МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра высшей алгебры и защиты информации

Широканов Андрей Юрьевич

Аннотация к дипломной работе:

Криптосистемы с открытым ключом

Научный руководитель:
доктор физ.-мат. наук,
профессор В.В. Беняш-Кривец

Минск 2024

РЕФЕРАТ

Дипломная работа: 36 страниц, 2 иллюстрации, 4 таблицы, 6 источников, 1 приложение.

КРИПТОСИСТЕМЫ, ОТКРЫТЫЙ КЛЮЧ, ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Цель исследования: Изучение принципов работы и особенностей криптосистем с открытым ключом, с акцентом на основные алгебраические определения, а так же алгоритмы *RSA*, эллиптические кривые и **ECDSA**.

В конце работы проведен обзор существующих источников, посвященных криптографии и криптосистемам с открытым ключом.

В первой главе мной были описанны основные определения полей, их свойств и роли в криптографии.А так же свойства конечных полей и их применение в криптографии, особенно в контексте криптосистемы *RSA*. Конечные поля обеспечивают надежную основу для выполнения сложных математических операций, необходимых для шифрования и дешифрования данных.

Во второй главе подробно рассмотрены принципы работы алгоритма *RSA*, его преимущества и недостатки.

Далее были рассмотрены эллиптические кривые, исследованы свойства эллиптических кривых и их применение в криптографии.

В последней главе подробно описана работа *Elliptic Curve Digital Signature Algorithm* (**ECDSA**), включая его принципы, преимущества и примеры применения.

Данная работа демонстрирует основные принципы работы криптосистем с открытым ключом, и их важность в современной информационной безопасности. Рассмотренные материалы позволяют оценить потенциал и перспективы развития криптографии, а также подчеркнуть значимость выбранных тем в контексте защиты конфиденциальности, целостности и доступности информации.

На основе проведенного анализа были выделены ключевые аспекты криптосистем с открытым ключом, включая их основные принципы работы, преимущества и ограничения. Полученные результаты могут служить основой для дальнейших исследований в области криптографии и информационной безопасности.

В заключение, данная работа демонстрирует глубокое понимание крипто-

систем с открытым ключом, их исторического развития и текущих тенденций в этой области. Рассмотренные материалы позволяют не только лучше понять теоретические основы криптографии, но и оценить практическую значимость этих знаний в современном мире, где безопасность информации играет ключевую роль.

РЭФЕРАТ

Дыпломная праца: 36 старонак, 1 іллюстрацыі, 4 табліцы, 6 крыніц, 1 дадатак.

КРЫПТАСІСТЭМЫ, АДКРЫТЫ КЛЮЧ, ЭЛІПТЫЧНЫЯ КРЫВЫЯ

Мэта даследавання: Вывучэнне прынцыпаў працы і асаблівасцяў крыптасістэм з адкрытым ключом, з акцэнтам на асноўныя алгебраічныя вызначэнні, а таксама алгарытмы *RSA*, эліптычныя крывыя і **ECDSA**.

У канцы працы праведзены агляд існых крыніц, прысвечаных крыптаграфіі і крыптасістэмам з адчыненым ключом.

У першым раздзеле мной былі апісаны асноўныя вызначэнні палёў, іх уласцівасцей і ролі ў крыптаграфіі. А таксама ўласцівасці канчатковых палёў і іх прымяненне ў крыптаграфіі, асабліва ў кантэксце крыптасістэмы *RSA*. Канчатковыя палі забяспечваюць надзейную аснову для выканання складаных матэматычных аперацый, неабходных для шыфравання і дэшыфраванні дадзеных.

У другім раздзеле падрабязна разгледжаны прынцыпы працы алгарытму *RSA*, яго перавагі і недахопы.

Далей былі разгледжаны эліптычныя крывыя, даследаваны ўласцівасці эліптычных крывых і іх прымяненне ў крыптаграфіі.

У апошнім раздзеле падрабязна апісана праца *Elliptic Curve Digital Signature Algorithm* (**ECDSA**), уключаючы яго прынцыпы, перавагі і прыклады ўжывання.

Дадзеная праца дэманструе асноўныя прынцыпы працы крыптасістэм з адкрытым ключом, і іх важнасць у сучаснай інфармацыйнай бяспецы. Разгледжаныя матэрыялы дазваляюць ацаніць патэнцыял і перспектывы развіцця крыптаграфіі, а таксама падкрэсліць значнасць выбраных тэм у кантэксце абароны прыватнасці, цэласнасці і даступнасці інфармацыі.

На аснове праведзенага аналізу былі выдзелены ключавыя аспекты крыптасістэм з адкрытым ключом, уключаючы іх асноўныя прынцыпы працы, перавагі і абмежаванні. Атрыманыя вынікі могуць служыць асновай для далейшых даследаванняў у галіне крыптаграфіі і інфармацыйнай бяспекі.

У заключэнне, дадзеная праца дэманструе глыбокае разуменне крыптасістэм з адкрытым ключом, іх гістарычнага развіцця і бягучых тэндэнцый у гэтай

галіне. Разгледжаныя матэрыялы дазваляюць не толькі лепш зразумець тэарэтычныя асновы крыптаграфіі, але і ацаніць практычную значнасць гэтых ведаў у сучасным свеце, дзе бяспека інфармацыі гуляе ключавую ролю.

ABSTRACT

Graduate thesis: 36 pages, 2 figures, 4 tables, 6 citations, 1 attachment.

CRYPTOSYSTEMS, PUBLIC KEY, ELLIPTIC CURVES

Research Objective: To study the principles and features of public-key cryptosystems, focusing on basic algebraic definitions, as well as the algorithms *RSA*, elliptic curves and **ECDSA**.

The paper concludes with a review of existing sources on cryptography and public key cryptosystems.

In the first chapter I described the basic definitions of fields, their properties and their role in cryptography, as well as the properties of finite fields and their application in cryptography, especially in the context of the *RSA* cryptosystem. Finite fields provide a secure basis for performing the complex mathematical operations required to encrypt and decrypt data.

Chapter 2 detailed the principles of the *RSA* algorithm, its advantages and disadvantages.

Then elliptic curves were considered, properties of elliptic curves and their application in cryptography were investigated.

The last chapter describes the *Elliptic Curve Digital Signature Algorithm* (**ECDSA**) in detail, including its principles, advantages, and application examples.

This paper demonstrates the basic principles of public-key cryptosystems and their importance in modern information security. The materials reviewed allow to evaluate the potential and prospects of cryptography development, as well as to emphasize the significance of the selected topics in the context of protecting confidentiality, integrity and availability of information.

Based on the analysis, key aspects of public-key cryptosystems were highlighted, including their basic operating principles, advantages and limitations. The results obtained can serve as a basis for further research in the field of cryptography and information security.

In conclusion, this paper demonstrates a thorough understanding of public key cryptosystems, their historical development and current trends in the field. The reviewed materials allow not only to better understand the theoretical foundations of cryptography, but also to evaluate the practical significance of this knowledge in

the modern world where information security plays a key role.

Оглавление

ВВЕДЕНИЕ

Создание криптографии с открытым ключом Диком и Хеллманом в 1976 году и последующее изобретение криптосистемы с открытым ключом *RSA* Ривестом, Шамиром и Адлеманом в 1978 году - переломные события в долгой истории секретных коммуникаций. Трудно переоценить значение криптосистем с открытым ключом и связанных с ними схем цифровой подписи в современном мире компьютеров и Интернета.

Криптография тесно связана с современной электронной связью. Однако криптография - дело довольно древнее, первые примеры относятся примерно к 2000 году до нашей эры, когда в Древнем Египте использовались нестандартные ”секретные” иероглифы. С египетских времен криптография в той или иной форме использовалась во многих, если не в большинстве, культур, в которых появилась письменность. Например, существуют документально подтвержденные случаи тайнописи в Древней Греции, а именно *скитала* Спарты, или знаменитый шифр Цезаря в Древнем Риме, о котором мы узнаем подробней в первой главе.

Далее представлена, схема криптологии 0.1. Стоит обратить внимание что, основная сфера не криптография а криптология. Криптоллогия разделяеться на две основные ветки **криптография** и **криптоанализ**.

Криптография - это наука о тайнописи, цель которой - скрыть смысл сообщения.

Криптоанализ - это наука, а иногда и искусство *взлома* криптосистем. Можно подумать, что взлом шифров предназначен для разведывательных и военных целей, или даже, организованной преступности, и не должен включаться в се-

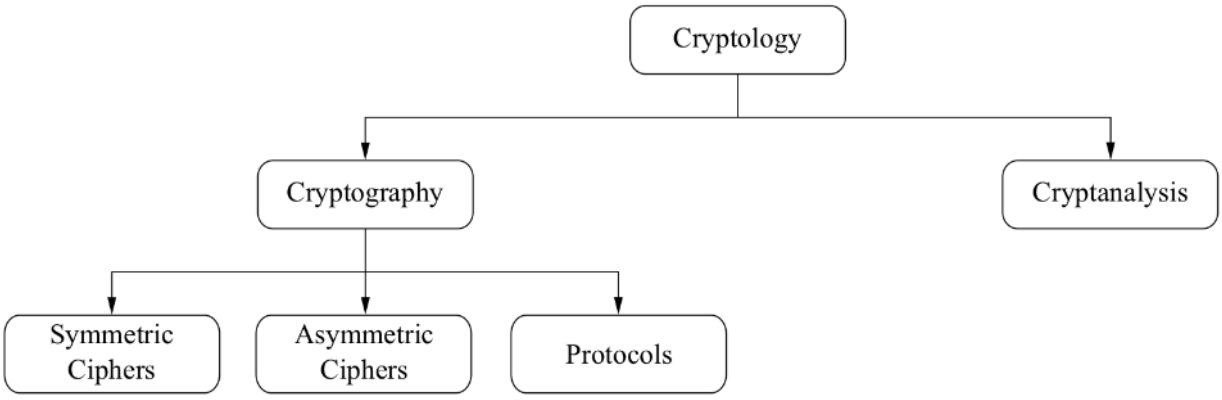


Рис. 0.1: Обзор сфер криптологии

рьезную классификацию научных дисциплин. Однако в настоящее время криптоанализом занимаются в основном респектабельные исследователи в академических кругах. Криптоанализ имеет огромное значение для современных криптосистем: без людей, которые пытаются сломать криптометоды, невозможно узнать действительно ли они безопасны или нет.

Так как, криптоанализ это основной метод для того что бы убедться в безопасности криптосистемы, он является неотъемлемой частью криптологии. Но нельзя сказать что криптоанализ это простая наука. Так, часто можно наблюдать что, реализация алгоритма шифрования весьма тривиальная вещь, с другой стороны реализация алгоритма который мог бы взломать построенную систему может быть очень сложной, а иногда, и не выполнимой задачей. Учитывая вышесказанное, в данной работе будет рассмотрена только криптография, хотя в некоторых главах упомянания криптоанализа будут встречаться.

Теперь вернемся к 0.1. Сама криптография делится на три основные ветви:

Симметричные алгоритмы - это то, на чем, по мнению многих людей, основана криптография: две стороны имеют метод шифрования и дешифрования, для которого у них есть общий секретный ключ. Вся криптография с древнейших времен до 1976 года была основана исключительно на симметричных методах. Симметричные шифры до сих пор широко используются, особенно для шифрования данных и проверки целостности сообщений.

Асимметричные алгоритмы (или алгоритмы с открытым ключом) В 1976 году Уитхелд Диф, Мартин Хеллман и Ральф Меркл представили совершенно другой тип шифра. В криптографии с открытым ключом пользователь владеет не только секретным ключом, как в симметричной криптографии, но и открытым ключом. Асимметричные алгоритмы могут использоваться для таких приложений, как цифровые подписи и установление ключей, а также для классического шифрования данных.

Криптографические протоколы или коротко, криптопротоколы занимаются применением криптографических алгоритмов. Симметричные и асимметричные алгоритмы можно рассматривать как строительные блоки, с помощью которых можно реализовать такие приложения, как безопасная связь в Интернете. Схема Transport Layer Security (TLS), которая используется в каждом веббраузере, является примером криптографического протокола.

Строго говоря, хэш-функции, которые будут упомянуты в дальнейшем, об-

разуют третий класс алгоритмов, но в то же время они имеют некоторые общие свойства с симметричными шифрами.

В большинстве криптографических приложений в практических системах симметричные и асимметричные алгоритмы (а зачастую и хэш-функции) используются вместе. Это иногда называют *гибридными схемами*. Причина использования обоих семейств алгоритмов заключается в том, что у каждого из них есть свои сильные и слабые стороны.

ГЛАВА 1
ВВЕДЕНИЕ В КРИПТОГРАФИЮ. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ.

1.1 Конечные поля в криптографии.

Конечные поля играют важную роль в криптографии из-за своих свойств, которые обеспечивают эффективность и безопасность различных криптографических алгоритмов. Вот основные причины, почему конечные поля важны в криптографии:

- **Математическая сложность**: Операции в конечных полях могут быть выполнены с использованием простых алгоритмов, что делает их эффективными для использования в криптографических системах. Например, операции сложения и умножения в конечных полях могут выполняются с использованием классов вычетов.
- **Стойкость к атакам**: Многие криптографические протоколы, такие как алгоритмы шифрования и эллиптическая криптография, используют конечные поля для обеспечения стойкости к различным видам атак, включая атаки перебором и атаки с использованием линейного или дифференциального криптоанализа.
- **Эффективность вычислений**: Алгоритмы, использующие конечные поля, могут быть реализованы с высокой эффективностью на современных вычислительных устройствах, что позволяет обеспечить быструю обработку данных в криптографических приложениях.

Также стоит упомянуть что конечные поля используются в самых востребованных областях криптографии таких как:

- **Шифрование**: Многие симметричные и асимметричные алгоритмы шифрования, такие как *AES* (*Advanced Encryption Standard*) и *RSA* (*Rivest-Shamir-Adleman*), используют операции над конечными полями для зашифрования и расшифрования данных.
- **Эллиптическая криптография**: В эллиптической криптографии конечные поля используются для определения кривых, над которыми выполняются операции шифрования и подписи.
- **Хэширование**: В некоторых алгоритмах хэширования, таких как *SHA-*

256 (*Secure Hash Algorithm 256-bit*), операции выполняются над конечными полями для генерации хэш-значений.

- **Цифровые подписи**: В протоколах для цифровых подписей, таких как *DSA* (*Digital Signature Algorithm*), конечные поля используются для генерации ключевой пары и подписи сообщений.

И это далеко не все примеры. Конечные поля широко применяются во многих других криптографических протоколах и алгоритмах для обеспечения безопасности и эффективности.

1.2 Предшествующие определения.

Рассмотрим предшествующие определения. Пожалуй, стоит начать с определения поля:

Определение 1.0.1 ***Полем*** *называется множество* $\mathbb{F}$ *с заданными ассоциативными, коммутативными, а также дистрибутивными операциями сложения и умножения, имеющее нейтральный элемент относительно сложения* 0*, относительно умножения* 1*, обратные элементы относительно сложения и обратные элементы относительно умножения ко всем кроме* 0*.*

Если раскрыть определение подробнейб то множество $\mathbb{F}$ с заданными на нем алгеброическими операциями сложения $+$ и умножения $*$: $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, $* : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, то есть $\forall a, b \in \mathbb{F}\ (a+b) \in \mathbb{F}, a * b \in \mathbb{F}$ называется полем $\langle \mathbb{F}, +, * \rangle$, если выполняются следующие аксиомы из определения:

1. Комутативность сложения: $\forall a, b \in \mathbb{F}\ a + b = b + a$
2. Ассоциативность сложения: $\forall a, b, c \in \mathbb{F}\ (a + b) + c = a + (b + c)$
3. Существование нейтрального элемента относительно сложения: $\exists 0 \in \mathbb{F} : \forall a \in \mathbb{F} a + 0 = a$
4. Существование обратного элемента относительно сложения: $\forall a \in \mathbb{F} \exists - a \in \mathbb{F} : a + (-a) = 0$
5. Комутативность умножения: $\forall a, b \in \mathbb{F}\ a * b = b * a$
6. Ассоциативность умножения: $\forall a, b, c \in \mathbb{F}\ (a * b) * c = a * (b * c)$
7. Существование нейтрального элемента относительно умножения: $\exists e \in \mathbb{F} \setminus \{0\} : \forall a \in \mathbb{F} a * e = a$
8. Существование обратного элемента для ненулевых элементов относительно умножения: $(\forall a \in \mathbb{F} : a \neq 0)\ \exists a^{-}1 \in \mathbb{F} : a * a^{-}1 = e$

9. Дистрибутивность умножения относительно сложения: $\forall a, b, c \in \mathbb{F}\ a * (b + c) = a * b + a * c$

К примеру, следующие поля являются основными во многих областях математики: $\mathbb{Q}$ - поле рациональных чисел,$\mathbb{R}$ - поле вещественных чисел, $\mathbb{C}$ - поле комплексных чисел, $\mathbb{Z}/p\mathbb{Z}$ - поле классов вчетов по модулю простого числа p. Последнее поле так же млжет обозначаться $\mathbb{F}_p$, реже $GF(p)$.

Определение 1.0.2 ***Векторное пространство*** *может быть определено над любым полем $\mathbb{F}$ с помощью тех же свойств, которые используются для определения векторного пространства на вещественных числах. Любое векторное пространство имеет* ***базис****, а количество элементов в базисе называется его* ***размерностью****. Поле расширения, под которым мы понимаем большее поле, содержащее $\mathbb{F}$, автоматически является векторным пространством над $\mathbb{F}$. Оно называется* ***конечным расширением****, если оно является векторным пространством конечной размерности. Под степенью конечного расширения мы понимаем его размерность как векторного пространства. Одним из распространенных способов получения расширений поля $\mathbb{F}$ является присоединение элемента к $\mathbb{F}$: мы говорим, что $\mathbb{K} = \mathbb{F}(\alpha)$, если $\mathbb{K}$ - это поле, состоящее из всех рациональных выражений, образованных с помощью α и элементов $\mathbb{F}$.*

Определение 1.0.3 ***Кольцо многочленов*** *над полем $\mathbb{F}$ в наборе переменных $X = X_1, ..., X_m$, обозначаемое $\mathbb{F}[X]$, состоит из всех конечных сумм произведений степеней $X_1, ..., X_m$ с коэффициентов в $\mathbb{F}$. (При $m = 2$ часто используется X и Y вместо X_1 и X_2, а при $m = 3$ - X, Y, Z.) Сложение и умножение многочленов в $\mathbb{F}[X]$ производится так же, как и в случае многочленов над вещественными числами. Мы говорим, что g делит f где $f, g \in \mathbb{F}[X]$, если существует многочлен $h \in \mathbb{F}[X]$ такой, что $f = gh$.* ***Непреводимые*** *многочлены $f \in \mathbb{F}[X]$ - это такие многочлены, что из соотношения $f = gh$ следует, что либо g, либо h - константа; они играют среди многочленов ту же роль, что простые числа среди целых чисел. Степень d многочлена от одной переменной - это наибольшая степень X, которая встречается с ненулевым коэффициентом. Многочлен называется* ***нормированым*** *если коэффициент X^d является* 1

Кольца многочленов (по одной или нескольким переменным) имеют уникальную факторизацию, то есть каждый многочлен в $\mathbb{F}[X]$ может быть записан

одним и только одним способом (за исключением констант) как произведение непреводимых элементов $\mathbb{F}[X]$.

Определение 1.0.4 *Элемент α в некотором расширеном поле $\mathbb{K}$, содержащем $\mathbb{F}$, считается **алгебраическим** над $\mathbb{F}$, если существует многочлен от одной переменной $f(X) \in \mathbb{F}[X]$ такой, что $f(\alpha) = 0$. В этом случае существует **единственный** нормированый непреводимый многочлен в $\mathbb{F}[X]$, в котором α является корнем (и любой другой многочлен, которому удовлетворяет α, должен быть кратным этому нормированому непреводимому многочлену). Этот многочлен называется **минимальным многочленом** от α.*

Если минимальный многочлен от α имеет степень d, то любой элемент $\mathbb{F}(\alpha)$ (то есть любое рациональное выражение, содержащее степени α и элементы $\mathbb{F}$) может быть выражен как линейная комбинация степеней $1, \alpha, \alpha^2, ..., \alpha^{d-1}$. Таким образом, эти степени α образуют базис $\mathbb{F}(\alpha)$ над $\mathbb{F}$, и поэтому степень расширения, получаемого при присоединении α, совпадает со степенью минимального многочлена.

Определение 1.0.5 *Любой другой корень α' из минимального многочлена α называется сопряженным α над $\mathbb{F}$. Произведение всех сопряженных α (включая само α) называется его **нормой**. Если α' является сопряженным α, то поля $\mathbb{F}(a)$ и $\mathbb{F}(a')$ изоморфны посредством отображения, переводящего любое выражение с α в то же самое выражение с заменой α на α'. **Изоморфность** означает, что между двумя полями существует взаимозначное соответствие, сохраняющее сложение и умножение. Если окажется, что $\mathbb{F}(a)$ и $\mathbb{F}(a')$ - одно и то же поле, то говорят, что отображение, переводящая α в α', дает **автоморфизм** поля.*

К примеру у $\sqrt{3}$ есть сопряженный элемент $-\sqrt{3}$ над полем $\mathbb{Q}$ и отображение $a+b\sqrt{3} \to a-b\sqrt{3}$ есть ни что иное, как афтоморфизм поля $\mathbb{Q}(\sqrt{2})$ (который состоит из всех действительных чисел вида $a + b\sqrt{3}$ с рациональными a и b).

Определение 1.0.6 ***Производная полинома** с одной переменной или **частная производная полинома** с несколькими переменными определяеться как nX^{n-1}, (не как придел, т.к. определение предела не имеет смысла без введения определений расстояния или топологии в $\mathbb{F}$).*

Определение 1.0.7 *Для любого полинома $f(X) \in \mathbb{F}[X]$ с одной переменной, существует расширенние $\mathbb{K}$ поля $\mathbb{F}$ такое что $f(X) \in \mathbb{K}[X]$ можно представить как произведение линейных множителей (или что равнасильно, f содержит d корней с учетом кратности, где d это степень полинома f), таких что $\mathbb{K}$ наименьшее расширение поля $\mathbb{F}$, содержащее эти корни. $\mathbb{K}$ - называется полем разложения f. Поле разложения определяеться с точностью до изоморфизма, это значит, что если есть поле $\mathbb{K}'$ удволетворяющее тем же свойствам, то существует взаимозначное отображения $\mathbb{K} \to \mathbb{K}'$ в котором сохраняются операции слодения и умножения.*

Например для полинома $f(X) = X^2 - 2$ полем разложения будет поле $\mathbb{Q}(\sqrt{3})$. Но для полинома $f(X) = x^3 - 3 \in \mathbb{Q}[X]$ что бы получить поле разложения нужно присоединить как и $\sqrt[3]{2}$ так и $\sqrt{-3}$. (Так как комплексными корнями 1 являются корни $\frac{-1\pm\sqrt{-3}}{2}$ то добавление $\sqrt{-3}$ так же означает добавление остальных корней 1).

Определение 1.0.8 *Если поле $\mathbb{F}$ обладает свойством, что каждый многочлен с коэффициентами в $\mathbb{F}$ полностью разлогается на линейные множители, то мы говорим, что $\mathbb{F}$ алгебраически замкнуто. Эквивалентно, достаточно потребовать, чтобы каждый многочлен с коэффициентами в $\mathbb{F}$ имел корень в $\mathbb{F}$.*

Например, поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.

Определение 1.0.9 *Наименьшее алгебраически замкнутое поле расширения $\mathbb{F}$ называется **алгебраическим замыканием** $\mathbb{F}$. Оно обозначается $\overline{\mathbb{F}}$. Например, алгебраическим замыканием поля действительных чисел является поле комплексных чисел.*

Определение 1.0.10 *Если при сложении нейтрального относительно умножения элемента 1 с самим собой в $\mathbb{F}$ никогда не получается 0. то мы говорим, что $\mathbb{F}$ имеет **характеристику ноль**; в этом случае $\mathbb{F}$ содержит копию поля рациональных чисел. В противном случае существует простое число p такое, что $1 + 1 + ... + 1$ (p раз) равно 0, и p называется **характеристикой** поля $\mathbb{F}$. В этом случае $\mathbb{F}$ содержит копию поля $\mathbb{Z}/p\mathbb{Z}$, которое называется его **простым полем**.*

1.3 Конечные поля в криптографии. Построение конечных полей.

Пусть $\mathbb{F}_q$ обозначает поле, в котором есть конечное число q элементов. Очевидно, что конечное поле не может иметь характеристику нуль; поэтому пусть p - характеристика $\mathbb{F}_q$. Тогда $\mathbb{F}_q$ содержит простое поле $F_p = \mathbb{Z}/p\mathbb{Z}$, а значит, является векторным пространством - обязательно конечной размерности - над $\mathbb{F}_p$. Пусть f обозначает его размерность как $\mathbb{F}_p$ - векторного пространства. Выбрав базис, мы можем установить взаимно однозначное соответствие между элементами этого f-мерного векторного пространства и множеством всех f-выборок элементов в F_p. Отсюда следует, что в F_p должно быть p^f элементов. То есть q - это степень характеристики p.

Вскоре мы увидим, что для каждой степени простого числа $q = p^f$ существует поле из q элементов, и оно уникально (вплоть до изоморфизма).

Но сначала давайте рассмотрим *порядок* ненулевых элементов поля $\mathbb{F}_q$. Под порядком ненулевого элемента мы понимаем наименьшую положительную степень, равную 1.

Есть $q-1$ ненулевых элементов, и согласно определению поля, они образуют абелеву группу относительно умножения. Это означает, что произведение двух ненулевых элементов ненулевое, ассоциативный закон и коммутативный закон выполняются, существует тождественный элемент 1, и любой ненулевой элемент имеет обратный. Группа ненулевых элементов из $\mathbb{F}_q$ обозначается $\mathbb{F}_q^*$.

Легко доказуемый факт о конечных группах состоит в том, что порядок любого элемента должен делиться на количество элементов в группе. Таким образом, порядок любого $a \in F_q^*$ делится на $q-1$.

Определение 1.0.11 *Образующий элемент g конечного поля $\mathbb{F}_q$ - это элемент порядка $q-1$; эквивалентно, g является образующий элементом, если степени g проходят через все ненулевые элементы $\mathbb{F}_g$.*

Теорема 1.0.12 *Каждое конечное поле имеет образующий элемент. Если g - генератор поля $\mathbb{F}_q^*$, то g^j также является генератором тогда и только тогда, когда НОД$(j, q-1) = 1$. Таким образом, всего существует $\varphi(q-1)$ различных генераторов F_q^*, где φ обозначает φ-функцию Эйлера.*

Примечание. Функция Эйлера (обозначается $\varphi(n)$) - мультипликативная функция принимающая значение равное количеству взаимно простых с n натуральных чисел, меньшее или равное n.

Лемма 1.0.13 *Для любого целого числа N, верно что $\sum_{d|N} \varphi(d) = N$.*

Например $18 = \sum_{d|18} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) = 1 + 1 + 2 + 2 + 6 + 6 = 18$

Следствие 1.0.14 *Для каждого простого числа n существует целое число p такое, что степени p исчерпывают все классы вычетов остатков по модулю n.*

Например с помощью тройки можно получить все вычеты пятерки, а именно степени тройки по модулю пяти принимают следующие значения $3, 4, 2, 1$.

Поле $\mathbb{F}_2$ состоит из двух элементов, но его можно определить по-разному в зависимости от выбора элементов и задания операций сложения и умножения над ними:

- Как набор из двух чисел «0» и «1», на котором операции сложения и умножения определяются как сложение и умножение чисел с результатом, заданным по модулю 2. Со стандартной арифметикой $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$. Эта логика лежит в основе двоичной системы компьютеров.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

- Как множество из двух логических объектов «ЛОЖЬ» (F) и «ИСТИНА» (T), на котором операции сложения и умножения определены как булевые операции «исключающее или» и «и».

+	F	T
F	F	T
T	T	F

$\times$	F	T
F	F	F
T	F	T

ГЛАВА 2
КРИПТОСИСТЕМА RSA

2.1 Алгоритм RSA.

В 1978 году Рональд Линн Ривест, Ади Шамир и Леонард Макс Адлеман (англ. Ronald Linn **R**ivest, Adi **S**hamir, Leonard Max **A**dleman) предложили алгоритм, обладающий рядом интересных для криптографии свойств. На его основе была построена система шифрования с открытым ключом, которая была названа по первым буквам фамилий авторов - система RSA. Криптосистема RSA стала первой системой, пригодной как для шифрования, так и для цифровой подписи. Алгоритм используется в большом количестве криптографических приложений.

Рассмотрим следующие теоремы:

Теорема 2.0.1 ***(Малая теорема Ферма)****: если p простое число не делящее a, то $a^{p-1} \equiv 1 \mod p$.*

Теорема 2.0.2 ***(Китайская теорема об остатках)****: Пусть $n_1, ..., n_k$ — попарно взаимно простые (то есть НОД$(n_i, n_j) = 1$ для $i \neq j$) натуральные числа и $c_1, ..., c_k \in \mathbb{Z}$. Тогда система сравнений $x \equiv x_i \mod n_i$, $i = 1, ..., k$ имеет целое решение x_0 , причем это решение единственно по модулю $n = n_1 \cdot ... \cdot n_k$.*

Рассмотрим принцип построения криптосистемы шифрования RSA с открытым ключом.

- Создание пары из закрытого и открытого ключей.
    1. Случайно выбрать большие простые различные числа p и q, для которых $\log_2 p \simeq \log_2 q > 1024$ бит (следует отметить, что задача поиска больших простых чисел обладает довольно большой вычислительной сложностью).
    2. Вычислить произведение $n = pq$.
    3. Вычислить функцию Эйлера $\varphi(n) = (p-1)(q-1)$.
    4. Выбрать случайное целое число $e \in [3, \varphi(n-1)]$ взаимно простое с $\varphi(n)$: НОД$(\varphi(n), e) = 1$.
    5. Вычислить число d такое, что $d \cdot e = 1 \mod \varphi(n)$.

6. Закрытым ключом будем называть пару чисел n и d, открытым ключом – пару чисел n и e.

- Шифрование с использованием открытого ключа.
  1. Сообщение представляют целым числом $m \in [1, n-1]$.
  2. Шифртекст вычисляется как: $c = m^e \mod n$. Шифртекст – также целое число из диапазона $[1, n-1]$.
- Расшифрование с использованием закрытого ключа. Владелец закрытого ключа вычисляет $m = c^d \mod n$.

Покажем корректность схемы шифрования RSA. В результате расшифрования шифртекста c (полученного путём шифрования открытого текста m) легальный пользователь имеет:

$$\begin{aligned} c^d = m^{ed} \mod p = m^{1+\alpha_1 \cdot \varphi(n)} \mod p = \\ = m^{1+\alpha_1 \cdot (p-1)(q-1)} \mod p = \\ = m1 + \alpha_2 \cdot (p-1) \mod p = \\ = m \cdot m^{\alpha_2 \cdot (p-1)} \mod p. \end{aligned}$$

Если m и p это взаимно простые число, то из малой теоремы Ферма следует, что:

$$\begin{aligned} m^{(p-1)} = 1 \mod p, \\ c^d = m \cdot m^{\alpha_2 \cdot (p-1)} = \\ = m \cdot (m^{(p-1)})^{\alpha_2} = \\ = m \cdot 1^{\alpha_2} = \\ = m \mod p. \end{aligned}$$

Если же m и p не являются взаимно простыми, то есть p является делителем m (p – простое число), то $m = 0 \mod p$ и $c^d = 0 \mod p$. В результате, для любых m верно, что $c^d = m \mod p$. Аналогично доказывается, что $c^d = m \mod q$. Из китайской теоремы об остатках следует:

$$\begin{cases} n = p \cdot q, \\ c^d = m \mod p, \Rightarrow c^d = m \mod n, \\ c^d = m \mod q. \end{cases}$$

Рассмотрим пример создания открытых и закрытых ключей, в криптосистеме RSA:

1. **Выбор простых чисел.** $p = 41$, $q = 23$.
2. **Вычисление модуля** n**.** Для этого перемножим p и q: $n = p \cdot q = 41 \cdot 23 = 943$.
3. **Вычисление функции Эйлера.** Вычислим по формуле $\varphi(n) = (p-1) \cdot (q-1)$: $\varphi(943) = (41-1) \cdot (23-1) = 40 \cdot 22 = 880$.
4. **Выбор открытого ключа** e**.** Выбираем число e, которое удовлетворяет условиям описаным выше. Для этого примера, выберем $e = 17$, число взаимно простое с 880 и большее чем единица.
5. **Вычисление закрытого ключа** d: Число d вычисляем как обратное к e по модулю $\varphi(n)$. Для этого можно использовать **алгоритм Евклида** или **Расширенный алгоритм Евклида**. В данном случае, $d = 2759$, так как $17 \cdot 2759 \equiv 1 \mod 880$.
6. **Создание пар ключей**: открытый ключ - $(n, e) = (943, 17)$; закрытый ключ - $(n, d) = (943, 2759)$.
7. **Шифрование сообщения**: Допустим, нам нужно зашифровать сообщение ”A”. Сначала преобразуем каждую букву в соответствующий числовой код (например, A = 65, B = 66 и т.д). Затем используем формулу шифрования *RSA*: $C = M^e \mod n$ где M - числовой код сообщения, e - открытый ключ, n - модуль. Для сообщения состоящего мз одной буквы ”A” $M = 65$ получаем: $C = 65^{17} \mod 943$.
8. **Расшифровка сообщения**: Используя формулу $M = C^d \mod n$ получим: $M = 65^{2759} \mod 943$.

ГЛАВА 3
Эллиптические кривые. Электронная подпись.

3.1 Эллиптические Кривые

3.1.1 Эллиптические кривые

Эллиптические кривые широко используются в разных областях математики таких как факторизация целых чисел, проверка на первичность, но наибольшее распространение они получили в построении криптосистем. Одна из основных причин интереса к криптосистемам основанным на эллиптических кривых, является то, что эти кривые источник огромного количества конечных абелевых групп с богатой алгебраической структурой.

Во многих отношениях группы эллиптических кривых аналогичны мультипликативным группам конечного поля. Однако у них имеют два преимущества: их гораздо больше, и они обеспечивают ту же безопасность при меньшем размере ключа. Подробнее об этом мы расскажем позже.

Эллиптическая кривая E над полем $\mathbb{F}$ это кривая уравнение которой имеет следующий вид:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, a_i \in \mathbb{F} \tag{3.1}$$

Введём обозначения: $E(\mathbb{F})$ множество точек $(x, y) \in \mathbb{F}_2$, удовлетворяющих этому уравнению, вместе с «*точкой на бесконечности*», обозначаемой O. Если $\mathbb{K}$ - любое расширение поля $\mathbb{F}$, то $E(\mathbb{K})$ обозначает множество $(x, y) \in \mathbb{K}_2$, удовлетворяющее 3.1, вместе с O. Для того чтобы кривая 3.1 была эллиптической кривой, она должна быть гладкой. Это означает, что не существует точки $E(\overline{\mathbb{F}})$ (напомним, что $\overline{\mathbb{F}}$ обозначает *алгебраическое замыкание* $\mathbb{F}$ см. (1.0.9)), в которой следующие уравнения

$$a_1Y = 3X^2 + a_2X + a_4, \qquad 2Y + a_1X + a_3 = 0 \tag{3.2}$$

не выполняются для $\forall(x, y) \in E(\overline{\mathbb{F}})$.

Допустим $\mathbb{F}$ не является полем характеристики 2, тогда без потери общности можно предположить, что $a_1 = a_3 = 0$. В случае характеристики 2 мы имеем

так называемый «суперсингулярный» случай с $Y^2 + a_3Y$ слева в 3.1 и «несуперсингулярный» случай с $Y^2 + a_1XY$ слева; в последнем случае без потери общности мы можем предположить, что $a_1 = 1$. (С характеристикой 2 мы также можем предположить, что $a_2 = 0$ в суперсингулярном случае и что $a_4 = O$ в несуперсингулярном случае).

Если характеристика $\mathbb{F}$ не равна ни 2, ни 3, то, упростив левую часть 3.2, линейной заменой переменных (а именно, $X \to X \to \frac{1}{3}a_2$) мы можем удалить и член X^2. То есть, без потери общности мы можем предположить, что наша эллиптическая кривая задается уравнением вида:

$$Y^2 = X^3 + aX + b, a, b \in \mathbb{F}, \qquad char\mathbb{F} \neq 2, 3 \tag{3.3}$$

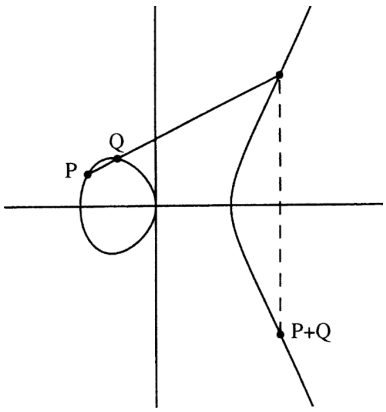
В этом случае условие гладкости кривой эквивалентно требованию, чтобы кубическое уравнение справа не имело кратных корней. Это справедливо тогда и только тогда, когда дискриминант $X^3 + aX + b$, который равен $(-4a^3 + 27b^2)$, ненулевой. Вспомним что дискриминант многочлена степени d с корнями $r_1, ..., r_d$ вычисляется по формуле $\prod_{i \neq j}(r_i - r_j) = (-1)^{d(d-1)/2} \prod_{i<j}(r_i - r_j)^2$.

Для любого расширения $\mathbb{K}$ поля $\mathbb{F}$, множество $E(\mathbb{K})$ образует абелеву группу, нейтральным элементом которой является O. Чтобы объяснить правила добавления точек, лучше всего сначала рассмотреть эллиптические кривые, определенные над полем вещественных чисел $\mathbb{R}$.

Можно заметить, что при больших X кривая уходит в бесконечность подобно функции $Y = X^{\frac{3}{2}}$, которую легко можно параметризовать, задав $X = T^2$ и $Y = T^3$. Часто говорят, что «X имеет степень 2» и «Y имеет степень 3». Подстрочные индексы a в 3.1 обозначают степени, которые должны быть присвоены коэффициентам, чтобы уравнение 3.1 было однородным, то есть, чтобы каждый член имел общую степень 6. Именно поэтому традиционно принято обозначать подстрочные знаки в 3.1 таким образом, который на первый взгляд выглядит немного необычно.

3.1.2 Группоовой закон

Определение 3.0.1 *Пусть E - эллиптическая кривая над вещественными числами, заданная уравнением 3.3, и пусть P и Q - две точки на E. Мы определяем отрицательный к P элемент и сумму $P + Q$ по следующим правилам:*



1. *Если P - точка на бесконечности, то мы определяем $-P$ как O. Для любой точки Q мы определяем $O + Q$ как Q; то есть Oслужит «нулевым элементом» группы точек. Далее будем предполагать, что ни P, ни Q не являются точками на бесконечности.*
2. *Отрицательная точка $-P$ - это точка с той же x-координатой, что и P, но отрицательной y-координатой; то есть, $-(x, y) = (x, -y)$. Из уравнения 3.3 следует, что $(x, -y)$ лежит на кривой всегда, когда лежит (x, y). Если $Q = -P$, то мы определяем $P+Q$ как точку на бесконечности O.*
3. *Если P и Q имеют разные x-координаты, то вскоре мы покажем, что прямая $l = PQ$ пересекает кривую еще ровно в одной точке R (если только l не является касательной к кривой в точке P, тогда берем $R = P$, или в точке Q, тогда берем $R = Q$). Мы определяем $P + Q$ как $-R$, то есть зеркальное отражение (по отношению к оси x) третьей точки пересечения. Геометрическая конструкция, дающая $P+Q$, показана на рисунке ниже.*
4. *Последний случай состоит в том, что $P = Q$. Тогда введём обозначения: l - касательная к кривой в точке P, и R - единственная отличная точка пересечения l с кривой, тогда $2P = -R$. (R принимается за P, если P - точка перегиба).*

Приведенный выше набор правил можно кратко изложить следующим образом:

Сумма трех точек пересечения прямой с кривой равна нулю.

Если прямая проходит через точку на бесконечности O, то это соотношение имеет вид $P + \widetilde{P} + O = O$ (где P и $\widetilde{P}$ - симметричные точки), т.е. $\widetilde{P} = -P$. В

противном случае она имеет вид $P + Q + R = O$, где P, Q и R - три точки из правила 3) или 4).

Теперь расммотрим, почему существует еще ровно одна точка, в которой прямая l проходящая через P и Q пересекает кривую заодно выведем формулу для координат этой третьей точки, а значит, и для координат $P + Q$.

Введём обозначения: (x_1, y_1), (x_2, y_2) и (x_3, y_3) координаты P, Q и $P + Q$, соответственно. Мы хотим выразить x_3 и y_3 с помощью x_1, y_1, x_2, y_2. Предположим, что мы находимся в случае 3) определения $P + Q$, и $y = \alpha x + \beta$ - уравнение прямой через P и Q (которая в случае 3) не является вертикальной прямой). Тогда $\alpha = (y_2 - y_1)/(x_2 - x_1)$, а $\beta = y_1 - \alpha x_1$. Точка $(x, \alpha x + \beta)$ l лежит на эллиптической кривой тогда и только тогда, когда $(\alpha x + \beta)^2 = x^3 + ax + b$. Таким образом, для каждого корня кубического уравнения $x^3 - (\alpha x + \beta)^2 + ax + b$ существует одна точка пересечения. Мы уже знаем, что существуют два корня x_1 и x_2, потому что $(x_1, \alpha x_1 + \beta)$, $(x_2, \alpha x_2 + \beta)$ - это точки P, Q на кривой. Поскольку сумма корней полинома равна минус коэффициенту второй по старшинству степени, то третий корень в данном случае равен $x_3 = \alpha^2 - x_1 - x_2$. Это приводит к выражению для x_3, а значит, и для обеих координат $P + Q = (x_3, -(\alpha x_3 + \beta))$, в терминах$x_1, y_1, x_2, y_2$:

$$\begin{aligned} x_3 &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 &= -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3). \end{aligned} \tag{3.4}$$

Случай, когда $P = Q$, аналогичен, за исключением того, что α теперь является производной dy/dx при P. Неявное дифференцирование уравнения 3.3 приводит к формуле $\alpha = (3x_1^2 + a)/2y_1$, и таким образом мы получаем следующие формулы для координат дважды P:

$$\begin{aligned} x_3 &= (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 \\ y_3 &= -y_1 + (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3). \end{aligned} \tag{3.5}$$

Пример. Пусть $P = (0, 0)$ на эллиптической кривой $Y^2 + Y = X^3 - X^2$. Найти $2P = P + P$ и $3P = P + 2P$.

Решение. Сначала преобразуем уравнение к виду 3.3, произведя замену переменных $Y \to Y - \frac{1}{2}, X \to X + \frac{1}{3}$. На этой кривой P превращается в

$Q = (-\frac{1}{3}, -\frac{1}{2})$. Используя 3.5, получаем $2Q = (\frac{2}{3}, -\frac{1}{2})$. Тогда из 3.4 имеем $3Q = 2Q + Q = (\frac{2}{3}, \frac{1}{2})$. Заметим, что $3Q = -(2Q)$, и, следовательно, Q - точка порядка 5, то есть $5Q = O$. Возвращаясь к исходной кривой, мы имеем $2P = (1, -1)$, $3P = (1, 0) = -2P$.

Приведенное выше определение $P+Q$ превращает точки на эллиптической кривой в абелеву группу. И как в любой абелевой группе, мы используем обозначение nP для P добавленного к самому себе n раз, если n положительно, и $-P$, добавленного к самому себе $|n|$ раз, если n отрицательно.

Рассмотрим точку O подробней. По определению, она является тождественным элементом группового закона. На приведенном выше графике кривой $Y^2 = X^3 - X$ эту точку следует представить как расположенную бесконечно далеко вверх по оси y, в предельном направлении наиболее крутых касательных к кривой. Это «третья точка пересечения» любой вертикальной линии с кривой; то есть такая линия имеет точки пересечения вида (x_1, y_1), $(x_1, -y_1)$ и O.

3.1.3 Эллиптические кривые над конечным полем

В дальнейшем считаем, что $\mathbb{F}$ - это конечное поле $\mathbb{F}_q$ из $q = p^f$ элементов. Обозначим E - эллиптическая кривая, определенная над $\mathbb{F}_q$. Если р $p \neq 2, 3$, то полагаем, что E задается уравнением вида 3.3. Если $p = 3$, то нам также нужно разрешить ${}^X2$-терминал справа в 3.3. Если $p = 2$, то есть два случая: неперсингулярный:

$$Y^2 + XY = X^3 + a_2X^2 + a_6 \tag{3.6}$$

и суперсингулярный случай:

$$Y^2 + a_3Y = X^3 + a_4X + a_6 \tag{3.7}$$

Если эллиптическая кривая E определена над $\mathbb{F}_g$, то она также определена над $\mathbb{F}_{q^r}$ для $r = 1, 2, ...$, и поэтому имеет смысл искать решения, так называемые «$\mathbb{F}_{q^r}$-точки», в расширениях поля определяющего уравнения кривой. Тогда N_r обозначает число F_{q^r}-точек на E. (Таким образом, $N_1 = N$ - это число точек с координатами в нашем «базовом поле» $\mathbb{F}_q$).

В эллиптической криптографии важное место занимает теорема Хассе, которая позволяет дать оценку числа точек на эллиптической кривой над конечным полем:

Теорема 3.0.2 *N - F_q-точек на E. Тогда*

$$|N - (q+1) \leq 2\sqrt{q}|$$

3.2 Криптосистемы на основе эллиптических кривых

Криптосистемы на основе эллиптических кривых были предложены в 1985 году независимо друг от друга Виктором Миллером и Нилом Коблицем. Два преимущества заключались в следующем: **А)** большая гибкость в выборе группы (то есть для каждого простого числа q существует только одна мультипликативная группа $\mathbb{F}_q^*$, но существует множество групп эллиптических кривых $E/\mathbb{F}q$), и особенно **Б)** отсутствие алгоритмов субэкспоненциального времени для взлома системы, если E выбрано подходящим образом.

Через несколько лет после изобретения криптосистем на основе эллиптических кривых Менезес, Окамото и Ванстоун нашли новый способ решения проблемы дискретного логарифма, на которой основана безопасность криптосистем на основе эллиптических кривых. А именно, задав эллиптическую кривую E, определенную на $\mathbb{F}_q$, они использовали сопряжение Вейля для вложения E в мультипликативную группу некоторого расширения $\mathbb{F}_{q^k}$. Это сводит проблему к дискретной логарифмической задаче в $F_{q^k}^*$. Однако для того, чтобы это было полезно, степень расширения k должна быть небольшой. По сути, единственными эллиптическими кривыми, для которых k мала, являются суперсингулярные. К ним относятся несколько простых уравнений, а также все уравнения вида 3.7 в характеристике 2; однако подавляющее большинство эллиптических кривых не являются суперсингулярными. Для них редукция Менезеса-Окамото-Ванстоуна почти никогда не приводит к алгоритму с субэкспоненциальным временем. Таким образом, основной открытый вопрос в криптографии на эллиптических кривых заключается в том, можно ли найти алгоритм с субэкспоненциальным временем для задачи дискретного логарифмирования на некотором классе несуперсингулярных эллиптических кривых.

Между тем, из-за прогресса в вычислении дискретных логарифмов конечных полей и факторизации целых чисел, размеры ключей, необходимые для обеспечения безопасности наиболее популярных систем с открытым ключом, существенно растут. Таким образом, статья Одлыжко на эту тему заканчивается

следующим предложением: «Поэтому, возможно, было бы разумно еще более серьезно рассмотреть криптосистемы на основе эллиптических кривых».

Одним из наиболее значимых вариантов использования криптосистемы с открытым ключом является обмен ключами (при этом фактическая передача сообщений будет осуществляться с помощью несвязанной системы закрытых ключей). Ключом может быть любое более или менее «случайное» целое число, о котором договорились два пользователя - Алиса и Ева, но которое не знает никто другой. Уникальная особенность криптографии с открытым ключом заключается в том, что Алиса и Ева могут прийти к общему ключу, используя только открытую, незашифрованную связь.

Первой криптосистемой с открытым ключом был обмен ключами Диффи-Хеллмана. Она может быть адаптирована для эллиптических кривых следующим образом. Сначала отметим, что «случайная» точка на эллиптической кривой E может служить ключом, поскольку Алиса и Ева могут заранее договориться о методе ее преобразования в целое число (например, они могут взять образ ее x-координаты под некоторым согласованным простым отображением из $\mathbb{F}_q$ в натуральные числа). Итак, предположим, что E - эллиптическая кривая над $\mathbb{F}_q$, а Q - согласованная (и общеизвестная) точка на кривой. Алиса тайно выбирает случайное целое число k_A и вычисляет точку k_AQ, которую она отправляет Еве. Аналогично, Ева тайно выбирает случайное число k_B, вычисляет k_BQ и отправляет его Алисе. Общий ключ равен $P = k_Ak_BQ$. Алиса вычисляет P, умножая точку, полученную от Евы, на ее секретное k_A. Ева вычисляет P, умножая точку, полученную от Алисы, на ее секретное k_B. Подслушивающий, который хотел бы постыдно шпионить за Алисой и Евой, должен был бы определить $P = k_Ak_BQ$, зная Q, k_AQ и k_BQ, но не k_A или k_B.

Задача подслушивающего называется *«проблема Диффи-Хеллмана для эллиптических кривых»*. Нетрудно модифицировать протокол Диффи-Хеллмана для передачи сообщений, используя идею *Эль-Гамаля*. Предположим, что набор единиц сообщений был вложен в E по некоторому согласованному алгоритму, и Ева хочет отправить Алисе сообщение M. Алиса и Ева уже обменялись сообщениями k_AQ и k_BQ, как описано выше. Теперь Ева выбирает другое секретное случайное целое число l и отправляет Алисе пару точек $(lQ, M+l(k_AQ))$ чтобы расшифровать сообщение, Алиса умножает первую точку в паре на свое секретное число k_A, а затем вычитает результат из второй точки в паре. Систе-

мы Диффи-Хеллмана и Эль-Гамаля можно взломать, если решить «проблему дискретного логарифмирования в группе E.

Определение 3.0.3 *Задача дискретного логарифмирования в группе G с базисом $g \in G$ - это задача, заданная $y \in G$, о нахождении целого числа x такого, что $g^x = y$ ($xg = y$, когда групповая операция в G записывается аддитивно), при условии, что такое целое число существует (другими словами, при условии, что y находится в подгруппе, порожденной g). Таким образом, в случае $G = E$ задача дискретного логарифма эллиптической кривой по основанию $Q \in E$ - это задача, заданная $P \in E$, нахождения целого числа x такого, что $P = xQ$, если такое число x существует.*

3.3 ECDSA (Elliptic Curve Digital Signature Algorithm)

Цифровая подпись это важгейший элемент в криптографии для обеспечения безопасности и целостности данных. Одним из наиболее эффективных методов создания цифровых подписей является использование цифровой подписи эллиптической кривой (ECDSA). ECDSA представляет собой вариант алгоритма цифровой подписи DSA, который использует криптографию на основе эллиптических кривых (ECC).

ECC основана на сложности решения задачи дискретного логарифма по эллиптическим кривым (ECDLP). Эта форма криптографии предлагает ряд преимуществ перед традиционными методами, такими как RSA, включая меньший размер ключа при сохранении аналогичного уровня безопасности. Например, 256-битная подпись ECDSA обладает той же степенью защиты, что и 3072-битная подпись RSA.

Алгоритм ECDSA работает с помощью математических операций над точками на эллиптической кривой. Он использует пару ключей: *открытый ключ*, который может быть общедоступным, и *закрытый ключ*, который должен оставаться конфиденциальным. Подпись генерируется путем применения закрытого ключа к хешу сообщения, а затем проверка подлинности подписи осуществляется с использованием открытого ключа.

Эллиптические кривые, используемые в ECDSA, описываются их параметрами домена, которые определяются различными криптографическими стан-

дартами, такими как SECG: SEC 2 и Brainpool (RFC 5639).

ECDSA играет важную роль во многих современных системах безопасности, включая блокчейн технологии, такие как Bitcoin, где он гарантирует, что средства могут быть потрачены только законными владельцами.

Вычисление ключей для **ECDSA** (от англ. *elliptic curve digital signature*) можно описать шагами следующего алгоритма:

1. Использование эллиптической кривой E с
   - модулем p
   - коэффицентами a и b
   - точкой A, порождающей циклическую группу простого порядка q
2. Выбор случайного целого числа d где $0 < d < q$.
3. Вычисление $B = dA$. Теперь ключи выглядят следующим образом:
   $k_{pub} = (p, a, b, q, A, B)$
   $k_{pr} = (d)$

Стоит обратить внимание на то, что мы поставили задачу дискретного логарифмирования, где целое число d является закрытым ключом, а результат скалярного умножения, точка B, является открытым ключом.

Подпись **ECDSA** состоит из пары целых чисел (r, s). Каждое значение имеет ту же битовую длину, что и q, что делает подписи достаточно компактными. Используя открытый и закрытый ключи, подпись для сообщения x вычисляется следующим образом:

1. Выбор целого числа в качестве случайного ключа k_E с $0 < k_E < q$.
2. Вычисление $R = k_E A$.
3. $r = x_R$.
4. Вычисление $s \equiv (h(x) + d \cdot r)k_E^{-1} \mod q$.

На шаге 3 переменной r присваивается x-координата точки R. Для вычисления s сообщение x должно быть хэшировано с помощью функции h. Длина выхода хэш-функции должна быть не меньше длины q. Для полного понимания **ECDSA** необходимо изучить хэш-функции, но из-за ограниченний по времени эта тема будет оставлена для дальнейшего изучения. Пока же достаточно знать, что хэш-функция сжимает x и вычисляет *fingerprint*, который можно рассматривать как представитель x.

Процесс проверки подписи выглядит следующим образом:

1. Вычислить вспомогательное значение $w \equiv s^{-1} \mod q$.

2. Вычислить вспомогательное значение $u_1 \equiv w \cdot h(x) \mod q$.
3. Вычислить вспомогательное значение $u_2 \equiv w \cdot r \mod q$.
4. Вычислите $P = u_1 A + u_2 B$.
5. Верификация $ver_{k_{pub}}(x, (r, s))$ следует из:

$$x_P \begin{cases} \equiv r \mod q \Rightarrow \text{действительная подпись} \\ \not\equiv r \mod q \Rightarrow \text{недействительная подпись} \end{cases} \tag{3.8}$$

В последнем шаге обозначение x_P указывает на x-координату точки P. Проверяющий принимает подпись (r, s) только в том случае, если x_P имеет то же значение, что и параметр подписи r по модулю q. В противном случае подпись следует считать недействительной.

ЗАКЛЮЧЕНИЕ

В данной дипломной работе была проведено детальное исследование криптосистем с открытым ключом, сосредоточенное на основных принципах и механизмах их функционирования. Основное внимание было уделено изучению основополагающих понятий в области криптографии, таких как конечные поля и эллиптические кривые, которые являются фундаментальными для разработки современных криптосистем.

В первой части работы были рассмотрены основные определения поля, включая их свойства и применение в криптографии. Эта глава наглядно иллюстрирует, как поля используются в качестве математической основы для создания безопасных алгоритмов шифрования и цифровых подписей.

Далее был подробно описан процесс использования конечных полей в криптографии, а также их роль в формировании криптосистемы RSA. Этот раздел освещает принципы работы RSA, его преимущества и недостатки, а также пример использования и реализации.

Следующим этапом исследования стала изучение эллиптических кривых и их применения в криптографии. Эллиптические кривые представляют собой мощный инструмент для создания криптосистем высокого уровня безопасности, что подтверждается их использованием во многих современных стандартах и протоколах.

Особое внимание было уделено *Elliptic Curve Digital Signature Algorithm* (**ECDSA**), который является одним из наиболее распространенных методов создания цифровых подписей на основе эллиптических кривых. В этом разделе были рассмотрены основные принципы работы **ECDSA**, его преимущества перед другими методами цифровой подписи и примеры его применения в различных областях.

В заключение, данная работа демонстрирует глубокое понимание криптосистем с открытым ключом, их исторического развития и текущих тенденций в этой области. Рассмотренные материалы позволяют не только лучше понять теоретические основы криптографии, но и оценить практическую значимость этих знаний в современном мире, где безопасность информации играет ключевую роль.

Литература

1. Christof Paar J. Understanding Cryptography. A Textbook for Students and Practitioners. Springer, 2010.
2. Neal Koblitz. Algebraic Aspects of Cryptography. Springer, 1998.
3. Jeffrey Hoffstein J., Jill Pipher. An Introduction to Mathematical Cryptography. Springer, 2014.
4. Н.Коблицп. КУРС ТЕОРИИ ЧИСЕЛ И КРИПТОГРАФИИ. Москва: Научное изд-во ТВП, 2001.
5. ivanp7. bgu-rfikt-diplom. https://github.com/ivanp7/bgu-rfikt-diplom. Шаблон LaTex.
6. Odlyzko A. M. iscrete logarithms in finite fields and their cryptographic significance. Springer, 1985.

ПРИЛОЖЕНИЕ

Далее представлен пример реализации шифрования RSA на языке GO:

```
1
2  package main
3
4  import (
5      "crypto/rand"
6      "fmt"
7      "math/big"
8  )
9
10 func eulerPhi(p, q *big.Int) *big.Int {
11     return big.NewInt(0).
12     Sub(p, big.NewInt(1)).
13     Mul(big.NewInt(0).
14     Sub(q, big.NewInt(1)))
15 }
16
17 func generatePrimes() (*big.Int, *big.Int) {
18     p := new(big.Int)
19     q := new(big.Int)
20     for {
21         p, _ = rand.Prime(rand.Reader, 64)
22         q, _ = rand.Prime(rand.Reader, 64)
23         if p.Cmp(q) != 0 {
24             break
25         }
26     }
27     return p, q
28 }
29
30 func modInverse(a, m *big.Int) *big.Int {
31     g, x, _ := extendedGCD(a, m)
32     if g == 1 {
33         return x.Mod(x.Neg(a), m)
34     }
35     return nil
36 }
37
38 func extendedGCD(a, b *big.Int) (int, *big.Int, *big.Int) {
39     if a.IsZero() {
40         return 0, big.NewInt(0), big.NewInt(1)
41     }
42     g, x, y := extendedGCD(b, a.Rem(a, b))
43     return g, y, x.Sub(x, y.Mul(y, a.Div(b, a)))
```

```
44 }
45
46 func main() {
47
48     p, q := generatePrimes()
49     fmt.Println("p:", p)
50     fmt.Println("q:", q)
51
52     n := new(big.Int).Mul(p, q)
53     fmt.Println("n:", n)
54
55     phi := eulerPhi(p, q)
56     fmt.Println("phi(n):", phi)
57
58     e := big.NewInt(17)
59     for e.Cmp(phi) <= 0 || e.GCD(phi).Cmp(big.NewInt(1))!= 1 {
60         e.Add(e, big.NewInt(1))
61     }
62
63     fmt.Println("e:", e)
64
65     d := modInverse(e, phi)
66     fmt.Println("d:", d)
67
68     message := big.NewInt(65)
69     ciphertext := new(big.Int).Exp(message, e, n)
70     fmt.Println("Ciphertext:", ciphertext)
71
72     plaintext := new(big.Int).Exp(ciphertext, d, n)
73     fmt.Println("Plaintext:", plaintext)
74 }
```