шифрования, основанный на использовании квантовых битов для передачи и защиты информации с высоким уровнем безопасности [1].

Для квантового шифрования характерны следующие принципы: квантовая суперпозиция, принцип неопределенности и квантовая запутанность.

Целью квантовой криптографии является защита данных от квантовых угроз. Квантовая криптография, также называемая квантовым шифрованием, использует свойства квантовой механики для обеспечения безопасности данных. Квантовая криптография использует непредсказуемость природы материи на квантовом уровне для шифрования и дешифрования сообщений, что обеспечивает более высокий уровень безопасности. Информация в классических методах шифруется в битах, в то время как в квантовой криптографии используются кубиты.

Наиболее известным примером квантовой криптографии является квантовое распределение ключей (КРК), позволяющее двум сторонам обмениваться данными безопасно, значительно снижая риски взлома. В отличие от других методов, квантовое распределение ключей позволяет взаимодействующим сторонам обнаружить попытки перехвата сообщения за счет ввода ошибок в структуру кубитов при попытке взлома или измерения данных. Кроме того, квантовая криптография теоретически устойчива к увеличению мощности квантовых вычислений.

При этом, каналы связи квантового распределения ключей требуют тщательной настройки и надлежащего набора аппаратного обеспечения, такого как оптоволоконные соединения и фотонные излучатели для передачи и приема зашифрованных данных. В масштабах предприятия создание инфраструктуры для КРК может обойтись в несколько миллионов долларов, при этом для внедрения необходимы специализированные аппаратные каналы [2, 3].

Подробное сравнение методов шифрования представлено в таблице 1.

Таблица 1. Сравнительный анализ классических и квантовых методов шифрования
Table 1. Comparative Analysis of Classical and Quantum Encryption Methods

Характеристика	Классические методы шифрования	Квантовые методы шифрования
1	2	3
Скорость шифрования	150 Кбит –1 Гбит/с	1–10 Мбит/с
Сложность реализации	Необходимость в специализированном оборудовании присутствует только в случае повышения производительности. Необходимость в специализированной среде отсутствует. Достаточными являются общие знания о криптографии и управлении ключами.	Необходимость в специализированных устройствах (квантовые источники фотонов, детекторы и оптические волокна). Необходимость в специализированной инфраструктуре – надежной оптической сети. Необходимость в глубоких знаниях в области квантовой механики.
Возможности применения	Используется для шифрования различных объемов данных, таких как файлы, сетевые потоки, ключи шифрования и цифровые подписи.	Используется для защиты транзакций, обеспечения безопасности в чувствительных операциях, защиты данных в корпоративных сетях, обеспечения безопасности при подключении к сети и для защиты систем управления и мониторинга.

Продолжение таблицы 1
Continuation of table 1

1	2	3
Уязвимость к атакам	Методы уязвимы к следующим атакам: атака по шифротексту, атака по открытому тексту, атака на ключ, атака на алгоритм, атака на временные уязвимости, атака на подмену ключа. Менее безопасный вид шифрования.	Методы уязвимы к следующим атакам: атаки на источник квантовых битов, атаки на каналы передачи, атаки на протоколы, шум и потери в канале, атаки при помощи квантовых компьютеров. Более безопасный вид шифрования.
Стоимость реализации	Стоимость реализации варьируется в зависимости от метода, однако затраты сравнительно небольшие ввиду возможности реализации на стандартном оборудовании.	Для реализации требуются значительные инвестиции ввиду затрат на оборудование, развивающиеся технологии, а также обучение сотрудников.

Заключение

Исходя из данных в таблице видно, что классические методы шифрования остаются актуальными для защиты многих типов данных, но их уязвимость к атакам делает их менее перспективными для крупных систем с оборотом конфиденциальных данных. Квантовые методы шифрования обеспечивают высокий уровень безопасности благодаря уникальным свойствам квантовой механики, однако их реализация требует специализированного оборудования и знаний. Таким образом, выбор между этими методами зависит от конкретных требований безопасности и доступных ресурсов.

Список использованных источников

1. Алефиренко В.М., Ефремова А.Ю., Асиненко А.М. (2024) Анализ современных подходов к классификации методов шифрования. *SCIENCE TIME* (12), 45–50.
2. Stefano D.L., Tristan M., Samy C. (2024) Cryptographic security: Critical to Europe's digital sovereignty *European Parliamentary Research Service*. (11), 1–8.
3. Danda B.R., Kayhan Z.G. (2018) Smart Cities Cybersecurity and Privacy. USA. Washington.

References

1. Alefirenko V.M., Yafremava A.Y., Asinenko A.M. (2024) Analysis of Modern Approaches to the Classification of Encryption Methods. *SCIENCE TIME* (12), 45–50 (in Russian).
2. Stefano D.L., Tristan M., Samy C. (2024) Cryptographic security: Critical to Europe's digital sovereignty *European Parliamentary Research Service*. (11), 1–8.
3. Danda B.R., Kayhan Z.G. (2018) Smart Cities Cybersecurity and Privacy. USA. Washington.

Сведения об авторах

Ефремова А.Ю., ассистент кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», al617e13@gmail.com.
Морозова А.Н., магистрант кафедры проектирования информационно-компьютерных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», annamorozova417@gmail.com.

Information about the authors

Yafremava A.Y., Assistant Professor of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", al617e13@gmail.com
Morozova A.N., Master's degree student of the Electronic Technique and Technology Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", annamorozova417@gmail.com.