УДК 004.421.5

А. В. Кизино
Белорусский государственный технологический университет,
г. Минск, Беларусь

РАЗРАБОТКА МЕТОДА ШИФРОВАНИЯ КЛЮЧА НА ОСНОВЕ ДВИЖЕНИЯ МЫШИ

Аннотация. В докладе представлен метод создания криптографически стойкого ключа на основе движений мыши. Веб-приложение использует координаты 0X и 0Y, угол между векторами и скорость перемещения курсора для создания уникальных последовательностей. Метод рекомендован для криптографических систем в качестве метода для генерации случайных цифровых последовательностей.

A.V. Kizino
Belarusian State Technological University,
Minsk, Belarus

DEVELOPMENT OF A KEY ENCRYPTION METHOD BASED ON MOUSE MOVEMENT

Abstract. *The article presents a method for creating a cryptographically secure key based on mouse movements. The web application uses the coordinates 0X and 0Y, the angle between vectors, and the speed of cursor movement to create unique sequences. The method is recommended for cryptographic systems as a method for generating random digital sequences.*

Введение. Современные методы шифрования и кодирования основаны на числовых комбинациях или ключах, которые должны быть уникальными и безопасными. Слабые или повторяющиеся комбинации могут привести к взлому. Уникальный ключ в защите авторских прав – это цифровая подпись автора. Криптографически стойкие генераторы псевдослучайных чисел (ГПСЧ) имеют высокую степень энтропии благодаря непредсказуемым явлениям или физической активности (сетевая активность, активность жесткого диска, клавиатуры, движение мыши и т. д.) [1]. Другие методы генерации случайных последовательностей включают генерацию на основе радиоактивного распада, атмосферного шума и фотонных событий. Движения мыши моделируют двумерный хаос и могут генерировать 256-битные ключи, тогда как для криптографической безопасности достаточно 128-битных [2,3]. Микродвижения кисти при использовании мыши формируют уникальные координаты, отличающиеся даже при одинаковых действиях пользователя.

Движения мыши также используются для подтверждения личности, однако этот метод не является исчерпывающим из-за высокой энтропии [4]. Метод генерации ключа на основе движений мыши включает сбор данных о координатах курсора, скорости и направлении движения для создания последовательности случайных чисел, обеспечивая высокий уровень безопасности и непредсказуемости.

Предложенный метод обладает рядом преимуществ по сравнению с другими подходами к генерации случайных последовательностей. Во-первых, использование физических движений пользователя обеспечивает высокую степень непредсказуемости и устойчивости к воспроизведению. Во-вторых, данный метод не требует специализированного оборудования, в отличие от методов, основанных на радиоактивном распаде или фотонных событиях, и может быть легко реализован на любом персональном компьютере. В-третьих, высокая энтропия движений мыши обеспечивает более высокий уровень безопасности и уникальности генерируемых ключей, что делает данный метод надежным и эффективным для применения в криптографических системах.

Основная часть. Для реализации данного метода необходимо было определить начальное количество параметров, которые должен содержать ключ, который впоследствии будет преобразован в требуемый формат. На начальном этапе было решено выбрать четыре параметра: координата по оси 0X, координата по оси 0Y, угол между двумя случайными векторами последовательности и скорость перемещения курсора между двумя зафиксированными точками. В качестве начальной области был выбран квадрат размером 1000×1000 пикселей.

Для вычисления точек используются две системы координат: экранная и декартовая. Экранная система используется для получения позиции курсора в пределах указанной области, позволяя определять координаты в диапазоне [0;1000] и избегать перехода к отрицательным значениям. Декартовая система позволяет корректно вычислить угол в градусах между векторами, благодаря возможности использовать отрицательные координаты, что обеспечивает точное определение угла в диапазоне [0;180] градусов.

Кроме того, скорость вычисляется как расстояние между двумя точками, деленное на время между фиксациями точек. Скорость измеряется в пикселях в секунду, что позволяет учитывать мельчайшие изменения в движениях курсора и делает процесс генерации ключа более точным и непредсказуемым. Такой подход позволяет получить

данные высокой энтропии, что существенно повышает стойкость ключа к криптографическим атакам.

В результате исследовательской работы было разработано веб-приложение для генерации ключа на основе пользовательских движений мыши. Это приложение предназначено для создания криптографически стойких ключей, используя уникальные микродвижения мыши, которые трудно предсказать и воспроизвести. Для использования приложения необходимо запустить его на персональном компьютере и нажать кнопку «Старт». Затем пользователь должен выполнять хаотичные движения мышью в пределах обозначенной области на экране. Эти движения записываются и анализируются в реальном времени. По завершении генерации область блокируется, и на компьютере пользователя создается json-файл, содержащий сгенерированный ключ. Пример ключа, полученного за 10 секунд, представлен на рисунке 1.


```
{"Key":"416091ed2572e68a97385372f5e5878544decc066383ecd36d4c785f1b196f9ee498745b9a8db9516d4b9d
67da4e1c3b155d9f5ed9c1d08f8a44d1763fecefd8ff97b0600ff26172754a6a64405590dcb419929e11546b933838
90f3a5e128a7fec868d13ec2fa001e9ee59dbb39994ce637fb4ff45c558593376decc6801fd8d30e756ba41e0fb445
8eff008e1f28f2a1b021bb3670b188d8843764b74f545986f3197b657b1437a7865a05113fc07fb74d60877b4960a9
cf793c06e34d84a13323095731f1a6a448101d90468bcf38bccc7a1ccb23dd484b8addbe7f7ebd425589bf4f1f4d3c
e893ecdb73969c1faead519618b27486d11aa75a72bcd3867e4971d55771bb43111c1ed962e74036ce6653097b7f8e
995c49ed6e7ed7246b1f08344f3aa07ff46d0fa6fcdb5467687a5a4a9b7a09ca77c11f60d19c5736576654e0e045b7
2431024ec160ed97b30392c7f79b0f5f1d76212a26f7ac77f94bf25396c57b39c347156c92b8e3655f0f73633974b0
98b6719248888fa685bc13ac5743245f0f042fcefce6802f1abd60692f1a9fe1a22edf03b8132d79346e242a727699
3f2d3ebc178c50a60b41ef5371a65f174e52b5965a4b87a0b85a4a9937de3548f7fa77c447926948414668743a7d45
b5b0e46f457a184138457a2558c745f1a72860462d6fc8bc462d802ff446e060ce1846e06f6477471c28226c4d6589
acd9726cf12e856e7e2a1e2c4d30d902e032d6ad3d5e4efeabc2a46d8aac9f9d418d361218127c6e2cfe3779782642
5d392a90315bd7a7bcad5550f0a89c686326224a8153a525a370610547a76a18a79c906d561c04a66fe43511a0"}
```


Рис 1. Сгенерированный ключ

Для определения вероятности генерации двух одинаковых ключей была использована формула из теории вероятности. Вероятность P генерации двух идентичных ключей может быть вычислена как P=1/N, где N - общее количество возможных уникальных ключей. При длине ключа в 256 бит количество возможных комбинаций равно 2^{256}. Таким образом, вероятность получения двух одинаковых ключей составляет:

$$P = \frac{1}{2^{256}}$$

Это значение примерно равно 1.5×10−771.5, что показывает, что вероятность дублирования ключей практически стремится к нулю.

Среднее время подбора ключа методом грубой силы было оценено с учетом общей энтропии сгенерированного ключа и вычислительных возможностей современных систем. Метод грубой силы подразумевает перебор всех возможных комбинаций до нахождения правильного ключа. В нашем случае среднее время подбора ключа составило $5{,}79\times10^{65}$ лет, что является более чем удовлетворительным для использования в криптографически стойких

системах. Это время было рассчитано с учетом текущих технологий и скорости вычислений, что гарантирует высокий уровень безопасности созданных ключей.

Вывод. В результате исследования был разработан веб-приложение для генерации криптографически стойких ключей на основе движений мыши. Приложение записывает хаотичные движения курсора в пределах обозначенной области экрана, анализируя их в реальном времени. Вероятность генерации двух одинаковых ключей вычисляется по формуле из теории вероятности и составляет 1.5×10^{-77}, что практически исключает дублирование. Среднее время подбора ключа методом грубой силы оценивается в 5.79×10^{65} лет. Это подтверждает высокий уровень безопасности и делает метод надежным для использования в криптографических системах.

Список использованных источников

1. Картушев Н.А., Морозова А.А. Принцип работы генератора случайных паролей [Электронный ресурс] // Теория и практика современной науки. 2017. №9 (27). Режим доступа: https://cyberleninka.ru/article/n/printsip-raboty-generatora-sluchaynyh-paroley (дата обращения: 10.10.2024).
2. Hu Y., Liao X., Wong K.-w., Zhou Q. A true random number generator based on mouse movement and chaotic cryptography [Электронный ресурс] // Chaos, Solitons & Fractals. 2009. Vol. 40. No. 5. P. 2286-2293. ISSN 0960-0779. Режим доступа: https://doi.org/10.1016/j.chaos.2007.10.022 (дата обращения: 10.10.2024).
3. Lucks S. On the Security of the 128-bit Block Cipher DEAL [Электронный ресурс] // Knudsen L. (ред.) Fast Software Encryption. FSE 1999. Lecture Notes in Computer Science, vol 1636. Springer, Berlin, Heidelberg, 1999. Режим доступа: https://doi.org/10.1007/3-540-48519-8_5 (дата обращения: 10.10.2024).
4. Осин А.В., Мурашко Ю.В. Обзор методов идентификации пользователя на основе цифровых отпечатков [Электронный ресурс] // Труды учебных заведений связи. 2023. №5. Режим доступа: https://cyberleninka.ru/article/n/obzor-metodov-identifikatsii-polzovatelya-na-osnove-tsifrovyh-otpechatkov (дата обращения: 10.10.2024).
5. Schrittwieser S., Katzenbeisser S. Code Obfuscation against Static and Dynamic Reverse Engineering [Электронный ресурс] // Filler T., Pevný T., Craver S., Ker A. (ред.) Information Hiding. IH 2011. Lecture Notes in Computer Science, vol 6958. Springer, Berlin, Heidelberg, 2011. Режим доступа: https://doi.org/10.1007/978-3-642-24178-9_19 (дата обращения: 11.10.2024).