ЭВОЛЮЦИЯ МЕТОДОВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Г.Г. Коновалов, *студент*
Д.А. Бощенко, *студент*
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2025-10-2-55-59

Аннотация. *В статье рассматривается эволюция методов криптографической защиты информации – от древних шифров до современных постквантовых алгоритмов. Показаны основные этапы развития криптографии: использование простых подстановочных систем в античности и Средневековье, появление механических и электромеханических устройств в Новое время, переход к симметричным алгоритмам в эпоху вычислительной техники, революция асимметричной криптографии. Отдельное внимание уделено открытиям квантовой эпохи и перспективам развития постквантовых методов защиты.*

Ключевые слова: *криптография, шифрование, симметричные алгоритмы, асимметричные алгоритмы, RSA, AES, электронная подпись, квантовые вычисления, постквантовая криптография, информационная безопасность.*

В настоящее время информация превратилась в один из краеугольных ресурсов, от сохранности и конфиденциальности которой зависят безопасность государства, бизнеса и личная жизнь каждого человека. По мере стремительного роста цифровых технологий, усиления глобализационных процессов и расширения сетей коммуникаций вопрос защиты информации обрел особую актуальность. Кибератаки, нелегальный доступ и утечки данных каждый раз напоминают, насколько критически важны надёжные методы защиты информации.

Криптография – это область, изучающая способы трансформации данных, позволяющие скрыть их смысл и вместе с тем гарантировать подлинность. Сквозь тысячелетия методы шифрования информации постепенно менялись – от простейших подстановочных схем и громоздких механических устройств до изощрённых математических алгоритмов, лежащих в основе современных стандартов информационной безопасности.

Истоки криптографии

Криптография имеет глубокие исторические корни. Первые попытки сокрытия смысла сообщений относятся ещё к древним цивилизациям, когда возникла необходимость сохранять тайну военной или дипломатической переписки. Несмотря на примитивность методов, именно тогда были заложены основы, которые впоследствии привели к формированию современных систем защиты данных.

Одним из самых ранних известных способов шифрования является «шифр Цезаря», использовавшийся в Древнем Риме. Его суть заключалась в том, что каждая буква исходного текста заменялась на другую, отстоящую от неё в алфавите на фиксированное число позиций. Простота метода делала его легко реализуемым, но вместе с тем и уязвимым для дешифрования.

Другим интересным примером криптографии античных времён является спартанская скитала – деревянный цилиндр, на который наматывалась узкая полоска пергамента. Сообщение писалось вдоль поверхности цилиндра, и только при намотке на такой же стержень текст можно было прочитать[4]. Данный метод нельзя назвать стойким по современным меркам, но он является примером использования физического устройства в криптографическом процессе.

В Средние века криптография получила новое развитие благодаря арабским учёным. Персидский математик аль-Кинди описал методы частотного анализа, показав, что устойчивость простых подстановочных шифров невелика. Этот шаг стал важной вехой в истории, он положил начало систематическому подходу к взлому шифров и развитию криптоанализа как науки.

В Европе позднего Средневековья и раннего Нового времени шифры начали широко использоваться в дипломатической переписке. Применялись более сложные подстановочные системы, появлялись первые попытки полиафавитных шифров. Одним из наиболее известных примеров стал шифр Виженера, основанный на последовательном использовании нескольких алфавитов. На протяжении нескольких столетий он считался практически неразрушимым и получил название «le chiffre indéchiffrable» - «неразгаданный шифр» [7].

Криптография в новое время

С наступлением Нового времени начался новый виток развития криптографии, связанный с усложнением государственных и военных структур, ростом дипломатических связей и необходимостью более надёжной защиты информации. Если в древности и Средневековье преобладали простые шифры подстановки и перестановки, то в XVII-XIX веках начали появляться механические устройства и более сложные системы, обеспечивавшие повышенную стойкость.

Одним из первых примеров можно назвать дисковые шифры, предложенные в XVI веке. Такие устройства позволяли менять алфавиты подстановки, что значительно усложняло задачу для криптоаналитиков. В дальнейшем эта идея была развита в «цилиндре Джэффферсона» – механическом шифраторе, состоявшем из набора вращающихся дисков с алфавитами [7]. При правильной настройке он позволял формировать различные комбинации подстановок и считался достаточно надёжным для своего времени.

Ключевым этапом в развитии криптографии стало появление электромеханических шифровальных машин. Наиболее известной из них является немецкая «Энигма», созданная в 1920-х годах. Она использовала систему роторов, которые при каждом нажатии клавиши изменяли схему подстановки, благодаря чему каждый символ шифровался уникальным образом. «Энигма» широко применялась германскими вооружёнными силами во время Второй мировой войны и долгое время считалась неуязвимой [4].

Однако, усилия криптоаналитиков, в том числе работа А. Тьюринга и его коллег, показали, что даже столь сложные системы могут быть взломаны с помощью математического анализа и специальных методов. Успешное дешифрование сообщений, передаваемых с помощью «Энигмы», сыграло значительную роль в исходе войны, став одним из важнейших примеров практического значения криптографии и криптоанализа.

Переход к компьютерной эре

С середины XX века криптография вступила в новый этап развития, тесно связанный с появлением электронных вычислительных машин. Если ранее основой защиты были механические и электромеханические устройства, то теперь криптографические методы стали базироваться на математических алгоритмах, которые реализовывались средствами компьютерной техники. Этот период стал переходным от традиционной к современной криптографии.

Первоначально большинство систем строилось на принципах симметричного шифрования, где для зашифрования и расшифрования использовался один и тот же секретный ключ. Классическим примером является DES (Data Encryption Standard), разработанный в США в 1970-е годы и утверждённый Национальным институтом стандартов и технологий (NIST) в качестве федерального стандарта. DES представлял собой блочный шифр с длиной ключа 56 бит, что на момент его появления обеспечивало высокий уровень защиты [5].

В Советском Союзе был создан собственный алгоритм симметричного шифрования – ГОСТ 28147-89, утверждённый в 1989 году. Он имел структуру, схожую с DES, но отличался более длинным ключом (256 бит), что значительно увеличивало стойкость. Этот стандарт применялся для защиты информации в государственных и военных системах и стал важным этапом в развитии отечественной криптографии [6].

Несмотря на значительный прогресс, у симметричных систем существовали объективные недостатки. Главная проблема заключалась в распределении ключей: обе стороны должны были заранее договориться о секретном ключе, причём его передача по незащищённым каналам ставила под угрозу безопасность всей системы.

Кроме того, с развитием вычислительной техники возросла угроза полного перебора ключей (brute force). Если в 1970-х годах

взлом DES считался практически невозможным, то к концу 1990-х годов появились специализированные машины, способные за считанные часы проверить все варианты 56-битного ключа. Это стало сигналом к поиску новых решений и модернизации алгоритмов.

В этот же период активно развивались потоковые шифры, где данные зашифровывались по одному символу или биту за раз с использованием псевдослучайной последовательности. Такие методы обеспечивали высокую скорость обработки информации и нашли применение в телекоммуникациях и радиосвязи.

Революция асимметричной криптографии

Появление асимметричной криптографии стало настоящей революцией в области защиты информации. Если симметричные методы требовали наличия общего секретного ключа у обеих сторон, то асимметричная система позволила преодолеть этот барьер. Ключевая идея заключалась в разделении ключей на два: «открытый» (public key) и «закрытый» (private key). Открытый ключ мог свободно распространяться, а закрытый оставался известен только владельцу. Сообщение, зашифрованное открытым ключом, можно было расшифровать только с помощью соответствующего закрытого, и наоборот.

Этот подход был предложен в 1976 году Уитфилдом Диффи и Мартином Хеллманом. Их работа ввела понятие «обмена ключами по открытому каналу» – процедуру, при которой две стороны могли безопасно договориться о секретном ключе, не передавая его напрямую [7]. Метод Диффи-Хеллмана стал первым практическим алгоритмом, использующим свойства труднорешаемых математических задач. Его устойчивость базировалась на сложности вычисления дискретного логарифма в больших числовых полях.

Вскоре после этого, в 1977 году, Рональд Ривест, Ади Шамир и Леонард Адлеман предложили алгоритм, получивший название «RSA» по инициалам его создателей. Он стал первым полноценным шифром с открытым ключом, пригодным для широкого применения. Безопасность RSA основана на сложности факторизации больших чисел: разложение произведения двух больших простых чисел на множители является крайне ресурсоёмкой задачей для классических компьютеров [4]. Этот алгоритм быстро получил распространение, став основой для многих стандартов и протоколов.

Развитие асимметричных методов не ограничилось методом Диффи-Хеллмана и RSA. В 1980-е годы внимание исследователей привлекли так называемые «эллиптические кривые». Алгоритмы на их основе (ECC – Elliptic Curve Cryptography) обеспечивали сопоставимый уровень безопасности при значительно меньшей длине ключа. Например, ключ ECC длиной 256 бит по стойкости соответствует ключу RSA длиной порядка 3072 бит [5]. Это сделало эллиптические кривые особенно привлекательными для мобильных и встроенных систем, где важны скорость вычислений и экономия ресурсов.

Асимметричная криптография также породила такие явления, как электронная цифровая подпись (ЭЦП). С её помощью можно не только подтвердить подлинность автора сообщения, но и гарантировать целостность данных.

С распространением интернета асимметричная криптография стала неотъемлемым элементом защиты сетевых коммуникаций. Протоколы SSL/TLS, обеспечивающие безопасность веб-сайтов, используют гибридный подход: асимметричные алгоритмы применяются для безопасного обмена ключами, а затем симметричные шифры обеспечивают быструю передачу данных. Такая комбинация позволяет объединить сильные стороны обеих систем.

Криптография и квантовые технологии

Современные методы криптографической защиты информации считаются надёжными при условии ограниченности вычислительных ресурсов классических компьютеров. Однако, развитие квантовых технологий ставит под угрозу эффективность большинства используемых сегодня алгоритмов. Квантовые компьютеры, основанные на принципах суперпозиции и квантовой неопределённости, способны выполнять определённые вычисления значительно быстрее, чем традиционные системы. Эта технология открывает новые возможности, но одновременно создаёт серьёзные угрозы для информационной безопасности.

Основная угроза связана с тем, что квантовые алгоритмы позволяют эффективно решать

задачи, на которых основана стойкость многих классических криптосистем. Так, наибольшую известность получил алгоритм Шора, предложенный Питером Шором в 1994 году. Он способен за полиномиальное время выполнять факторизацию больших чисел и вычислять дискретные логарифмы – задачи, которые для классических компьютеров требуют астрономических затрат ресурсов [3]. Это означает, что RSA и метод Диффи-Хеллмана, являющиеся фундаментом современной криптографии с открытым ключом, могут быть взломаны при наличии достаточно мощного квантового компьютера.

Также серьёзную угрозу представляет алгоритм Гровера, который ускоряет поиск решения методом полного перебора. Хотя он не делает симметричные шифры полностью уязвимыми, их стойкость снижается вдвое. Например, при использовании ключа длиной 128 бит эффективная сложность атаки с применением квантового компьютера будет эквивалентна перебору 2^{64} вариантов. В связи с этим уже сегодня рекомендуется переходить на более длинные ключи (например, 256 бит для AES), чтобы компенсировать потенциальное снижение безопасности.

В ответ на новые угрозы сформировалось направление «постквантовой криптографии». В его рамках разрабатываются алгоритмы, устойчивые к квантовым атакам. Среди них можно выделить криптографию на решётках, многочленах, кодах и изогениях эллиптических кривых [2]. Эти подходы предлагают альтернативу RSA и ECC, сохраняя при этом возможность их практического использования в цифровых системах.

В 2016 году Национальный институт стандартов и технологий США (NIST) инициировал международный конкурс по отбору постквантовых алгоритмов. В финал вышли несколько кандидатов, среди которых были алгоритмы для шифрования (CRYSTALS-Kyber) и цифровой подписи (CRYSTALS-Dilithium, Falcon, SPHINCS+). Их внедрение в качестве новых стандартов произошло 13 августа 2024 года и стало основой будущей криптографической инфраструктуры [1].

Параллельно развивается и направление «квантовой криптографии», использующее принципы квантовой физики для защиты информации. Наиболее известен метод квантового распределения ключей (QKD – Quantum Key Distribution), позволяющий передавать секретные ключи по оптическим каналам с гарантией выявления попыток перехвата. Хотя практическое применение таких систем пока ограничено высокой стоимостью и сложностью оборудования, они рассматриваются как перспективное дополнение к классическим методам защиты.

Заключение.

История криптографии ярко демонстрирует, насколько неразрывно развитие человеческой цивилизации связано с потребностью защищать информацию. От простейших подстановочных шифров античности до замысловатых математических алгоритмов современности путь этой науки постоянно ставит друг напротив друга создателей средств защиты и криптоаналитиков, стремящихся их взломать.

При этом, будущее этой науки тесно связано с наступлением квантовой эпохи. Угроза компрометации традиционных алгоритмов заставляет учёных разрабатывать постквантовые подходы и искать новые схемы защиты. Уже сейчас активно ведётся работа над стандартизацией квантово-устойчивых методов и над развитием квантовой криптографии.

Подводя итог всему вышесказанному, следует подчеркнуть, что эволюция криптографических средств защиты данных – это не просто хроника технических достижений, а показатель всеобщей потребности в защите информации в постоянно изменяющемся мире. Поэтому с уверенностью можно заявить, что криптография и дальше останется одной из ведущих дисциплин XXI века, закладывающей фундамент доверия безопасности информации в цифровом обществе.

Библиографический список

1. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. – [Электронный ресурс]. – Режим доступа: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

2. Tsyganov I. Cryptographic methods of information protection / I. Tsyganov // Languages in professional communication. – Екатеринбург: ООО «Издательский Дом «Ажур», 2020. – P. 728-732.

3. Акыев Г.А. Обзор новых методов защиты информации, таких как квантовые криптографические системы и оптические методы обнаружения взлома / Г.А. Акыев // Вестник науки. – 2025. – Т. 4, № 1(82). – С. 805-809.

4. Аминев В.М. Эволюция криптографии: обзор исторических методов шифрования и их эволюция до современных технологий / В.М. Аминев // МОЛОДОЙ УЧЁНЫЙ. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 28-31.

5. Нестеренко А.Ю. Криптографические методы защиты информации: Учебник / А.Ю. Нестеренко, А.Б. Лось, М.И. Рожков. – 2-е изд. – Москва: Изд-во Юрайт, 2019. – 473 с.

6. Тарасов А.А. Криптографические Методы Защиты Информации: Учебник / А.А. Тарасов, О.В. Казарин, С.В. Запечников. – 1-е изд. – Москва: Изд-во Юрайт, 2019. – 309 с.

7. Эрнст М.В. История криптографии: от шифра Цезаря до современных алгоритмов / М.В. Эрнст // Сборник статей VII Международного научно-исследовательского конкурса, Пенза, 20 октября 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. – С. 47-49.

EVOLUTION OF CRYPTOGRAPHIC INFORMATION SECURITY METHODS

G.G. Konovalov, *Student*
D.A. Boshchenko, *Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *This article examines the evolution of cryptographic information security methods – from ancient ciphers to modern post-quantum algorithms. The main stages of cryptographic development are described: the use of simple substitution systems in antiquity and the Middle Ages, the emergence of mechanical and electromechanical devices in the modern era, the transition to symmetric algorithms in the computer age, and the revolution in asymmetric cryptography. Special attention is given to the discoveries of the quantum era and the prospects for the development of post-quantum security methods.*

Keywords: *cryptography, encryption, symmetric algorithms, asymmetric algorithms, RSA, AES, electronic signature, quantum computing, post-quantum cryptography, information security.*