УДК 004.056.55

ЗАЩИЩЕННАЯ ПЕРЕДАЧА ДАННЫХ В СИСТЕМЕ IOT ПРИ ПОМОЩИ МЕТОДА XOR

© 2024 И. А. Сырцов[1], Л.С. Крыжевич[2]

[1]студент направления подготовки 09.03.01 – Информатика и вычислительная техника
e-mail: ivansyrcov26@gmail.com
[2]кандидат технических наук, и.о. заведующего кафедрой информационной безопасности КГУ
e-mail : leonid@programist.ru

Курский государственный университет

В статье рассматривается использование метода XOR для шифрования данных в устройствах интернета вещей. Описаны принципы криптостойкости данного метода шифрования, принцип получения случайной последовательности чисел. На основе данного шифрования представлен пример системы интернета вещей, в которой реализовано шифрование методом XOR.

Ключевые слова: шифрование, сумма по модулю 2, XOR, гаммирование, интернет вещей, IoT, умные устройства

SECURE DATA TRANSFER IN THE IOT SYSTEM USING THE XOR METHOD

© 2024 I. A. Syrtsov[1], L. S. Kryzhevich[2]

[1]Student of the training direction 03.09.01 – Informatics and Computer Science
e-mail: ivansyrcov26@gmail.com
[2]Candidate of Technical Sciences
e-mail: leonid@programist.ru

The article discusses the use of the XOR method for encrypting data in Internet of Things devices. The principles of the cryptographic strength of this encryption method are described. The principle of obtaining a random sequence of numbers is also described. Based on this encryption, an example of an Internet of Things system is presented, in which encryption is implemented using the XOR method.

Keywords: encryption, modulo 2 sum, XOR, stream cipher, Internet of Things, IoT, smart devices.

В настоящее время системы интернета вещей (IoT) стали неотъемлемой частью современной жизни. Устройства IoT используются в различных областях, включая умные дома, здравоохранение, промышленную автоматизацию и сельское хозяйство. Однако вместе с их распространением увеличиваются и угрозы безопасности данных, передаваемых между устройствами. Защищенная передача данных является критическим аспектом, особенно в условиях все более усложняющихся кибератак и утечек информации. Согласно отчету Zscaler, количество атак на IoT устройства увеличилось на 700 % с 2019 г. По состоянию на 2021 г. только 24 % устройств IoT используют шифрование при передаче данных, оставляя 76 % устройств интернета

вещей полностью незащищенными [4; 5]. В связи с этим необходимость в надежных методах шифрования данных, которые обеспечивают конфиденциальность и целостность информации, возрастает.

Один из эффективных способов защиты данных в системах интернета вещей – использование метода XOR, или сумма по модулю 2. Этот метод базируется на шифровании данных с использованием случайной последовательности, называемой «гаммой». Криптостойкость данного шифрования обеспечивается правильным формированием гаммы. Согласно требованиям к гамме, повторное использование гаммы недопустимо, ввиду избыточности естественных языков результат поддаётся частотному анализу, то есть открытые тексты можно подобрать, не зная гамму. Также для формирования гаммы необходимо использовать последовательность случайных чисел, ведь если гамма не будет случайной, то для получения открытого текста потребуется подобрать только начальное состояние генератора псевдослучайных чисел. Длина гаммы также не может быть меньше длины открытого текста, ведь в противном случае для получения открытого текста потребуется подобрать длину гаммы, проанализировать блоки шифротекста угаданной длины, подобрать биты гаммы [3].

Примером реализации данного шифрования может служить система, в которой существуют следующие участники:

1. Умные устройства. Это физические устройства, оснащенные датчиками и микроконтроллером, способные собирать разнообразные данные, например, данные о климате, уровне освещенности или энергопотреблении. Каждое устройство осуществляет шифрование собранных данных и передает их на удаленный сервер для дальнейшей обработки [2].
2. База данных. Данный компонент представляет собой удаленное хранилище информации, где сохраняются собранные и обработанные данные от умных устройств.
3. Клиентское приложение. Данный компонент может принимать различные формы, такие как чат-бот в мессенджере, веб-приложение или мобильное приложение. Клиентское приложение получает данные от базы данных, расшифровывает их с помощью соответствующего ключа и предоставляет пользователю информацию о состоянии. Также клиентское приложение может использовать данные внутри себя для выполнения различных операций или аналитики.
4. Удостоверяющий центр. Это центр генерации ключей, может являться одним из клиентских приложений.

Принцип работы данной системы включает в себя несколько этапов. Первым этапом является «рукопожатие». Умное устройство отправляет в базу данных системное сообщение, которое впоследствии передается в клиентское приложение. В данном случае база данных служит неким буфером, всегда хранящим переданное сообщение, потому как если клиентское приложение по каким-либо причинам не примет сигнал, то так и не узнает, что умное устройство включилось в систему. Пример данного этапа можно наблюдать на рисунке 1.

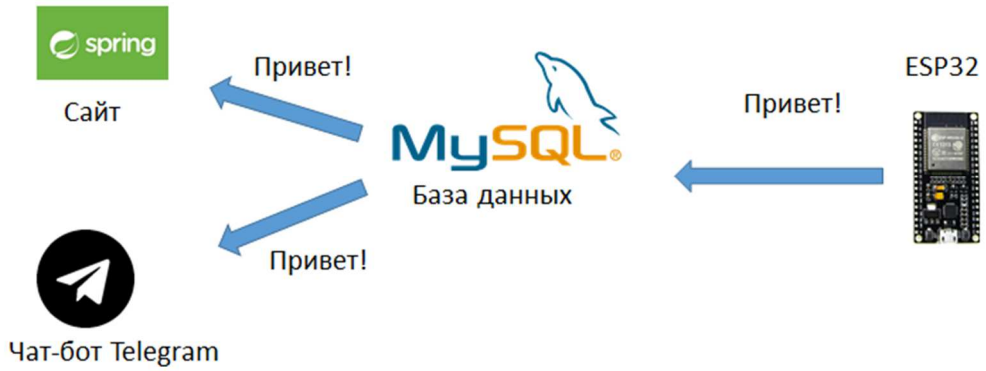

Рис. 1. Метод инициализации «Рукопожатие»

Следующим этапом является рассылка ключей, которая также происходит с помощью метода «сумма по модулю 2». Для этого у всех участников системы записана изначальная случайная последовательность, с помощью которой будет шифроваться и расшифровываться сгенерированный ключ, генерацией которого занимается чат-бот, являясь удостоверяющим центром. На рисунке 2 представлен алгоритм получения ключа.

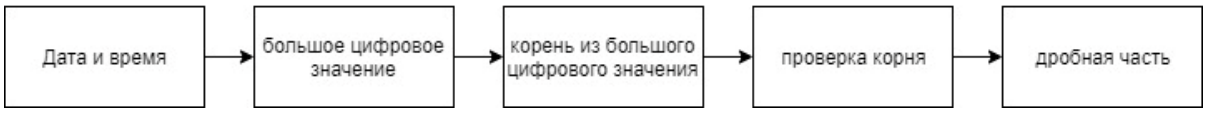

Рис. 2. Получение гаммы

Уникальное слово есть мгновенная дата и время, из этого следует, что большое цифровое значения всегда будет отличаться, как следствие – будет отличаться и дробная часть корня этого значения. Благодаря тому что дробная часть числа бесконечна, требования о равенстве гаммы и ее неповторимости соблюдены, также распределение чисел в дробной части соответствует равномерному распределению и является псевдослучайным, на рисунке 3 представлена гистограмма равномерного распределения.

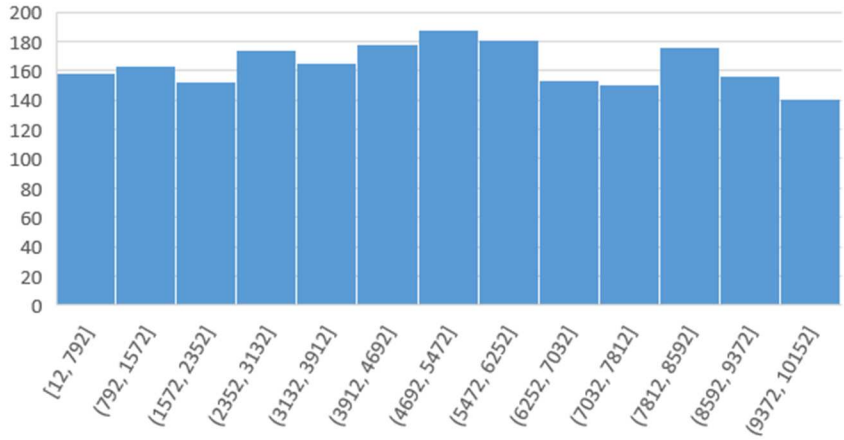

Рис. 3. Гистограмма равномерного распределения

Таким образом, после генерации ключа происходит операция «сумма по модулю 2» изначальной последовательности со сгенерированной. Далее происходит рассылка ключа и последующая расшифровка на умном устройстве. Для того чтобы удостоверяющий центр знал, что ключ получен и можно генерировать новое значение, остальные участники системы информируют удостоверяющий центр о получении и успешной расшифровке переданного сообщения. Пример данного этапа представлен на рисунке 4.

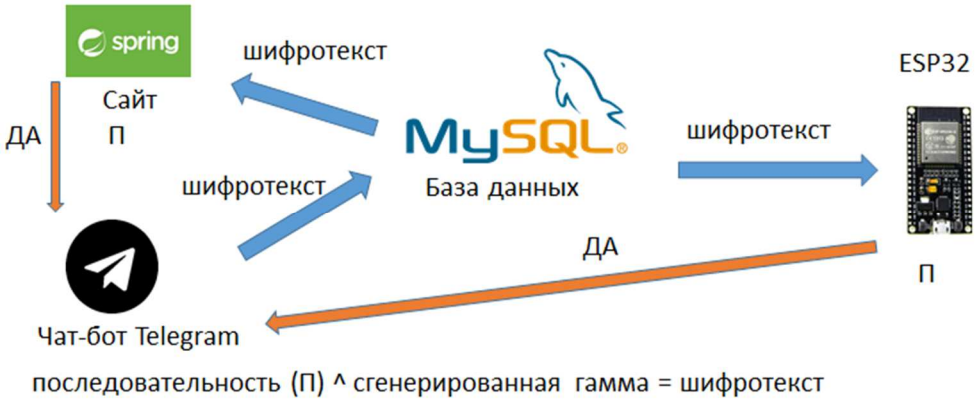

Рис. 4. Рассылка ключей

Следующим этапом является получение умным устройством данных с сенсоров, шифрование полученным ключом и отправка в базу данных, откуда в дальнейшем данные будут отправлены в клиентское приложение, которое расшифрует сообщение и выдаст пользователю или будет использовать для выполнения различных операций внутри себя. Далее система возвращается к этапу генерации и рассылки нового ключа, который впоследствии шифруется с помощью последовательности, сгенерированной в прошлой итерации системы. Все участники системы знают прошлый сгенерированный ключ, поэтому смогут расшифровать новый.

Стоит отметить, что при генерации или получении новой гаммы старая забывается (исключением является лишь изначальная последовательность), в результате чего будут утеряны ключи дешифрования к переданным с умных устройств данным в случае долговременного хранения их в зашифрованном виде в базе данных. В данном случае есть два решения проблемы. Первым вариантом является хранение всех ключей в базе данных, но если злоумышленник расшифрует один из ключей, то получит доступ ко всем остальным, как следствие – получит доступ к данным. Вторым и более правильным вариантом является перешифровка данных с помощью других методов шифрования, например, отечественный шифр «Кузнечик». При реализации данной системы был выбран именно 2-й вариант. Пример работы заключительного этапа представлен на рисунке 5. На рисунке 6 представлен пример данных, зашифрованных методом «сумма по модулю 2».

Рис. 5. Заключительный этап

id	encrypted
1	0x7c 0x62 0x2f 0x5a 0x27 0x35 0x40 0x14 0x37 0x17 0x15 0x1a 0x33 0x4 0x1c 0x6b 0x6d 0x37 0x6b 0x26 0x62 0x31 0x6a 0xa 0x1d
2	0xd 0x9 0xb 0x0 0xa 0x4 0x1 0xf 0x5 0x0 0x1 0xb 0x9 0x6 0x7 0x7 0x5 0x2 0x6 0xf 0xc 0xa 0xf 0x1 0x5 0x6 0x3 0x2 0x4 0x9 0x5 0x8 0xc 0x0 0x0 0x5 0x3 0x5 0x3 0x6 0x1 0x7 0x2 0x7 0x2 0x1 0x3 0x2 0xe 0x5

Рис. 6. Зашифрованные данные

Одной из особенностей данной системы является то, что изначальный ключ должен содержаться в строгом секрете, потому как в случае его раскрытия при первом этапе рассылки ключей злоумышленник узнает новый ключ и поэтому получит доступ к открытому тексту. Данная уязвимость может минимизироваться алгоритмом смены изначального ключа [1].

Таким образом, использование метода XOR для шифрования данных в IoT системах является надежным и эффективным способом защиты информации. Этот подход обеспечивает безопасность и конфиденциальность данных, что является ключевым фактором для успешного функционирования и развития умных систем в современных условиях. Внедрение таких методов позволяет повысить доверие пользователей и соответствовать современным требованиям безопасности, делая IoT системы более устойчивыми к угрозам и атакам.

Библиографический список

1. Основы теории кодирования: учеб. пособие. – СПб.: БХВ-Петербург, 2016. – 400 с.
2. Проблемы безопасности интернета вещей: учебное пособие – М.: Мир науки, 2021 [Электронный ресурс]. – URL: https://izd-mn.com/PDF/20MNNPU21.pdf.
3. *Шурховецкий, Г. Н.* Криптостойкость алгоритмов шифрования [Электронный ресурс] // Молодая наука Сибири: электрон. науч. журн. – 2018. – № 2. – Режим доступа: http://mnv.irgups.ru/toma/22-2018.
4. Cyber Attacks on IoT Devices Are Growing at Alarming Rates [Encryption Digest 64] [Электронный ресурс]. – URL: https://venafi.com/blog/cyber-attacks-iot-devices-are-growing-alarming-rates-encryption-digest-64/ (дата обращения: 12.05.2024).
5. IoT Security: Key Findings from Nokia's 2023 Threat Intelligence Report [Электронный ресурс]. – URL: https://www.electropages.com/blog/2023/06/rising-security-threat-iot-cyberattacks-nokias-latest-report (дата обращения: 12.05.2024).