

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ДЛЯ ШИФРУВАННЯ ТА ДЕШИФРУВАННЯ ДАНИХ

Старовіт А.В., науковий керівник Міловідов Ю.О.

У сучасному світі в якому цифрові технології відіграють значну роль у всіх сферах життя, питання захисту інформації набуває особливої актуальності. Кожного дня передаються та зберігаються величезні обсяги даних, серед яких також є конфіденційні та особисті. Забезпечення їхньої безпеки є одним із пріоритетів інформаційних систем. Одним із найефективнішим способів захисту інформації є використання методів шифрування та дешифрування.

Програмне забезпечення системи для шифрування та дешифрування даних дозволяє перетворювати відкриту інформацію у зашифрований вигляд, який неможливо прочитати без наявності спеціального ключа шифрування. Водночас, дешифрування дає змогу відновити початковий вигляд даних для уповноважених користувачів. Така система є важливою складовою в сферах кібербезпеки, електронного документообігу, банківських систем, захищеного зберігання тощо.

Існує безліч алгоритмів шифрування даних. Для вибору підходящого алгоритму проведено порівняння різних алгоритмів за їх складністю реалізації, швидкості роботи, безпеці, ресурсомісткості, перевагами та недоліками.

Алгоритми та їх принципи роботи:

- XOR – Кожен біт тексту поєднується з ключем за допомогою логічної операції XOR (^).
- AES – Дані поділяються на блоки по 128 бітів. Кожен блок проходить серію раундів, які включають підстановки, перестановки, зміщення стовпців і додавання ключа.
- RSA – Дані шифруються відкритим ключем і розшифровуються приватним. Побудований на основі математичної складності факторизації великих простих чисел.
- Caesar – Кожну літеру алфавіту зсувають на фіксовану кількість позицій.
- DES/3DES – Шифрує дані блоками по 64 біти з ключем по 56 бітів. Застосовує 16 раундів перестановок і підстановок.

Алгоритм	XOR	AES	RSA	Caesar	DES/3DES
Складність реалізації	Дуже проста	Складна	Дуже складна	Дуже проста	Середня
Швидкість роботи	Дуже висока	Висока	Низька	Висока	Середня
Безпека	Низька-середня (залежить від ключа)	Висока	Дуже висока	Дуже низька	Середня-висока
Ресурсомісткість	Мінімальна	Середня-висока	Висока	Мінімальна	Середня

Таблиця 1 – Порівняння алгоритмів шифрування

Переваги алгоритмів:

- XOR – Легко реалізується, потребує мінімум ресурсів.
- AES – Дуже надійний, широко використовується.
- RSA – Асиметричне шифрування, висока безпека.
- Caesar – Проста реалізація.
- DES/3DES – Стандартизовані методи.

Недоліки алгоритмів:

- XOR – Небезпечний при використанні постійного або слабкого ключа.
- AES – Потребує більше ресурсів і часу на реалізацію.
- RSA – Повільний особливо при роботі з великими обсягами.
- Caesar – Легко зламується, непридатний для серйозного використання.
- DES/3DES – Застарілі, менш безпечні порівняно з AES.

Висновки. За результатом аналізу алгоритмів найкращим вибором для даної системи є алгоритм XOR через його простоту реалізації, швидкодію, мінімальну потребу ресурсів, симетричність алгоритму та гнучкість у роботі з ключем.

Алгоритм XOR не найкращий для систем, що вимагають високого рівня криптографічного захисту, таких як банківські сервіси, шифрування та передавання через публічні мережі тощо. Але для локальної програмної системи, де основною метою є базовий захист (наприклад, від звичайного користувача або випадкового перегляду) – XOR цілком виправданий вибір.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. XOR cipher - <https://www.geeksforgeeks.org/cryptography>
2. Advanced Encryption Standard - https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
3. RSA cryptosystem - https://en.wikipedia.org/wiki/RSA_cryptosystem
4. Ceasar cipher - https://en.wikipedia.org/wiki/Caesar_cipher
5. Data Encryption Standard - https://en.wikipedia.org/wiki/Data_Encryption_Standard

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



**ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ
АСПЕКТИ РОЗРОБКИ
КОМП'ЮТЕРНИХ СИСТЕМ**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів