Технічні науки

УДК: 004.051

Чернишов Михайло Сергійович

студент

Харківського національного університету радіоелектроніки

Чернышов Михаил Сергеевич

студент

Харьковского национального университета радиоэлектроники

Chernyshov Myhailo

Student of the

Kharkiv National University of Radio Electronics

Ємельянова Катерина Олегівна

студент

Харківського національного університету радіоелектроніки

Емельянова Екатерина Олеговна

студент

Харьковского национального университета радиоэлектроники

Iemelianova Kateryna

Student of the

Kharkiv National University of Radio Electronics

Науковий керівник:

Олійник Олександр Олександрович

асистент кафедри ПІ

Харківський національний університет радіоелектроніки

ПОРІВНЯННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ АЛГОРИТМІВ ШИФРУВАННЯ ДАНИХ

СРАВНЕНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ
USING DATA ENCRYPTION ALGORITHMS EFFICIENCY COMPARISON

Анотація. *Досліджено криптостійкість та часові показники шифрування із застосуванням алгоритмів Цезаря, Віженера, DES, RSA.*

Ключові слова: *криптостійкість, алгоритм шифрування, дешифрування, ентропія, rsa, des, шифр Цезаря, шифр Віженера.*

Аннотация. *Исследовано криптостойкость и временные показатели шифрования с использованием алгоритмов Цезаря, Виженера, DES, RSA.*

Ключевые слова: *криптостойкость, алгоритм шифрования, дешифрование, энтропия, rsa, des, цифр Цезаря, шифр Виженера.*

Summary. *The cryptographic strength and time indicators of encryption using the algorithms of Caesar, Vigenere, DES, RSA have been investigated.*

Key words: *cryptographic strength, encryption algorithm, decryption, entropy, rsa, des, Caesar cipher, Vigenere cipher.*

Специфіка процесів, що сьогодні протікають у різноманітних сферах людського життя, визначається важливою спільною характеристикою – обміном інформацією. Значна її частина представляє собою персональні дані чи в цілому такі, що не призначені для вільного доступу усіх охочих. Інформація – цінний ресурс, тому існування способів її захисту є першочерговою перешкодою цифровій анархії.

Бурхливий розвиток обчислювальної техніки став причиною злету такої науки, як криптографія, завданням якої зараз переважно і є захист безпосередньо комп'ютерної інформації. Створено велику кількість криптографічних алгоритмів, які покликані захистити дані від зловмисника.

Проаналізувавши їх перелік, було виділено декілька з них (від тих, що відомі людству вже не перше тисячоліття, до найсучасніших), реалізовано програмно і порівняно їх ефективність. До них належать шифр Цезаря, шифр Віженера, DES, RSA.

Першим та найстарішим розглянутим алгоритмом є шифр Цезаря. Його суть є надзвичайно простою: кожен символ у зашифрованому тексті замінюється на рівновіддалений (відстань визначається ключем) зліва або справа. Із формулювання алгоритму стає зрозумілим, що процес шифрування та дешифрування не є затратним ні за часом, ні за ресурсами. Проте така простота зумовлює те, що й його злам легкою задачею. Простим перебором усіх можливих ключів, кількість яких дорівнюватиме розміру алфавіту, можна отримати розшифровку без застосування складних криптографічних методів, а за допомогою частотного аналізу даний шифр зламується елементарно.

Другий з алгоритмів – шифр Віженера, у ньому кожним елементом складного ключа є зсув, на який за шифром Цезаря буде зашифровано відповідну літеру у тексті. Теоретично можна згенерувати ключ, що буде за розміром відповідати тексту, який підлягає шифруванню, проте на практиці використання таких великих ключів є неможливим при роботі з великими обсягами даних. Тому ключ циклічно повторюється. Хоча це усе одно дозволяє «розмити» частотні характеристики, певні особливості появи літер у тексті зберігаються. Як наслідок, можна підібрати розмір ключа.

Алгоритм DES засновано на великій кількості перетворень, перемішувань, застосувань побітових операцій XOR, що дозволяють значно підвищити ентропію. Таким чином зміна навіть одного символу у тексті дозволяє значно вплинути на кінцевий результат шифрування блоку. Фрагмент реалізації алгоритму, у якому показано основні етапи його роботи, реалізований для виконання дослідження, наведено на рис. 1.

```
def __get_value_by_des_algorithm(
        cls, message: Message,
        stage_count: int, stage_keys: list[bitarray]
):
    block_count = message.get_block_count()
    cipher = bitarray()

    for i in range(block_count):
        message.make_initial_permutation_for_block(i)
        current_block = message.get_block(i)
        block_size = len(current_block)
        block_middle = block_size // 2
        block_parts = [
            current_block[:block_middle],
            current_block[block_middle:]
        ]

        cls.__do_feistel_rounds(block_parts, stage_count, stage_keys)
        merged_block_parts = cls.__get_merged_block_parts(block_parts)
        final_permutation_result = cls.__get_finally_permuted_block(
            merged_block_parts
        )
        cipher.extend(final_permutation_result)

    return cipher
```

Рис. 1. Фрагмент коду реалізації алгоритму DES

Недоліками даного алгоритму є те, що існують слабкі та частково слабкі ключі, а також невелика кількість можливих варіантів ключів, що із застосуванням сучасної техніки можна за прийнятний час перебрати.

Принцип асиметричного алгоритму RSA заснований на складності факторизації: легко знайти число, піднесене до певної степені, а виконати зворотну операцію досить складно. Визначено, що при розмірі ключа менше 1024 біт алгоритм не можна вважати криптостійким, адже спрощується підрахунок функції Ейлера, яка лежить в основі його реалізації.

Визначено час шифрування даних різної довжини (24, 144, 1152 байт) із застосуванням вище описаних алгоритмів, отримані результати візуалізовано у вигляді графіку (див. рис. 2).

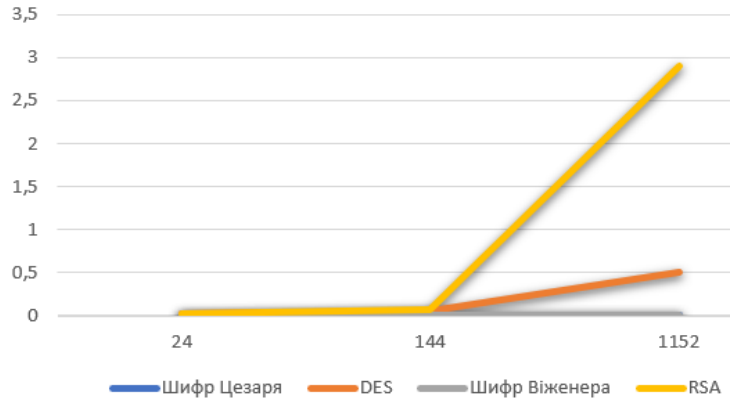

Рис. 2. Порівняння часу шифрування даних різними алгоритмами

Із даного графіку видно, що алгоритми Цезаря та Віженера під час шифрування потребують незначного проміжку часу, у DES же час роботи помітно зростає, що зумовлено складністю операцій, що у ньому застосовуються. Найбільш суттєвим є зростання часу шифрування при використанні RSA – у 5,7 разів порівняно із DES для даних довжиною 1152 байти.

Із отриманих результатів можна зробити висновок, що алгоритм RSA не має застосовуватися для шифрування даних великої довжини, він призначенням має бути обмін ключами симетричних алгоритмів, таких як алгоритми Цезаря, Віженера, DES (для шифрування і розшифрування використовується один ключ). Враховуючи недоліки розглянутих алгоритмів, не рекомендується використовувати шифрування Цезаря, а також шифр Віженера при шифруванні із використанням короткого відносно шифрованого тексту ключа, що циклічно повторюється.

Література

1. Панасенко С. П. Алгоритмы шифрования. СПб.: БХВ-Петербург, 2009. 276 с.
2. Романьков В. А. Введение в криптографию. Курс лекций. М.: Форум, 2012. 240 с.