Научная статья

УДК 004.056.55
DOI 10.25205/1818-7900-2025-23-4-74-93

Комбинированный матрично-блочный алгоритм шифрования с использованием эллиптических кривых

Ольга Алексеевна Сергеева
Анастасия Сергеевна Кутовая
Владислав Сергеевич Сергеев

Кемеровский государственный университет
Кемерово, Россия

okoin@yandex.ru; https://orcid.org/0000-0002-9204-6318
askutovaia@mail.ru
v1a05@ya.ru

Аннотация

В статье рассматривается блочный криптографический алгоритм с использованием двухкомпонентного общего секретного ключа, полученного по принципу ключевого обмена Диффи – Хеллмана на точках эллиптической кривой над полем Z_p. Цель алгоритма – устранить недостатки отдельных классических алгоритмов и за счет их комбинирования повысить общую стойкость системы. Генерация и обмен ключами между пользователями осуществляются по типу эллиптических криптографических систем с открытым ключом. При этом предлагается два способа генерации общих секретных ключей для взаимодействующих пользователей: применение криптографического протокола Диффи – Хеллмана на нескольких точках эллиптической кривой или дополнительное использование рекуррентной формулы. Элементы шифрования в алгоритме представлены блоками в виде квадратных матриц, построенных на координатах точек эллиптической кривой. Собственно шифрование проходит в два этапа, на первом из которых используется поточное гаммирование с операцией вычисления кратной точки эллиптической кривой, а на втором проводится формирование матричных блоков и выполняется их матричное преобразование Хилла с использованием обратной связи. Каждый этап шифрования задействует соответствующий ему компонент общего секретного ключа пользователей: числовую гамма-последовательность или квадратную ключ-матрицу. Криптографическая стойкость алгоритма базируется на трудоемкости решения задачи дискретного логарифмирования на эллиптических кривых и защищенности сервиса совместного доступа с безопасной аутентификацией взаимодействующих пользователей. Блочная реализация второго этапа шифрования обеспечивает стойкость системы к частотному анализу. В качестве иллюстрации работы приведенного алгоритма в статье пошагово разбирается пример шифрования/дешифрования текстового сообщения.

Ключевые слова

шифрование, криптографический алгоритм, протокол Диффи – Хеллмана, эллиптические кривые, кратная точка, гаммирование, преобразование Хилла, матричные блоки

Для цитирования

Сергеева О. А., Кутовая А. С., Сергеев В. С. Комбинированный матрично-блочный алгоритм шифрования с использованием эллиптических кривых // Вестник НГУ. Серия: Информационные технологии. 2025. Т. 23, № 4. С. 74–93. DOI 10.25205/1818-7900-2025-23-4-74-93

Combined Matrix-Block Encryption Algorithm Using Elliptic Curves

Olga A. Sergeeva, Anastasia S. Kutovaya, Vladislav S. Sergeev

Kemerovo State University
Kemerovo, Russian Federation

okoin@yandex.ru; https://orcid.org/0000-0002-9204-6318
askutovaia@mail.ru
v1a05@ya.ru

Abstract

The article examines a block cryptographic algorithm using a two-component shared secret key obtained according to the Diffie-Hellman key exchange principle on elliptic curve points over the field Z_p. The goal is to eliminate shortcomings of individual classical algorithms and, through their combination, increase overall system strength. Key generation and exchange between users are carried out using elliptic curve cryptographic systems with public key. Two methods are proposed for generating shared secret keys for interacting users: applying the Diffie-Hellman cryptographic protocol on multiple elliptic curve points or additionally using a recurrence formula. Encryption elements are represented by blocks as square matrices constructed on elliptic curve point coordinates. Encryption proceeds in two stages: the first uses stream cipher with scalar multiplication of elliptic curve points, and the second involves forming matrix blocks and performing Hill matrix transformation with feedback. Each encryption stage utilizes its corresponding component of the users' shared secret key: a numerical gamma sequence or a square key matrix. The cryptographic strength is based on the computational complexity of solving the discrete logarithm problem on elliptic curves and the security of the sharing service with secure authentication of interacting users. The block implementation of the second encryption stage ensures the system's resistance to frequency analysis. As an illustration of the presented algorithm's operation, the article provides a step-by-step example of encrypting/decrypting a text message.

Keywords

Encryption, cryptographic algorithm, Diffie-Hellman protocol, elliptic curves, scalar multiple, gamma encryption, Hill transformation, matrix blocks

For citation

Sergeeva O. A., Kutovaya A. S., Sergeev V. S. Combined matrix-block encryption algorithm using elliptic curves. *Vestnik NSU. Series: Information Technologies*, 2025, vol. 23, no. 4, pp. 74–93 (in Russ.) DOI 10.25205/1818-7900-2025-23-4-74-93

Введение

Поточное шифрование при непосредственном кодировании символов алфавита в классических криптосистемах имеет своим главным недостатком нестойкость к статистическому частотному анализу текста [1]. Для устранения подобных уязвимостей в криптосистемах, использующих числовое кодирование элементов шифрования, отдают предпочтение блочным видам реализации, при которых символы открытого текста объединяются в биграммы или числовые блоки фиксированной длины [2–4]. Использование числовых блоков наделяет шифр свойством перемешивания, при котором скрываются статистические зависимости между исходным и зашифрованным текстами. Такой подход не был рассмотрен ранее для эллиптических криптосистем ввиду особенности операций в группе точек эллиптической кривой [5–7]. Однако использование числовых координат точек кривой по отдельности с сохранением их порядка позволяет обойти это ограничение и рассмотреть блочную реализацию эллиптической криптосистемы [8].

Результаты

В качестве варианта блочной реализации эллиптической криптографической системы в работе рассматривается матрично-блочный криптографический алгоритм с использованием

двухкомпонентного общего секретного ключа, полученного по принципу ключевого обмена Диффи – Хеллмана на точках эллиптической кривой [9]. Для успешного сочетания сильных сторон асимметричных и симметричных криптосистем в алгоритме совместно применяются особенности ключевого обмена в эллиптических криптосистемах и классические методы симметричного шифрования, такие как гаммирование [10], матричное шифрование Хилла [11; 12] и шифрование с обратной связью блоков [13]. Алгоритм включает пять последовательных этапов:

I. Генерация и обмен открытыми ключами.

II. Генерация двух компонентов общего секретного ключа.

III. Кодирование открытого текста точками эллиптической кривой.

IV. Гаммирование кодированного текста с использованием операции вычисления кратной точки.

V. Формирование блоков и их матричное преобразование Хилла с обратной связью.

Опишем подробно основные этапы такого блочного алгоритма и приведем наглядный пример его работы.

1. Генерация двухкомпонентного общего секретного ключа на основе ключевого обмена Диффи – Хеллмана

Обязательным начальным этапом любой криптографической системы является этап генерации ключей пользователей [14]. Данная система организуется по принципу криптосистем с открытым ключом, в которых каждый пользователь имеет два типа личных ключей: секретный и открытый. В соответствии с протоколом ключевого обмена Диффи – Хеллмана на основе личных ключей двух взаимодействующих пользователей системы можно сгенерировать их общий секретный ключ [15].

Для согласования общих входных параметров криптографической системы и реализации ключевого обмена между пользователями в сервисе совместного доступа и использования файлов публикуется информация о следующих используемых в системе данных:

1) конечное поле вычетов Z_p по простому модулю p;

2) эллиптическая группа $E_p(a, b)$, состоящая из точек эллиптической кривой с уравнением $y^2 = x^3 + ax + b$, определенной над полем Z_p;

3) генерирующая точка $G = (x, y)$, $G \in E_p(a, b)$;

4) порядок N эллиптической группы $E_p(a, b)$, равный общему количеству элементов в эллиптической группе, включая бесконечно удаленную точку;

5) порядок n квадратной ключ-матрицы K – четное натуральное число;

6) инструкция преобразования числовых значений (матрицы) секретного ключа при нарушении условий их допустимости: число (первый элемент матрицы) увеличивается на единицу до первого подходящего значения;

7) рекуррентная формула для последовательности точек эллиптической группы (при необходимости);

8) используемый алфавит (множество символов), закодированный конечными точками эллиптической группы $E_p(a, b)$;

9) открытые ключи пользователей в виде конечной последовательности точек эллиптической группы $E_p(a, b)$.

Размещение перечисленной выше информации на сервисе совместного доступа позволяет организовать бесконтактную работу взаимодействующих пользователей криптосистемы, без необходимости предварительных встреч, переговоров и передачи данных по защищенным каналам связи. Данная информация не является конфиденциальной и доступна к ознакомлению и использованию всеми заинтересованными лицами. В пункте 6 речь идет о дистанци-

онной договоренности между взаимодействующими пользователями о конкретных действиях с целью устранения недопустимых числовых значений, в частности коэффициентов кратности для точек эллиптической кривой, приводящих к появлению точки в бесконечности. Принятая инструкция числовых преобразований может пригодиться пользователям на этапе генерации их общих секретных ключей при анализе невырожденности матричного ключа и числовых элементов гамма-последовательности, а также при вычислении точек ключа по рекуррентной формуле.

Далее на основе открытых ключей двух взаимодействующих пользователей по аналогии с ключевым обменом Диффи – Хеллмана генерируется их общий секретный ключ, состоящий в данном случае из двух компонентов: квадратной ключ-матрицы K фиксированного четного порядка n и числовой гамма-последовательности Г из n^2 чисел, построенных из координат выбранных точек эллиптической группы $E_p(a, b)$. Рассмотрим подробнее два возможных варианта генерации общего секретного ключа для двух воображаемых взаимодействующих пользователей данной криптосистемы Алисы и Боба.

1.1. Вариант с заданной числовой последовательностью секретного ключа

Генерация личных секретных ключей

Каждый из пользователей генерирует свою личную числовую последовательность S, состоящую из $n^2/2$ целых чисел, не кратных порядку N эллиптической группы $E_p(a, b)$. Числовая последовательность S и будет представлять секретный ключ данного пользователя.

Генерация открытого ключа

Каждый из пользователей, используя свой секретный ключ S и операцию вычисления кратной точки в эллиптической группе, вычисляет свою последовательность точек эллиптической группы $E_p(a, b)$. Полученная последовательность точек и будет выполнять роль открытого ключа данного пользователя. Рассмотрим генерацию открытого ключа на примере одного из пользователей, например Алисы. Пусть Алиса имеет своим секретным ключом числовую последовательность $S^A = \left(s_1^A, s_2^A, \ldots, s_{n^2/2}^A\right)$. Тогда она вычисляет последовательность точек кривой $E_p(a, b)$, перемножая элементы числовой последовательности S^A на известную генерирующую точку G:

$$s_1^A \cdot G = Q_1^A = \left(u_1, v_1\right),$$
$$s_2^A \cdot G = Q_2^A = \left(u_2, v_2\right),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{n^2/2}^A \cdot G = Q_{n^2/2}^A = \left(u_{n^2/2}, v_{n^2/2}\right).$$

В итоге будет сформирован открытый ключ Алисы в виде последовательности точек кривой $E_p(a, b)$:

$$Q^A = \left(Q_1^A, Q_2^A, \ldots, Q_{n^2/2}^A\right).$$

Свои открытые ключи пользователи также выкладывают в сервис совместного доступа.

Генерация общего двухкомпонентного секретного ключа

Имея доступ к открытому ключу своего напарника, пользователи находят общий секретный ключ в виде ключ-матрицы K. Рассмотрим процесс генерации общего секретного ключа на примере двух воображаемых пользователей-напарников Алисы и Боба. Алиса узнает от-

крытый ключ Боба $Q^B = \left(Q_1^B, Q_2^B, \ldots, Q_{n^2/2}^B\right)$, выложенный им на открытый сервис совместного доступа. Используя точки открытой последовательности Q^B и числа своей личной секретной последовательности S^A, Алиса находит последовательность точек общего секретного ключа как результат вычисления кратных точек в эллиптической группе $E_p(a, b)$:

$$s_1^A \cdot Q_1^B = P_1 = \left(\xi_1, \tau_1\right),$$
$$s_2^A \cdot Q_2^B = P_2 = \left(\xi_2, \tau_1\right),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$s_{n^2/2}^A \cdot Q_{n^2/2}^B = P_{n^2/2} = \left(\xi_{n^2/2}, \tau_{n^2/2}\right).$$

Из координат полученных точек Алиса формирует квадратную ключ-матрицу K, построчно записывая в нее координаты точек. Чтобы понять, как именно это происходит, предположим что $n = 4$ и Алиса указанным выше способом получила общую с Бобом секретную последовательность из $(4 \times 4)/2 = 8$ точек $\left(P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8\right)$, где $P_i = \left(\xi_i, \tau_i\right), i = 1, \ldots, 8$. Тогда ключ-матрица K получает размерность 4×4 и формируется по правилу

$$K = \begin{pmatrix} \xi_1 & \tau_1 & \xi_2 & \tau_2 \\ \xi_3 & \tau_3 & \xi_4 & \tau_4 \\ \xi_5 & \tau_5 & \xi_6 & \tau_6 \\ \xi_7 & \tau_7 & \xi_8 & \tau_8 \end{pmatrix}.$$

Точно такая же ключ-матрица получится у Боба – напарника Алисы, на основе его личной секретной числовой последовательности S^B и открытого ключа Алисы $Q^A = \left(Q_1^A, Q_2^A, \ldots, Q_{n^2/2}^A\right)$, так как

$$s_i^A \cdot Q_i^B = s_i^A \cdot (s_i^B \cdot G) = s_i^B \cdot (s_i^A \cdot G) = s_i^B \cdot Q_i^A, \; i = 1, \ldots, n^2/2.$$

Ключ-матрица K должна быть невырожденной, т. е. должна быть обратимой по модулю. Нарушение этого условия не позволит использовать этот матричный ключ и потребует его изменения в соответствии с инструкцией.

Кроме ключ-матрицы K, на основе полученной совместной последовательности точек P_i, $i = 1, \ldots, n^2/2$ ормируется числовая гамма-последовательность $\Gamma = \left\{x_1, y_1, x_2, y_2, \ldots, x_{\frac{n^2}{2}}, y_{\frac{n^2}{2}}\right\} = \left\{\gamma_i\right\}_{i=1}^{n^2}$ длиною n^2. Все числа этой последовательности независимо друг от друга будут использованы при шифровании как числовые коэффициенты кратности при вычислении кратных точек в эллиптической группе $E_p(a, b)$. Поэтому они должны соответствовать обязательному условию обратимости этой операции, а именно должны быть взаимно простыми с порядком эллиптической группы N, т. е. должно выполняться равенство $\text{НОД}\left(N, \gamma_i\right) = 1, i = 1, \ldots, n^2$. В противном случае при нарушении этого условия, согласно опубликованной инструкции, недопустимое числовое значение γ_i этой последовательности преобразуется путем последовательного увеличения на 1 до первого подходящего значения.

Таким образом, на основе общей секретной последовательности точек эллиптической кривой $\left\{P_i\right\}_{i=1}^{n^2/2}$, $P_i = (x_i, y_i) \in E_p(a, b)$ будет сгенерирован общий двухкомпонентный секретный ключ для взаимодействующих пользователей Алисы и Боба, представленный:

1) квадратной ключ-матрицей K размером $n \times n$;

2) числовой гамма-последовательностью $\Gamma = \left\{\gamma_i\right\}_{i=1}^{n^2}$.

1.2. Вариант с использованием рекуррентной формулы

Если в списке общих параметров системы порядок n ключ-матрицы K будет выбран достаточно большим, то, чтобы избежать сложности организации работы с большим объемом входных личных секретных данных, удобнее использовать рекуррентную формулу для вычисления последовательности точек общего секретного ключа пользователей.

В этом случае числовую последовательность личных секретных ключей пользователей достаточно задать двумя случайными целыми числами, не кратными порядку эллиптической группы N. С их помощью по тем же формулам, что и в предыдущем варианте, каждый пользователь находит свой открытый ключ, представляющий собой последовательность из двух точек эллиптической кривой, и публикует его на платформе сервиса совместного доступа.

После обмена открытыми ключами пользователи Алиса и Боб независимо друг от друга находят общий секретный ключ, состоящий из двух точек (P_1, P_2) эллиптической группы $E_p(a, b)$. Чтобы найти оставшиеся $\left(\frac{n^2}{2}-2\right)$ точек, необходимые для формирования ключ-матрицы K, пользователи используют рекуррентную формулу, опубликованную на открытом сервисе совместного доступа вместе с другими общими входными данными системы. Если порядок n ключ-матрицы не кратен порядку N эллиптической группы, то в качестве рекуррентной формулы может быть использована, например, такая формула по двум точкам:

$$P_{i+2} = n \cdot P_i + P_{i+1}, \tag{1}$$

где $i = 1, \ldots, n^2/2 - 2$; $P_1 \in E_p(a,b)$ – первая точка общего секретного ключа; $P_2 \in E_p(a,b)$ – вторая точка общего секретного ключа.

Если при вычислении по формуле (1) на каком-то i-м шаге $(i = 1, \ldots, n^2/2 - 2)$ кратная точка $n \cdot P_i$ окажется противоположной точкой для точки P_{i+1}, то, чтобы избежать в качестве результата их сложения точки в бесконечности, коэффициент кратности n в этом случае увеличивают на 1 до первого подходящего значения, т. е. значения, не кратного N, при котором точки $n \cdot P_i$ и P_{i+1} не будут являться противоположными. Договоренность о таких действиях также публикуется заранее на используемом сервисе совместного доступа для взаимодействующих пользователей.

Таким образом, на основе двух общих секретных входных точек P_1 и P_2, полученных по принципу ключевого обмена Диффи – Хеллмана, и известной рекуррентной формулы пользователями Алисой и Бобом бесконтактно будет сгенерирована общая секретная последовательность из $n^2/2$ точек эллиптической группы $E_p(a, b)$ и далее будут сформированы их общие секретные ключ-матрица K и гамма-последовательность Г. Стоит отметить, что открытая информация о значении порядка n ключ-матрицы K и о самой рекуррентной формуле без известных входных точек P_1 и P_2 не позволит несанкционированным пользователям сгенерировать последовательность точек общего секретного ключа Алисы и Боба, а значит, и определить их общую ключ-матрицу K. Информация об общих секретных входных точках P_1 и P_2 защищена высокой трудоемкостью решения задачи дискретного логарифмирования.

Формирование ключ-матрицы K и гамма-последовательности Г осуществляется из координат полученных точек $P_i, i = 1, \ldots, n^2/2,$ по той же схеме, как показано в предыдущем варианте.

Если в качестве входных секретных личных ключей пользователей взять последовательность из k целых чисел, где $k < n^2/2$, то открытые ключи пользователей будут представлены упорядоченным набором из k точек эллиптической группы. Тогда построение общего секретного ключа будет включать вычисление по принципу Диффи – Хеллмана последовательности

из k общих точек P_1, P_2, ..., P_k и определение оставшихся ($n^2/2 - k$) точек по рекуррентной формуле вида

$$P_{k+i} = n^{k-1} \cdot P_i + n^{k-2} \cdot P_{i+1} + \ldots + n \cdot P_{i+k-2} + P_{i+k-1}, \quad (2)$$

2. Шифрование/дешифрование с использованием двухкомпонентного общего секретного ключа

Любая криптографическая система состоит из двух взаимообратных алгоритмов: шифрования и дешифрования. Алгоритм шифрования с использованием двухкомпонентного общего секретного ключа состоит из двух последовательных этапов:

Этап 1: гаммирование

После кодирования открытого текста точками эллиптической кривой осуществляется его гаммирование с операцией умножения точек на числовой коэффициент, т. е. вычисления кратной точки, где в качестве коэффициентов кратности выступают числовые значения секретной гамма-последовательности. При этом сама гамма повторяется столько раз, сколько необходимо для покрытия всего открытого текста. В итоге будет получен промежуточный шифр, представляющий собой последовательность полученных кратных точек.

Этап 2: матричное преобразование

Координаты точек промежуточного шифра, полученного после гаммирования, объединяются в общую числовую последовательность с сохранением порядка следования точек и порядка их координат. Далее числовая последовательность разбивается на n^2-блоки, т. е. блоки последовательности длиною n^2. Если целое деление длины последовательности на n^2 невозможно и в итоге остается неполный блок, то в его конец добавляются значения, взятые с начала первого блока.

Из каждого полученного числового n^2-блока построчными срезами длиной n формируется квадратная матрица и промежуточный блочный шифр принимает вид последовательности матриц $\{T_i\}$. Далее каждая матрица из полученной последовательности умножается слева на ключ-матрицу K по модулю p с использованием обратной связи с предыдущей матрицей-блоком по правилу

$$C_1 = K \cdot T_1 \,(mod\ p),\ C_i = \left(K \cdot T_i + T_{i-1}\right)(mod\ p), i > 1. \quad (3)$$

Полученная последовательность матриц $\{C_i\}$ и представляет шифр по данному алгоритму.

Дешифрование также проходит в два этапа, но в обратном порядке. Общий алгоритм дешифрования имеет вид:

1. Определяется обратная матрица K^{-1} (*mod N*) для секретной ключ-матрицы K.
2. Вычисляются обратные значения по модулю N для числовых элементов гамма-последовательности Г: γ^{-1} (*mod N*), из которых составляется дешифрующая гамма-последовательность $Г^{-1}$ (*mod N*).
3. Каждая шифр-матрица C_i преобразуется по формуле матричного дешифрования с использованием обратной связи:

$$T_1 = K^{-1} \cdot C_1 \,(mod\ p),\ T_i = K^{-1} \cdot \left(C_i - T_{i-1}\right)(mod\ p),\ i > 1. \quad (4)$$

4. Из матриц T_i извлекаются построчные срезы, из элементов которых составляется последовательность числовых значений. Далее с сохранением порядка следования значения объединяются в упорядоченные пары, представляющие точки эллиптической группы $E_p(a, b)$.

5. Каждая точка из полученной последовательности точек эллиптической группы умножается на соответствующий элемент дешифрующей гамма-последовательности.

6. Полученный набор точек эллиптической группы декодируется в соответствующие символы алфавита и открытый текст восстанавливается.

3. Пример работы алгоритма с рекуррентной формулой для открытых ключей

Предположим, что для организации работы взаимодействующих пользователей на каком-либо сервисе совместного доступа и использования файлов была предварительно опубликована информация о следующих используемых в системе данных:

1) конечное поле вычетов Z_{43} по простому модулю $p = 43$;

2) эллиптическая группа $Z_{43}(17,24)$ состоящая из точек эллиптической кривой $y^2 = x^3 + 17x + 24$, определенной над полем Z_{43};

3) генерирующая точка $G = (16, 36)$, $G \in E_{43}(17, 24)$;

4) порядок $N = 51$ эллиптической группы $E_{43}(17, 24)$;

5) порядок $n = 4$ квадратной ключ-матрицы K – четное натуральное число;

6) инструкция преобразования числовых значений (матрицы) секретного ключа при нарушении условий их допустимости: число (первый элемент матрицы) увеличивается на единицу до первого подходящего значения;

7) рекуррентная формула (1) для последовательности точек эллиптической группы;

8) кодированный русский алфавит на точках эллиптической кривой $E_{43}(17, 24)$ (табл. 1).

Таблица 1

Кодированный алфавит

Table 1

Encoded alphabet

№	символ	точка	№	символ	точка	№	символ	точка
1	**А**	(0, 14)	18	**Р**	(18, 23)	35	**.**	(30, 10)
2	**Б**	(0, 29)	19	**С**	(19, 5)	36	**,**	(30, 33)
3	**В**	(2, 18)	20	**Т**	(19, 38)	37	**!**	(32, 21)
4	**Г**	(2, 25)	21	**У**	(21, 15)	38	**?**	(32, 22)
5	**Д**	(3, 4)	22	**Ф**	(21, 28)	39	**:**	(33, 12)
6	**Е**	(3, 39)	23	**Х**	(22, 9)	40	*****	(33, 31)
7	**Ё**	(6, 16)	24	**Ц**	(22, 34)	41	**0**	(35, 8)
8	**Ж**	(6, 27)	25	**Ч**	(24, 18)	42	**1**	(35, 35)
9	**З**	(7, 20)	26	**Ш**	(24, 25)	43	**2**	(36, 11)
10	**И**	(7, 23)	27	**Щ**	(25, 11)	44	**3**	(36, 32)
11	**Й**	(12, 8)	28	**Ъ**	(25, 32)	45	**4**	(39, 8)
12	**К**	(12, 35)	29	**Ы**	(26, 5)	46	**5**	(39, 35)
13	**Л**	(16, 7)	30	**Ь**	(26, 38)	47	**6**	(41, 5)
14	**М**	(16, 36)	31	**Э**	(28, 7)	48	**7**	(41, 38)
15	**Н**	(17, 18)	32	**Ю**	(28, 36)	49	**8**	(42, 7)
16	**О**	(17, 25)	33	**Я**	(29, 3)	50	**9**	(42, 36)
17	**П**	(18, 20)	34	**_**	(29, 40)			

На основании этой информации взаимодействующие пользователи Алиса и Боб генерируют сначала свои личные ключи – секретный и открытый, размещают информацию о своих открытых ключах на совместном сервере и затем приступают к генерации компонентов общего секретного ключа.

Генерация двухкомпонентного общего секретного ключа

Предположим, что Алиса своим секретным ключом выбрала упорядоченную числовую пару $S^A = (13,45)$, а Боб $S^B = (9,21)$.

Пользователи по отдельности находят свои открытые ключи в виде двух упорядоченных точек эллиптической группы $E_{43}(17, 24)$ (табл. 2).

Таблица 2

Генерация открытых ключей

Table 2

Public key generation

Алиса	**Боб**
$Q_1^A = 13 \cdot G = 13 \cdot (16,36) = (2,18);$ $Q_2^A = 45 \cdot G = 45 \cdot (16,36) = (29,3).$	$Q_1^B = 9 \cdot G = 9 \cdot (16,36) = (21,15);$ $Q_1^B = 21 \cdot G = 21(16,36) = (30,10).$

Полученные открытые ключи пользователей Алисы и Боба представлены в таблице, опубликованной на сервисе общего пользования (табл. 3).

Таблица 3

Публикация открытых ключей

Table 3

Public key publication

Алиса	**Боб**
$Q^A = ((2,18), (29,3))$	$Q^B = ((21,15), (30,10))$

Используя открытый ключ напарника и числовые значения своего личного секретного ключа, каждый из пользователей формирует ключ-матрицу K и гамма-последовательность Г. Для этого сначала вычисляются две начальные общие точки, из которых потом по рекуррентной формуле (1) вычисляются оставшиеся общие точки пользователей (табл. 4).

Таблица 4

Генерация общих секретных точек

Table 4

Shared secret point generation

Алиса	**Боб**
$P_1 = 13 \cdot (21,15) = (33,12);$ $P_2 = 45 \cdot (30,10) = (24,25).$	$P_1 = 9 \cdot (2,18) = (33,12);$ $P_2 = 21 \cdot (29,3) = (24,25).$
$P_3 = 4 \cdot P_1 + P_2 = 4 \cdot (33,15) + (24,25) = (33,31),$ $P_4 = 4 \cdot P_2 + P_3 = 4 \cdot (24,25) + (33,31) = (21,28),$ $P_5 = 4 \cdot P_3 + P_4 = 4 \cdot (33,31) + (21,28) = (42,7),$ $P_6 = 4 \cdot P_4 + P_5 = 4 \cdot (21,28) + (42,7) = (6,16),$ $P_7 = 4 \cdot P_5 + P_6 = 4 \cdot (42,7) + (6,16) = (24,25),$ $P_8 = 4 \cdot P_6 + P_7 = 4 \cdot (6,16) + (24,25) = (33,12).$	

В итоге из координат полученных точек в соответствии с их порядком каждый пользователь формирует секретную ключ-матрицу – первый компонент общего секретного ключа:

$$K = \begin{pmatrix} 33 & 12 & 24 & 25 \\ 33 & 31 & 21 & 28 \\ 42 & 7 & 6 & 16 \\ 24 & 25 & 33 & 12 \end{pmatrix}$$

и числовую последовательность:

$$\Gamma = (33,12,24,25,33,31,21,28,42,7,6,16,24,25,33,12).$$

Все элементы числовой последовательности проверяются на допустимость, и в случае нарушения условия допустимости для какого-либо элемента его числовое значение будет увеличиваться на единицу до тех пор, пока новое значение и порядок кривой $N = 51$ не станут взаимно простыми числами. В итоге этих действий Алиса и Боб независимо друг от друга получают гамма-последовательность – второй компонент общего секретного ключа:

$$\Gamma = (33 + 2, 12 + 1, 24 + 1, 25, 33 + 2, 31, 21 + 1, 28, 42 + 1,$$
$$7, 6 + 1, 16, 24 + 1, 25, 33 + 2, 12, + 1) =$$
$$= (35, 13, 25, 25, 35, 31, 22, 28, 43, 7, 7, 16, 25, 25, 35, 13).$$

Шифрование с использованием двухкомпонентного общего секретного ключа

Для наглядной демонстрации работы предложенного алгоритма шифрования предположим, что Алиса шифрует исходное сообщение, а Боб его расшифровывает. В качестве примера текста исходного сообщения возьмем тематическое предложение:

«АЛИСА_И_БОБ_ЯВЛЯЮТСЯ_ВЗАИМОДЕЙСТВУЮЩИМИ_ АГЕНТАМИ_КРИПТОГРАФИЧЕСКИХ_СИСТЕМ.»

Числовое значение длины текста сообщения, равное 74, не кратно 16, поэтому Алиса добавляет в конец текста 6 его первых символов и получает расширенный текст сообщения из 80 символов, которое не меняет своего первоначального смысла. Далее Алиса кодирует полученный текст точками эллиптической кривой E_{43} (17, 24) в соответствии с алфавитной таблицей (табл. 5).

Таблица 5

Кодирование открытого текста

Table 5

Plaintext encoding

А	**Л**	**И**	**С**	**А**	**_**	**И**	**_**	**Б**
(0,14)	(16,7)	(7,23)	(19,5)	(0,14)	(29,40)	(7,23)	(29,40)	(0,29)
О	**Б**	**_**	**Я**	**В**	**Л**	**Я**	**Ю**	**Т**
(17,25)	(0,29)	(29,40)	(29,3)	(2,18)	(16,7)	(29,3)	(28,36)	(19,38)
С	**Я**	**_**	**В**	**З**	**А**	**И**	**М**	**О**
(19,5)	(29,3)	(29,40)	(2,18)	(7,20)	(0,14)	(7,23)	(16,36)	(17,25)
Д	**Е**	**Й**	**С**	**Т**	**В**	**У**	**Ю**	**Щ**
(3,4)	(3,39)	(12,8)	(19,5)	(19,38)	(2,18)	(21,15)	(28,36)	(25,11)

Окончсание табл. 5

И	**М**	**И**	**_**	**А**	**Г**	**Е**	**Н**	**Т**
(7,23)	(16,36)	(7,23)	(29,40)	(0,14)	(2,25)	(3,39)	(17,18)	(19,38)

А	**М**	**И**	**_**	**К**	**Р**	**И**	**П**	**Т**
(0,14)	(16,36)	(7,23)	(29,40)	(12,35)	(18,23)	(7,23)	(18,20)	(19,38)

О	**Г**	**Р**	**А**	**Ф**	**И**	**Ч**	**Е**	**С**
(17,25)	(2,25)	(18,23)	(0,14)	(21,28)	(7,23)	(24,18)	(3,39)	(19,5)

К	**И**	**Х**	**_**	**С**	**И**	**С**	**Т**	**Е**
(12,35)	(7,23)	(22,9)	(29,40)	(19,5)	(7,23)	(19,5)	(19,38)	(3,39)

М	**.**	**А**	**Л**	**И**	**С**	**А**	**_**
(16,36)	(30,10)	(0,14)	(16,7)	(7,23)	(19,5)	(0,14)	(29,40)

После кодирования текста Алиса поэлементно накладывает на него гамма-последовательность Г и производит его гаммирование с операцией вычисления кратной точки на эллиптической кривой (табл. 6).

Таблица 6

Гаммирование

Table 6

Gamma encryption

(0,14)	**(16,7)**	**(7,23)**	**(19,5)**	**(0,14)**	**(29,40)**	**(7,23)**	**(29,40)**	**(0,29)**
35	13	25	25	35	31	22	28	43
(12,8)	(2,25)	(18,25)	(17,18)	(12,8)	(42,7)	(16,36)	(33,12)	(36,11)

(17,25)	**(0,29)**	**(29,40)**	**(29,3)**	**(2,18)**	**(16,7)**	**(29,3)**	**(28,36)**	**(19,38)**
7	7	16	25	25	35	13	35	13
(36,32)	(18,20)	(29,3)	(16,27)	(28,7)	(32,22)	(24,18)	(25,32)	(7,23)

(19,5)	**(29,3)**	**(29,40)**	**(2,18)**	**(7,20)**	**(0,14)**	**(7,23)**	**(16,36)**	**(17,25)**
25	25	35	31	22	28	43	7	7
(17,18)	(6,27)	(29,40)	(22,9)	(16,7)	(17,25)	(22,9)	(7,23)	(36,32)

(3,4)	**(3,39)**	**(12,8)**	**(19,5)**	**(19,38)**	**(2,18)**	**(21,15)**	**(28,36)**	**(25,11)**
16	25	25	35	13	35	13	25	25
(7,23)	(22,34)	(36,11)	(41,38)	(7,23)	(36,11)	(21,15)	(28,36)	(16,7)

(7,23)	**(16,36)**	**(7,23)**	**(29,40)**	**(0,14)**	**(2,25)**	**(3,39)**	**(17,18)**	**(19,38)**
35	31	22	28	43	7	7	16	25
(3,39)	(35,8)	(16,36)	(33,12)	(36,32)	(41,5)	(28,36)	(35,35)	(17,25)

(0,14)	**(16,36)**	**(7,23)**	**(29,40)**	**(12,35)**	**(18,23)**	**(7,23)**	**(18,20)**	**(19,38)**
25	35	13	35	13	25	25	35	31
(2,18)	(32,21)	(41,38)	(29,40)	(25,32)	(41,38)	(18,23)	(22,9)	(16,36)

Окончание табл. 6

(17,25)	**(2,25)**	**(18,23)**	**(0,14)**	**(21,28)**	**(7,23)**	**(24,18)**	**(3,39)**	**(19,5)**
22	28	43	7	7	16	25	25	35
(25,32)	(7,20)	(19,38)	(18,23)	(39,25)	(3,4)	(39,35)	(22,34)	(41,38)

(12,35)	**(7,23)**	**(22,9)**	**(29,40)**	**(19,5)**	**(7,23)**	**(19,5)**	**(19,38)**	**(3,39)**
13	35	13	25	25	35	31	22	28
(2,18)	(3,39)	(17,25)	(6,16)	(17,18)	(3,39)	(16,7)	(36,32)	(0,29)

(16,36)	**(30,10)**	**(0,14)**	**(16,7)**	**(7,23)**	**(19,5)**	**(0,14)**	**(29,40)**
43	7	7	16	25	25	35	13
(12,35)	(29,3)	(18,23)	(32,21)	(18,23)	(17,18)	(12,8)	(24,25)

В результате гаммирования Алиса получает последовательность точек эллиптической кривой, из координат которой построчно формирует квадратные матрицы размером 4 × 4 и в итоге получает промежуточный шифр в виде последовательности матриц $T_{ii=1}^{10}$:

$$T_1 = \begin{pmatrix} 12 & 8 & 2 & 25 \\ 18 & 23 & 17 & 18 \\ 12 & 8 & 42 & 7 \\ 16 & 26 & 33 & 12 \end{pmatrix} \qquad T_6 = \begin{pmatrix} 36 & 32 & 41 & 5 \\ 28 & 36 & 35 & 35 \\ 17 & 25 & 2 & 18 \\ 32 & 21 & 41 & 38 \end{pmatrix}$$

$$T_2 = \begin{pmatrix} 36 & 11 & 36 & 32 \\ 18 & 20 & 29 & 3 \\ 6 & 27 & 28 & 7 \\ 32 & 22 & 24 & 18 \end{pmatrix} \qquad T_7 = \begin{pmatrix} 29 & 40 & 25 & 32 \\ 41 & 38 & 18 & 23 \\ 22 & 9 & 16 & 36 \\ 25 & 32 & 7 & 20 \end{pmatrix}$$

$$T_3 = \begin{pmatrix} 25 & 32 & 7 & 23 \\ 17 & 18 & 6 & 27 \\ 29 & 40 & 22 & 9 \\ 16 & 7 & 17 & 25 \end{pmatrix} \qquad T_8 = \begin{pmatrix} 19 & 38 & 18 & 23 \\ 39 & 35 & 3 & 4 \\ 39 & 35 & 22 & 38 \\ 41 & 38 & 2 & 18 \end{pmatrix}$$

$$T_4 = \begin{pmatrix} 22 & 9 & 7 & 23 \\ 36 & 32 & 7 & 23 \\ 22 & 34 & 36 & 11 \\ 41 & 38 & 7 & 23 \end{pmatrix} \qquad T_9 = \begin{pmatrix} 3 & 39 & 17 & 25 \\ 6 & 16 & 17 & 18 \\ 3 & 39 & 16 & 7 \\ 36 & 32 & 0 & 29 \end{pmatrix}$$

$$T_5 = \begin{pmatrix} 36 & 11 & 21 & 15 \\ 28 & 36 & 16 & 7 \\ 3 & 39 & 35 & 8 \\ 16 & 36 & 33 & 12 \end{pmatrix} \qquad T_{10} = \begin{pmatrix} 12 & 35 & 29 & 3 \\ 18 & 23 & 32 & 21 \\ 18 & 23 & 17 & 18 \\ 12 & 8 & 24 & 25 \end{pmatrix}$$

Далее каждая матрица из полученной последовательности умножается слева на ключ-матрицу K по модулю $p = 43$ с использованием обратной связи по правилу (3):

$$C_1 = K \cdot T_1 (mod\ 43) = \begin{pmatrix} 10 & 41 & 39 & 4 \\ 20 & 3 & 34 & 17 \\ 12 & 3 & 37 & 34 \\ 36 & 1 & 19 & 6 \end{pmatrix} (mod\ 43),$$

$$C_2 = K \cdot T_2 + T_1 (mod\ 43) = \begin{pmatrix} 38 & 3 & 15 & 15 \\ 34 & 39 & 10 & 12 \\ 5 & 6 & 30 & 25 \\ 20 & 20 & 39 & 12 \end{pmatrix} (mod\ 43),$$

$$C_3 = K \cdot T_3 + T_2 (mod\ 43) = \begin{pmatrix} 11 & 10 & 2 & 21 \\ 12 & 4 & 8 & 37 \\ 14 & 0 & 37 & 25 \\ 12 & 21 & 25 & 36 \end{pmatrix} (mod\ 43),$$

$$C_4 = K \cdot T_4 + T_3 (mod\ 43) = \begin{pmatrix} 27 & 28 & 28 & 5 \\ 29 & 32 & 30 & 9 \\ 15 & 35 & 5 & 22 \\ 39 & 21 & 41 & 28 \end{pmatrix} (mod\ 43),$$

$$C_5 = K \cdot T_5 + T_4 (mod\ 43) = \begin{pmatrix} 40 & 17 & 20 & 19 \\ 23 & 27 & 17 & 35 \\ 26 & 10 & 5 & 27 \\ 4 & 40 & 11 & 20 \end{pmatrix} (mod\ 43),$$

$$C_6 = K \cdot T_6 + T_5 (mod\ 43) = \begin{pmatrix} 16 & 1 & 29 & 4 \\ 26 & 10 & 32 & 33 \\ 3 & 14 & 4 & 18 \\ 31 & 29 & 42 & 36 \end{pmatrix} (mod\ 43),$$

$$C_7 = K \cdot T_7 + T_6 (mod\ 43) = \begin{pmatrix} 15 & 29 & 7 & 35 \\ 21 & 7 & 15 & 24 \\ 33 & 0 & 10 & 38 \\ 27 & 32 & 26 & 14 \end{pmatrix} (mod\ 43),$$

$$C_8 = K \cdot T_8 + T_7 (mod\ 43) = \begin{pmatrix} 32 & 21 & 29 & 41 \\ 17 & 5 & 19 & 17 \\ 5 & 2 & 11 & 17 \\ 10 & 33 & 17 & 32 \end{pmatrix} (mod\ 43),$$

$$C_9 = K \cdot T_9 + T_8 (mod\ 43) = \begin{pmatrix} 1 & 28 & 6 & 22 \\ 19 & 7 & 8 & 24 \\ 27 & 37 & 5 & 39 \\ 20 & 35 & 30 & 13 \end{pmatrix} (mod\ 43),$$

$$C_{10} = K \cdot T_{10} + T_9 (mod\ 43) = \begin{pmatrix} 14 & 29 & 1 & 14 \\ 40 & 11 & 28 & 40 \\ 30 & 1 & 9 & 14 \\ 7 & 23 & 23 & 15 \end{pmatrix} (mod\ 43),$$

Полученная последовательность матриц $\{C_i\}_{i=1}^{10}$ представляет окончательный шифр, который Алиса отправляет Бобу.

Дешифрование

Боб, получив шифр в виде последовательности матриц $\{C_i\}_{i=1}^{10}$, приступает к его дешифрованию. Для этого он находит обратную матрицу по модулю $p = 43$ к ключ-матрице K:

$$K^{-1} (mod\ 43) = \begin{pmatrix} 33 & 12 & 24 & 25 \\ 33 & 31 & 21 & 28 \\ 42 & 7 & 6 & 16 \\ 24 & 25 & 33 & 12 \end{pmatrix}^{-1} (mod\ 43) = \begin{pmatrix} 29 & 9 & 40 & 5 \\ 8 & 36 & 19 & 3 \\ 30 & 34 & 26 & 17 \\ 22 & 7 & 6 & 41 \end{pmatrix}$$

и также обратные значения по модулю $N = 51$ к элементам гамма-последовательности Г:

$$35^{-1} = 35(mod\ 51) \qquad 31^{-1} = 28(mod\ 51) \qquad 43^{-1} = 19(mod\ 51)$$

$$13^{-1} = 4(mod\ 51) \qquad 22^{-1} = 7(mod\ 51) \qquad 7^{-1} = 22(mod\ 51)$$

$$25^{-1} = 49(mod\ 51) \qquad 28^{-1} = 31(mod\ 51) \qquad 16^{-1} = 16(mod\ 51)$$

В итоге обратная гамма-последовательность принимает вид:

$$\Gamma^{-1}\ (mod\ 51) = (35, 4, 49, 49, 35, 28, 7, 31, 19, 22, 22, 16, 49, 49, 35, 4).$$

После определения ключей дешифрования $K^{-1}\ (mod\ 51)$ и $\Gamma^{-1}\ (mod\ 51)$ Боб на первом этапе по дешифрующим формулам (4) умножает слева полученные от Алисы матрицы из последовательности $\{C_i\}_{i=1}^{10}$ на обратную ключ-матрицу с использованием связи с предыдущей матрицей и находит промежуточный шифр – последовательность матриц $\{T_i\}_{i=1}^{10}$:

$$T_1 = K^{-1} (mod\ 43) = \begin{pmatrix} 33 & 12 & 24 & 25 \\ 33 & 31 & 21 & 28 \\ 42 & 7 & 6 & 16 \\ 24 & 25 & 33 & 12 \end{pmatrix} (mod\ 43),$$

$$T_2 = K^{-1} \cdot \left(C_2 - T_1\right)(mod\ 43) = \begin{pmatrix} 36 & 11 & 36 & 32 \\ 18 & 20 & 29 & 3 \\ 6 & 27 & 28 & 7 \\ 32 & 22 & 24 & 18 \end{pmatrix} (mod\ 43),$$

$$T_3 = K^{-1} \cdot \left(C_3 - T_2\right)(mod\ 43) = \begin{pmatrix} 25 & 32 & 7 & 23 \\ 17 & 18 & 6 & 27 \\ 29 & 40 & 22 & 9 \\ 16 & 7 & 17 & 25 \end{pmatrix} (mod\ 43),$$

$$T_4 = K^{-1} \cdot \left(C_4 - T_3\right)(mod\ 43) = \begin{pmatrix} 22 & 9 & 7 & 23 \\ 36 & 32 & 7 & 23 \\ 22 & 34 & 36 & 11 \\ 41 & 38 & 7 & 23 \end{pmatrix} (mod\ 43),$$

$$T_5 = K^{-1} \cdot \left(C_5 - T_4\right)(mod\ 43) = \begin{pmatrix} 36 & 11 & 21 & 15 \\ 28 & 36 & 16 & 7 \\ 3 & 39 & 35 & 8 \\ 16 & 36 & 33 & 12 \end{pmatrix} (mod\ 43),$$

$$T_6 = K^{-1} \cdot \left(C_6 - T_5\right)(mod\ 43) = \begin{pmatrix} 36 & 32 & 41 & 5 \\ 28 & 36 & 35 & 35 \\ 17 & 25 & 2 & 18 \\ 32 & 21 & 41 & 38 \end{pmatrix} (mod\ 43),$$

$$T_7 = K^{-1} \cdot \left(C_7 - T_6\right)(mod\ 43) = \begin{pmatrix} 29 & 40 & 25 & 32 \\ 41 & 38 & 18 & 23 \\ 22 & 9 & 16 & 36 \\ 25 & 32 & 7 & 20 \end{pmatrix} (mod\ 43),$$

$$T_8 = K^{-1} \cdot \left(C_8 - T_7\right)(mod\ 43) = \begin{pmatrix} 19 & 38 & 18 & 23 \\ 39 & 35 & 3 & 4 \\ 39 & 35 & 22 & 38 \\ 41 & 38 & 2 & 18 \end{pmatrix} (mod\ 43),$$

$$T_9 = K^{-1} \cdot \left(C_9 - T_8\right)(mod\ 43) = \begin{pmatrix} 3 & 39 & 17 & 25 \\ 6 & 16 & 17 & 18 \\ 3 & 39 & 16 & 7 \\ 36 & 32 & 0 & 29 \end{pmatrix} (mod\ 43),$$

$$T_{10} = K^{-1} \cdot \left(C_{10} - T_9\right)(mod\ 43) = \begin{pmatrix} 12 & 35 & 29 & 3 \\ 18 & 23 & 32 & 21 \\ 18 & 23 & 17 & 18 \\ 12 & 8 & 24 & 25 \end{pmatrix} (mod\ 43),$$

На втором этапе дешифрования из упорядоченных матриц промежуточного шифра T_i (i = 1,…,10) Боб извлекает построчные срезы, составляет из их элементов последовательность числовых значений, которую затем разбивает на упорядоченные пары – точки эллиптической кривой. Далее для полученной последовательности точек Боб производит поэлементное наложение обратной гамма-последовательности Γ^{-1} (*mod* 51) и выполняет гаммирование с операцией умножения точки эллиптической кривой на числовой элемент обратной гамма-последовательности (табл. 7).

Таблица 7

Обратное гаммирование

Table 7

Inverse gamma encryption

(12,8)	**(2,25)**	**(18,25)**	**(17,18)**	**(12,8)**	**(42,7)**	**(16,36)**	**(33,12)**	**(36,11)**
35	4	49	49	35	28	7	31	19
(0,14)	(16,7)	(7,23)	(19,5)	(0,14)	(29,40)	(7,23)	(29,40)	(0,29)

(36,32)	**(18,20)**	**(29,3)**	**(16,27)**	**(28,7)**	**(32,22)**	**(24,18)**	**(25,32)**	**(7,23)**
22	22	16	49	49	35	4	35	4
(17,25)	(0,29)	(29,40)	(29,3)	(2,18)	(16,7)	(29,3)	(28,36)	(19,38)

(17,18)	**(6,27)**	**(29,40)**	**(22,9)**	**(16,7)**	**(17,25)**	**(22,9)**	**(7,23)**	**(36,32)**
49	49	35	28	7	31	19	22	22
(19,5)	(29,3)	(29,40)	(2,18)	(7,20)	(0,14)	(7,23)	(16,36)	(17,25)

(7,23)	**(22,34)**	**(36,11)**	**(41,38)**	**(7,23)**	**(36,11)**	**(21,15)**	**(28,36)**	**(16,7)**
16	49	49	35	4	35	4	49	49
(3,4)	(3,39)	(12,8)	(19,5)	(19,38)	(2,18)	(21,15)	(28,36)	(25,11)

(3,39)	**(35,8)**	**(16,36)**	**(33,12)**	**(36,32)**	**(41,5)**	**(28,36)**	**(35,35)**	**(17,25)**
35	28	7	31	19	22	22	16	49
(7,23)	(16,36)	(7,23)	(29,40)	(0,14)	(2,25)	(3,39)	(17,18)	(19,38)

(2,18)	**(32,21)**	**(41,38)**	**(29,40)**	**(25,32)**	**(41,38)**	**(18,23)**	**(22,9)**	**(16,36)**
49	35	4	35	4	49	49	35	28
(0,14)	(16,36)	(7,23)	(29,40)	(12,35)	(18,23)	(7,23)	(18,20)	(19,38)

(25,32)	**(7,20)**	**(19,38)**	**(18,23)**	**(39,25)**	**(3,4)**	**(39,35)**	**(22,34)**	**(41,38)**
7	31	19	22	22	16	49	49	35
(17,25)	(2,25)	(18,23)	(0,14)	(21,28)	(7,23)	(24,18)	(3,39)	(19,5)

Окончание табл. 7

(2,18)	**(3,39)**	**(17,25)**	**(6,16)**	**(17,18)**	**(3,39)**	**(16,7)**	**(36,32)**	**(0,29)**
4	35	4	49	49	35	28	7	31
(12,35)	(7,23)	(22,9)	(29,40)	(19,5)	(7,23)	(19,5)	(19,38)	(3,39)

(12,35)	**(29,3)**	**(18,23)**	**(32,21)**	**(18,23)**	**(17,18)**	**(12,8)**	**(24,25)**
19	22	22	16	49	49	35	4
(16,36)	(30,10)	(0,14)	(16,7)	(7,23)	(19,5)	(0,14)	(29,40)

В итоге описанных выше действий Боб получает набор точек эллиптической кривой, декодирует их в соответствующие символы алфавита по табл. 5 и тем самым восстанавливает открытый текст:

«АЛИСА_И_БОБ_ЯВЛЯЮТСЯ_ВЗАИМОДЕЙСТВУЮЩИМИ_
АГЕНТАМИ_КРИПТОГРАФИЧЕСКИХ_СИСТЕМ.АЛИСА_»

Последние 6 символов «АЛИСА_» дублируют начало текста, они были использованы для технической необходимости шифрования и не нарушают смысла исходного сообщения.

Замечание. Для повышения криптостойкости приведенного алгоритма для двух разных компонентов общего секретного ключа целесообразно использовать различные общие точки эллиптической кривой, сгенерированные по рекуррентной формуле (2).

Заключение

Рассмотренный в статье алгоритм двухэтапного шифрования имеет своей особенностью комплексный подход к защите текстовой информации, а именно: алгоритм комбинирует в себе симметричные и асимметричные методы классической криптографии с использованием точек эллиптической кривой, при этом на разных этапах шифрования использует различную математическую структуру шифруемых элементов. Как и любой комбинированный алгоритм шифрования, он сочетает в себе преимущества асимметричных эллиптических криптосистем с производительностью симметричных.

Криптографическая стойкость приведенного алгоритма основывается на трудоемкости решения задачи дискретного логарифмирования на эллиптических кривых (ECDLP) [16] и защищенности сервиса совместного доступа с безопасной аутентификацией взаимодействующих пользователей [17]. Блочная реализация второго этапа шифрования гарантирует стойкость шифра к статистическому анализу текста. Но, как и любая криптографическая система, базирующаяся на ключевом обмене Диффи – Хеллмана, предложенный алгоритм будет уязвим к атакам «человек посередине», так как не обеспечивает аутентификацию взаимодействующих пользователей. Использование данного алгоритма в комплексе с защищенными сервисами совместного доступа, предоставляющими доступ к общим данным только для уполномоченных пользователей через проверку их электронных цифровых подписей, позволяет минимизировать уязвимость к таким атакам и предоставляет надежную защиту конфиденциальности.

Список литературы

1. **Свечников С. Н.** Частотный анализ при использование классических криптоалгоритмов // Инновации в науке и практике. Уфа: Вестник науки, 2020. С. 57–62.
2. **Сергеева О. А., Кутовая А. С.** Основы криптографии: учеб.-метод. пособие [Электронный ресурс]; Кемеров. гос. ун-т. Электрон. дан. (2,26 Мб). Кемерово: КемГУ, 2024. Систем. требования: Intel Pentium (или аналогичный процессор других производителей), 1,2 ГГц; 512 Мб оперативной памяти; видеокарта SVGA, 1280x1024 High Color (32 bit); 2Мб свободного дискового пространства; операционная система Windows XP и выше; Adobe Reader. Загл. с экрана, № госрегистрации: 0322400576, 26.02.2024.
3. **Земор Ж.** Курс криптографии. М.-Ижевск: Регулярная и хаотическая динамика, 2019. 256 с.
4. **Гулевич С. А.** Общие сведения о современной криптографии и подходах к ее изучению // RATIO ET NATURA. 2022. № 2 (6).
5. **Кузнецов А. В., Шишкина, Э. Л.** Методы алгебраической геометрии в криптографии: учеб. пособие. Воронеж: Издательский дом ВГУ, 2023. 125 с.
6. **Жданов О. Н., Чалкин Т. А.** Эллиптические кривые и их применение в криптографии: учеб. пособие. Красноярск: СибГАУ, 2011. 65 с.
7. **Жданов О. Н., Чалкин Т. А.** Эллиптические кривые. Основы теории и криптографические приложения. URSS: Либроком, 2020. 200 с.
8. **Кутовая А. С., Сергеева О. А.** Комбинированный блочный алгоритм шифрования с открытым ключом на базе эллиптической кривой: в сб.: Фундаментальные и прикладные исследования в физике, химии, математике и информатике // Материалы симпозиума XIX (LI) Междунар. науч. конф. студентов, аспирантов и молодых ученых, г. Кемерово, 2024. Кемеров. гос. ун-ет. С. 151–154.
9. **Стрельцова А. С., Ухваркин С. П., Филимонов В. В.** Применение эллиптических кривых в алгоритме Диффи – Хеллмана // Научный альманах. 2019. № 1-3 (51). С. 62–64.
10. **Гущин А. В., Осипов М. Н.** Криптографические методы защиты информации: учеб. пособие. Самара, 2024. Самарский ун-т. 126 с.
11. **Кутовая А. С.** Матричные алгоритмы криптографической защиты информации // Фундаментальные и прикладные исследования в физике, математике и информатике. Кемерово: Кемеровский гос. ун-т, 2022. С. 171–174.
12. **Мунерман В. И.** Реализация алгоритма шифрования Хилла на основе алгебры многомерных матриц // Системы высокой доступности. 2019. Т. 15, № 1. С. 21–27.
13. **Жуков А. Е.** Системы блочного шифрования: учеб. пособие по курсу «Криптографические методы защиты информации». М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. 79 с.
14. **Карпов А. В., Ишмуратов Р. А.** Введение в криптографию: учеб. пособие. Казань: Казан. ун-т, 2024. 128 с.
15. **Молдовян А. А., Молдовян Д. Н., Левина А. Б.** Протоколы аутентификации с нулевым разглашением секрета: учеб. пособие. СПб: Университет ИТМО, 2016. 55 с.
16. **Семаев И. А.** О вычислении логарифмов на эллиптических кривых. Дискрет. матем., 1996. Т. 8, вып. 1. С. 65–71.
17. 13 сервисов для безопасного общего доступа и обмена файлами. URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351556.php (дата обращения: 23.09.2025).

References

1. **Svechnikov S. N.** Frequency analysis in the application of classical cryptographic algorithms. *Innovations in Science and Practice*. Ufa: LLC "Scientific Publishing Center "Vestnik Nauki"", 2020, p. 57–62.
2. **Sergeeva O. A., Kutovaya A. S.** Fundamentals of cryptography: educational and methodological guide [Electronic resource]; Kemerovo State University. Electronic data (2.26 MB). Kemerovo: KemSU, 2024. System requirements: Intel Pentium (or similar processor from other manufacturers), 1.2 GHz; 512 MB RAM; SVGA video card, 1280x1024 High Color (32 bit); 2 MB free disk space; Windows XP operating system or higher; Adobe Reader. Title from screen, State registration No.: 0322400576, 26.02.2024.
3. **Zémor G.** A course in cryptography. Moscow-Izhevsk: SRC "Regular and Chaotic Dynamics", 2019. 256 p.
4. **Gulevich S. A.** General information about modern cryptography and approaches to its study. *RATIO ET NATURA*. 2022. No. 2 (6).
5. **Kuznetsov A. V., Shishkina E. L.** Methods of algebraic geometry in cryptography: textbook. Voronezh: VSU Publishing House, 2023. 125 p.
6. **Zhdanov O. N., Chalkin V. A.** Elliptic curves and their application in cryptography: textbook. Krasnoyarsk: SibSAU, 2011. 65 p.
7. **Zhdanov O. N., Chalkin T. A.** Elliptic curves. Fundamentals of theory and cryptographic applications. Moscow: URSS: Librokom, 2020. 200 p.
8. **Kutovaya A. S., Sergeeva O. A.** Combined block encryption algorithm with public key based on elliptic curve. *In: Fundamental and Applied Research in Physics, Chemistry, Mathematics and Computer Science. Proceedings of the Symposium of the XIX (LI) International Scientific Conference of Students, Graduate Students and Young Scientists*, Kemerovo, 2024. Kemerovo: Kemerovo State University, 2024, p. 151–154.
9. **Streltsova A. S., Ukhvarkin S. P., Filimonov V. V.** Application of elliptic curves in the Diffie-Hellman algorithm. *Scientific Almanac*. 2019, no. 1-3 (51), p. 62–64.
10. **Gushchin A. V., Osipov M. N.** Cryptographic methods of information protection: textbook / A. V. Gushchin, M. N. Osipov. Samara: Samara University Publishing House, 2024. 126 p.
11. **Kutovaya A. S.** Matrix algorithms for cryptographic information protection. *Fundamental and Applied Research in Physics, Mathematics and Computer Science*. Kemerovo: Kemerovo State University, 2022, p. 171–174.
12. **Munerman V. I.** Implementation of the Hill encryption algorithm based on the algebra of multidimensional matrices. *Highly Available Systems*. 2019, vol. 15, no. 1, pp. 21–27.
13. **Zhukov A. E.** Block cipher systems: textbook for the course "Cryptographic methods of information protection". Moscow: Bauman MSTU Publishing House, 2013. 79 p.
14. **Karpov A. V., Ishmuratov R. A.** Introduction to cryptography: textbook. Kazan: Kazan University, 2024. 128 p.
15. **Moldovyan A. A., Moldovyan D. N., Levina A. B.** Zero-knowledge authentication protocols: textbook. St. Petersburg: ITMO University, 2016. 55 p.
16. **Semaev I. A.** On the computation of logarithms on elliptic curves. *Discrete Mathematics and Applications*. 1996, vol. 8, no. 1, pp. 65–71.
17. 13 services for secure shared access and file URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/351556.php (accessed: 23.09.2025).

Сведения об авторах

Сергеева Ольга Алексеевна, кандидат физико-математических наук, доцент кафедры фундаментальной математики Кемеровского государственного университета

Кутовая Анастасия Сергеевна, магистр, учитель математики и информатики СОШ № 31 им. В. Д. Мартемьянова

Сергеев Владислав Сергеевич, магистрант 2-го курса кафедры фундаментальной математики Кемеровского государственного университета

Information about the Authors

Olga A. Sergeeva, Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Fundamental Mathematics Kemerovo State University, Russia, Kemerovo

Anastasia S. Kutovaya, Master's degree holder, teacher of mathematics and informatics Secondary General Education School No. 31 named after V. D. Martemyanov

Vladislav S. Sergeev, Second-year master's student at the Department of Fundamental Mathematics Kemerovo State University

Статья поступила в редакцию 02.09.2025;
одобрена после рецензирования 15.11.2025; принята к публикации 15.11.2025

The article was submitted 02.09.2025;
approved after reviewing 15.11.2025; accepted for publication 15.11.2025