РОЗРОБКА СИСТЕМИ АВТОМАТИЗОВАНОГО ПРОЕКТУВАННЯ КОМБІНОВАНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Надірян Г.О., Челак В.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Важливість захисту даних зростає, оскільки обсяг даних продовжує зростати з безпрецедентною швидкістю. Крім того, навички та можливості вилучення різних типів персональних даних розвиваються надзвичайно швидко. Несанкціонована обробка особистих даних може завдати великої шкоди людям і компаніям.

У доповіді представлено об'єднання трьох різних типів алгоритмів шифрування для того, щоб використовувати переваги кожного з них, і спроектувати систему, яка забезпечує високий рівень безпеки.

В ході проведення дослідження було проведено порівняльний аналіз криптографічних алгоритмів, з метою виявлення засобів, які повинні забезпечити більш високу точність, безпеку та ефективність [1].

Кожен алгоритм шифрування має як свої переваги, так і недоліки. Щоб усунити недоліки кожного з шифрів запропоновано використовувати комбіновані алгоритмі шифрування.

Основна частина роботи розглядає симетричний алгоритм AES, що використовується для шифрування даних, асиметричного RSA для обміну ключем (шифрування ключа) і HMAC-SHA512 для аутентифікація між сервером-клієнтом.

Отримані результати показали можливість використання комбінованих алгоритмів шифрування для того, щоб забезпечити більш високий рівень зберігання даних та їх безпечну передачу.

Літератури:

1. *Zoran Hercigonja* Comparative Analysis of Cryptographic Algorithms. Режим доступу: https://ijireeice.com/wp-content/uploads/2013/03/IJIREEICE10-a4-nivetha-A-COMPARATIVE-ANALYSIS-OF-CRYPTOGRAPHY-ALGORITHMS.pdf, 2016