УДК 004.056

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Р.Д. Осипов, П.Б. Гусаков
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В условиях цифровой трансформации защита информации становится критически важной для обеспечения конфиденциальности, целостности и доступности данных. Криптография играет ключевую роль в создании безопасных коммуникационных каналов и защите персональных данных. В данной статье рассматриваются основные принципы криптографии, современные алгоритмы шифрования и актуальные вызовы, включая угрозы, связанные с развитием квантовых компьютеров.

Анализируются способы применения криптографических методов в различных сферах, таких как финансовая система, государственные структуры и интернет вещей (IoT).
Ключевые слова: Цифровая трансформация; криптография; шифрование; конфиденциальность; целостность; аутентификация; квантовые компьютеры; интернет вещей; цифровая экономика; безопасность данных.

CRYPTOGRAPHIC INFORMATION PROTECTION

R.D. Osipov, P.B. Gusakov
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. In the era of digital transformation, information protection becomes critically important for ensuring the confidentiality, integrity, and availability of data. Cryptography plays a key role in creating secure communication channels and protecting personal data. This article discusses the basic principles of cryptography, modern encryption algorithms, and current challenges, including threats related to the development of quantum computers. The article also analyzes the application of cryptographic methods in various fields, such as the financial system, government structures, and the Internet of Things (IoT).
Keywords: Digital transformation; cryptography; encryption; confidentiality; integrity; authentication; quantum computers; Internet of Things; digital economy; data security

Введение

В условиях цифровой трансформации защита информации становится критически важной для обеспечения конфиденциальности, целостности и доступности данных. Криптография, как наука о методах шифрования, играет ключевую роль в создании безопасных коммуникационных каналов, защите персональных данных и предотвращении кибератак. Сегодня она применяется повсеместно: от мессенджеров и онлайн-банкинга до государственных систем управления и IoT-устройств. В данной работе рассматриваются основные принципы криптографии, современные алгоритмы, а также актуальные вызовы, связанные с развитием технологий.

Основная часть

Криптография не только обеспечивает защиту данных, но и способствует развитию цифровой экономики, защищая транзакции, персональные данные и интеллектуальную собственность. В эпоху больших данных и интернета вещей (IoT) криптографические методы становятся неотъемлемой частью технологической инфраструктуры. Однако с развитием технологий возникают новые угрозы, такие как квантовые компьютеры, которые могут поставить под угрозу существующие криптографические системы.

Криптография имеет многовековую историю. Еще в Древнем Египте и Месопотамии использовались простые шифры для защиты важных сообщений. Значительный вклад в развитие криптографии внесли такие методы, как шифр Цезаря, который применялся в Римской империи и заключался в сдвиге букв на фиксированное число позиций. Этот метод, несмотря на свою простоту, стал основой для более сложных алгоритмов.

Особое место в истории криптографии занимает роторная машина «Энигма», использовавшаяся Германией во Второй мировой войне. Ее взлом группой Алана Тьюринга стал поворотным моментом в истории криптоанализа. Это событие не только изменило ход войны, но и заложило основы для развития современных компьютеров.

В середине XX века появление компьютеров значительно ускорило развитие криптографии. Симметричные алгоритмы, такие как DES, разработанный в 1970-х

годах, заложили основу для современных стандартов шифрования. DES стал первым широко используемым алгоритмом, одобренным правительством США. Эволюция криптографии тесно связана с прогрессом в математике и компьютерных технологиях, что позволило перейти от простых замен к сложным алгоритмам, устойчивым к атакам.

Криптография базируется на трех ключевых принципах: конфиденциальность, целостность и аутентификация. Конфиденциальность обеспечивает доступ к данным только авторизованным сторонам. Это достигается за счет шифрования, которое делает информацию недоступной для посторонних. Целостность гарантирует отсутствие несанкционированных изменений. Хеш-функции и цифровые подписи позволяют обнаружить любые попытки изменения данных. Аутентификация подтверждает подлинность источника данных, что важно для предотвращения атак, таких как подмена личности (spoofing).

Основными компонентами криптографии являются шифрование, дешифрование и ключи. Шифрование – это процесс преобразования открытого текста в зашифрованный (шифротекст). Дешифрование – обратный процесс. Ключи – это секретные параметры, определяющие алгоритм преобразования.

Существуют различные типы криптосистем. Симметричные системы, такие как AES и DES, используют один ключ для шифрования и дешифрования. Их преимущество заключается в высокой скорости, но они сталкиваются с проблемой управления ключами. Асимметричные системы, такие как RSA и ECC, используют пару ключей (публичный и приватный). Они решают проблему распределения ключей, но требуют больше вычислительных ресурсов. Хеш-функции, такие как SHA-256, преобразуют данные в уникальную строку фиксированной длины и используются для проверки целостности.

Современная криптография предлагает широкий спектр методов для защиты данных. Одним из наиболее популярных симметричных алгоритмов является AES (Advanced Encryption Standard), принятый в 2001 году. Он использует ключи длиной 128, 192 или 256 бит и широко применяется в VPN, Wi-Fi сетях (WPA2/WPA3) и защите файлов. AES считается одним из самых безопасных алгоритмов благодаря своей устойчивости к атакам.

Для асимметричного шифрования часто используется алгоритм RSA, основанный на сложности факторизации больших чисел. Он применяется для цифровых подписей и обмена ключами. Однако с развитием квантовых компьютеров RSA становится уязвимым. В качестве альтернативы используется ECC (Elliptic Curve Cryptography), который обеспечивает аналогичную безопасность при меньшей длине ключа. Например, 256 бит ECC эквивалентны 3072 бит RSA. Это делает ECC особенно полезным для IoT-устройств и блокчейн-технологий, таких как Bitcoin и Ethereum.

Квантовая криптография набирает популярность в свете развития квантовых компьютеров. Протоколы, такие как BB84, используют законы квантовой механики для обнаружения подслушивания. Квантовая криптография обеспечивает абсолютную безопасность, основанную на принципах квантовой физики.

Постквантовая криптография становится важным направлением исследований. Алгоритмы, такие как NTRU и McEliece, устойчивы к атакам на квантовых компьютерах. Они активно разрабатываются и стандартизируются организациями, такими как NIST.

Криптография находит применение в различных сферах. В финансовой сфере она используется для защиты онлайн-платежей через TLS-шифрование и EMV-чипы в банковских картах. Криптография защищает миллиарды транзакций ежедневно.

В государственных системах криптография обеспечивает защиту гостайн и используется для электронной подписи. Например, в России применяется стандарт ГОСТ Р 34.10-2012.

С ростом числа подключенных устройств в рамках интернета вещей (IoT) криптография становится критически важной для защиты данных. Она используется для шифрования данных с датчиков и аутентификации устройств.

В блокчейн-технологиях криптография обеспечивает работу смарт-контрактов и защиту транзакций. Например, в Ethereum используется алгоритм ECDSA для цифровых подписей.

Современная криптография сталкивается с рядом вызовов и угроз, которые требуют постоянного внимания и адаптации. Одной из наиболее серьезных угроз является развитие квантовых компьютеров. Эти устройства, основанные на принципах квантовой механики, способны решать задачи, которые классическим компьютерам недоступны. В частности, квантовые компьютеры могут взломать многие из существующих криптографических алгоритмов, таких как RSA и ECC, за счет использования алгоритма Шора. Это ставит под угрозу безопасность данных, защищенных этими методами. В ответ на эту угрозу активно разрабатываются постквантовые криптографические алгоритмы, которые устойчивы к атакам с использованием квантовых вычислений.

Еще одной значительной проблемой является социальная инженерия. Даже самая надежная криптосистема становится уязвимой, если пользователь по неосторожности передаст свои ключи или пароли злоумышленнику. Фишинговые атаки, мошенничество и другие методы социальной инженерии продолжают оставаться эффективными, поскольку они эксплуатируют человеческий фактор, а не технические уязвимости.

Законодательные ограничения также представляют собой вызов для криптографии. В некоторых странах правительства требуют от разработчиков предоставления "бэкдоров" – специальных механизмов, позволяющих обходить шифрование для целей национальной безопасности. Однако такие требования создают риски, поскольку бэкдоры могут быть использованы не только государственными органами, но и злоумышленниками.

Атаки сторонних каналов (side-channel attacks) – еще одна серьезная угроза. Эти атаки не направлены на взлом самого алгоритма шифрования, а используют косвенные данные, такие как время выполнения операций, энергопотребление или электромагнитное излучение, чтобы извлечь секретные ключи. Защита от таких атак требует разработки специализированных методов, которые минимизируют утечку информации через сторонние каналы.

Наконец, рост числа подключенных устройств в рамках интернета вещей (IoT) создает новые вызовы для криптографии. Многие IoT-устройства имеют ограниченные вычислительные ресурсы, что затрудняет использование традиционных криптографических методов. Кроме того, недостаточное внимание к безопасности в процессе разработки таких устройств делает их уязвимыми для атак.

Заключение

Криптография остается краеугольным камнем информационной безопасности, однако ее развитие требует постоянной адаптации к новым технологическим и социальным вызовам. Внедрение постквантовых алгоритмов, повышение осведомленности пользователей и укрепление международного сотрудничества

в области стандартизации – ключевые направления для обеспечения безопасности данных в будущем.

Криптография продолжает развиваться, и ее роль в защите данных будет только возрастать. В условиях глобальной цифровизации и увеличения числа кибератак криптографические методы становятся неотъемлемой частью технологической инфраструктуры. Будущее криптографии связано с разработкой новых алгоритмов, устойчивых к квантовым атакам, а также с интеграцией криптографических методов в новые технологии, такие как искусственный интеллект и квантовые сети.

Список использованных источников

1. Мартынов Л. М. Алгебра и теория чисел для криптографии. М.: Лань. 2024. 456 с.
2. Омассон Жан-Филипп. О криптографии всерьез. Практическое введение в современное шифрование. М.: ДМК Пресс. 2021. 328 с.
3. Применко Э. А., Борисов А. В. Алгебраические основы криптографии в задачах и упражнениях. Учебное пособие. М.: КУРС. 2023. 104 с.
4. Рацеев С. М. Математические методы защиты информации и их основы. Сборник задач. М.: Лань. 2023. 140 с.

References

1. Martynov L. M. Algebra and Number Theory for Cryptography. Moscow: Lan, 2024. 456 pages.
2. Omasson Jean-Philippe. Serious Cryptography: A Practical Introduction to Modern Encryption. Moscow: DMK Press. 2021. 328 pages.
3. Primenko E. A., Borisov A. V. Algebraic Foundations of Cryptography in Problems and Exercises. Textbook. Moscow: KURS. 2023. 104 pages.
4. Ratseev S. M. Mathematical Methods of Information Protection and Their Foundations. Collection of Problems. Moscow: Lan. 2023. 140 pages.

Сведения об авторах

Осипов Р.Д., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», osipovr695@gmail.com.
Гусаков П.Б., магистр, начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», p.gusakov@bsuir.by.

Information about the authors

Osipov R.D., Cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", osipovr695@gmail.com
Gusakov P.B., Master, Head of the Cycle, Educational Institution "Belarusian State University of Informatics and Radioelectronics", p.gusakov@bsuir.by.