# ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В ПРОЦЕССЕ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ

*Филиппов Н.С.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Саломатин С.Б. – к.т.н.,доцент*

В работе рассмотрен и реализован алгоритмы шифрования и цифровой подписи, основанные на эллиптических кривых, с целью защиты персональных данных пользователей в процессе разработки веб-приложений. Произведен анализ криптостойкости алгоритмов.

В процессе разработки веб-приложений часто возникают задачи, для выполнения которых необходимо взаимодействовать с клиентской базой данных, содержащей в себе персональные данные пользователей. Защиту персональных данных на территории Евросоюза регулирует «Общий регламент о защите данных».

*GDPR* (*General Data Protection Regulation*) - это новый всеобъемлющий закон о защите данных (вступивший в силу 25 мая 2018 г.) в ЕС, который усиливает защиту персональных данных в свете быстрого технологического развития, усиления глобализации и более сложных международных потоков персональных данных. Он обновляет и заменяет набор действующих национальных законов о защите данных на единый свод правил, которые могут применяться в каждом государстве-члене ЕС. *GDPR* регулирует «обработку» данных для лиц из стран ЕС, которая включает сбор, хранение, передачу или использование. Любая организация, которая обрабатывает персональные данные лиц из ЕС, подпадает под действие закона, независимо от того, имеет ли организация физическое присутствие в ЕС. *GDPR* также включает в себя обязательные корпоративные правила для организаций, которые узаконивают передачу персональных данных за пределы ЕС, и штраф в размере 4% от годовой выручки для организаций, которые не выполняют обязательств по соблюдению *GDPR*.

В ходе работы были реализованы алгоритмы шифрования и цифровой подписи на языке программирования *Python*. Так как криптография на эллиптических кривых не предоставляет прямого метода шифрования, то для решения этой проблемы была использована гибридная схема шифрования, использующая схему обмена ключами ECDH (*Elliptic Curve Diffie-Hellman*), чтобы получить общий секретный ключ для симметричного шифрования и дешифрования данных.

Процессы шифрования и дешифрования, используя гибридную схему, представлены на рисунках 1 и 2.

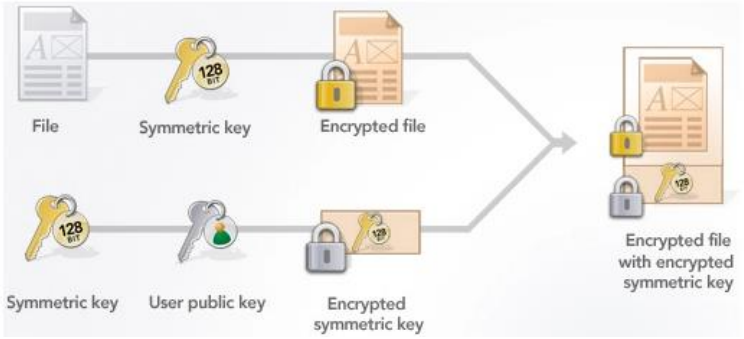


Рисунок 1 – Процесс шифрования

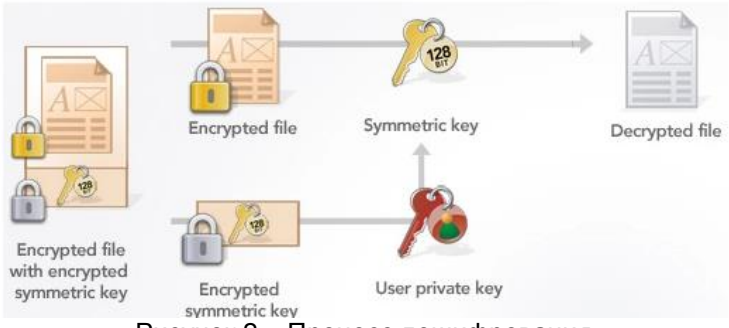


Рисунок 2 – Процесс дешифрования

В случае гибридной схемы симметричный ключ отправляется в зашифрованном виде с помощью асимметричного открытого ключа. Это означает, что только авторизованный получатель с соответствующим закрытым ключом может принять и расшифровать переданный симметричный

ключ. В то же самое время отправитель симметричного ключа использует свой закрытый ключ для создания электронной подписи с помощью алгоритма *ECDSA* (*Elliptic Curve Digital Signature Algorithm*), которая позволяет получателю, используя соответствующий открытый ключ, однозначно его идентифицировать. Основа для организации симметрично зашифрованного канала связи будет заложена только после того, как произошел обмен этими ключами, и они были расшифрованы.

Этот комбинированный способ устраняет следующие недостатки, а именно: небезопасная передача ключа для симметричного шифрования и малая скорость, присущая асимметричной технологии шифрования.

В ходе работы была выбрана эллиптическая кривая secp256k1, так как в соответствии с текущим уровнем техники, безопасный уровень криптостойкости при использовании эллиптических кривых достигается при использовании 256-битных ключей.

Результаты шифрования данных различной длины представлены в таблице 1 и рисунке 1.

Таблица 1 – Результаты шифрования и дешифрование данных различной длины

| Длина сообщения, Мб. | Длина зашифрованного сообщения, Мб. | Время шифрования, с. | Время дешифрования, с. |
|---|---|---|---|
| 0,001 | 0,002213 | 0,080 | 0,053 |
| 0,01 | 0,020213 | 0,084 | 0,054 |
| 0,1 | 0,200213 | 0,085 | 0,054 |
| 1 | 2,000213 | 0,11 | 0,056 |
| 2 | 4,000213 | 0,12 | 0,057 |

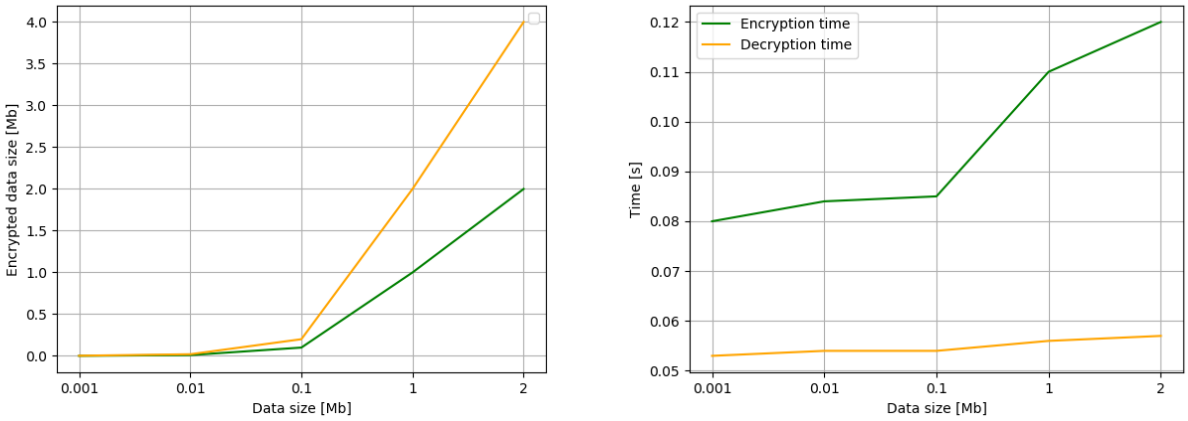


Рисунок 1 - Результаты шифрования и дешифрование данных различной длины

В заключении можно отметить, что шифрование с использованием алгоритмов, основанных на эллиптических кривых, увеличивает размер исходных данных в 2 раза, а время. Шифрование данных требует больше времени, чем дешифрование. Общее затраченное время увеличивается пропорционально изменению длины исходного сообщения.

Главным преимуществом эллиптической криптографии над остальными способами криптографии является малый размер ключа относительно других схем асимметричного шифрования. Это свойство особенно важно при реализации криптографических протоколов в условиях ограниченности ресурсов памяти и производительности. Также следует отметить, что помимо общих алгоритмов арифметики эллиптических кривых, существует много специфических алгоритмов, разработанных для кривых специального вида, которые позволяют добиться еще большего преимущества в эффективности.

***Список использованных источников:***

1. *SEC 2: Recommended Elliptic Curve Domain Parameters. Daniel R. L. Brown. – NIST, 2010 – 37 с.*
2. *Болотов А. А., Гашков С. Б., Фролов А. Б. Глава 2. Протоколы на эллиптических кривых // Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. — М.: КомКнига, 2006. — С. 83—86.*
3. *Elliptic Curve Digital Signature Algorithm. D. Johnson, A. Meneses. – 2000 – 55 с.*
4. *Elaine Barker, Lily Chen, Allen Roginsky, Miles Smid. Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography - http://nvlpubs.nist.gov/. — National Institute of Standards and Technology, 2013.*