РЕФЕРАТ

Актуальність теми. З поглибленням цифровізації сучасного суспільства виникають нові виклики у забезпеченні конфіденційності та безпеки інформації, яка обмінюється через комп'ютерні мережі. Асиметричні алгоритми шифрування стають ключовими інструментами у захисті даних від несанкціонованого доступу.

Об’єктом дослідження є процес передачі інформації в комп'ютерних мережах, де дані зашифровані асиметричними алгоритмами.

Предметом дослідження є вивчення та аналіз ефективності асиметричних алгоритмів у забезпеченні безпеки передачі інформації через комп'ютерні мережі.

Мета роботи. дослідження та оцінка застосування асиметричних алгоритмів у передачі зашифрованої інформації в комп'ютерних мережах, а також розробка рекомендацій щодо покращення процесів шифрування та дешифрування даних.

Наукова новизна. Розроблений застосунок дозволяє відправляти повідомлення, зашифровані асиметричними алгоритмами. Застосунок демонструє наглядність роботи асиметричного шифрування та можливість використовувати ці алгоритми через готовий інтерфейс.

Практична цінність. Результати дослідження можуть бути використані для розробки та удосконалення засобів захисту інформації в різних сферах, включаючи фінанси, медицину та галузі, пов'язані із зберіганням особистих даних.

Апробація роботи. Основні положення та результати роботи були представлені та обговорювались на V Міжнародній науково-практичній конференції молодих вчених та студентів «Інженерія програмного забезпечення і передові інформаційні технології» (SoftTech-2023)

Структура та обсяг роботи. Дипломна робота складатиметься з вступу, чотирьох розділів, висновків та списку використаних джерел літератури. Загальний обсяг роботи буде складати 72 сторінки.

Ключові слова: асиметричне шифрування, шифрування, асиметричні алгоритми шифрування

ABSTRACT

Relevance of the topic. With the deepening digitization of contemporary society, new challenges arise in ensuring the confidentiality and security of information exchanged through computer networks.

The object of research is the process of transmitting information in computer networks where data is encrypted using asymmetric algorithms.

The subject of research is the study and analysis of the effectiveness of asymmetric algorithms in securing the transmission of encrypted information in computer networks, as well as the development of recommendations for improving data encryption and decryption processes.

The purpose of the study. The goal of this thesis is to investigate and evaluate the application of asymmetric algorithms in the transmission of encrypted information in computer networks, as well as to develop recommendations for improving encryption and decryption processes.

Scientific novelty. The developed application allows sending messages encrypted with asymmetric algorithms. The application demonstrates the transparency of asymmetric encryption and the ability to use these algorithms through a ready-made interface.

The practical value of obtained results can be used to develop and improve information security tools in various sectors, including finance, medicine, and areas related to the storage of personal data.

Approval of the work. The main provisions and results of the work were presented and discussed at the V International Scientific and Practical

Conference of Young Scientists and Students "Software Engineering and Advanced Information Technologies" (SoftTech-2023).

Structure and scope of the work. The thesis will consist of an introduction, four chapters, conclusions, and a list of used literature sources. The total volume of the work will be 72 pages.

Keywords: asymmetric encryption, encryption, asymmetric encryption algorithms