МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 23-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2019 р.

Том 9

КОНФЕРЕНЦІЯ «УПРАВЛІННЯ ЗНАННЯМИ ТА КОНКУРЕНТНА РОЗВІДКА»

Харків 2019

23-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 9. – Харків: ХНУРЕ. 2019. – 144 с.

В збірник включені матеріали 23-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Видання підготовлено кафедрою Соціальної інформатики та
Науково-навчальним центром управління знаннями
Харківського національного університету радіоелектроніки

61166 Україна, Харків, просп. Науки, 14
тел./факс: (057) 7021397

E-mail: mref21@nure.ua, d_si@nure.ua

Організатори конференції:

Харківський національний університет радіоелектроніки

Національний технічний університет «Харківський політехнічний інститут»

ITHEA International Scientific Society (Болгарія)

Інститут кібернетики імені В.М. Глушкова НАН України (Київ)

Інститут телекомунікацій та глобального інформаційного простору НАН України (Київ)

Національний авіаційний університет (Київ)

Національний університет "Львівська політехніка"

Національний аерокосмічний університет ім. Н.Е. Жуковського

Спільнота аналітиків та професіоналів конкурентної розвідки

Національний центр управління та випробування космічних засобів

Програмний комітет конференції:

Проф., д.т.н., зав. каф. соціальної інформатики Харківського національного університету радіоелектроніки Соловйова Катерина Олександрівна – **голова.**

Проф., д.т.н., зав. каф. системного аналізу та управління Національного технічного університету «Харківський політехнічний інститут» Куценко Олександр Сергійович - **співголова.**

Академік НАНУ, зам. директора Інституту кібернетики Національної академії наук України Палагін Олександр Васильович (Київ).

Assoc. prof. dr. Krassimir Markov, Institute of Mathematics and Informatics of Bulgarian Academy of Sciences, директор Інституту інформаційних теорій та програм Інформаційного наукового товариства ITHEA (Болгарія).

Завідувач лабораторією штучного інтелекту та інженерії знань, проф., доктор Абдель-Бадеех М. Салем (університет Айн-Шамс, Єгипет).

Доктор - системний аналітик відділу безпеки атомних станцій Шведського нагляду над радіаційною безпекою Ільїна Олена Юріївна (Sweden).

Проф., д.т.н., декан математичного факультету Запорізького національного університету Гоменюк Сергій Іванович.

Проф., д.т.н., зав. каф. безпеки інформаційних технологій Національного авіаційного університету Корченко Олександр Григорович (Київ).

С.н.с., к.т.н., доцент, с.н.с. Інституту кібернетики імені В.М. Глушкова Національної академії наук України Величко Віталій Юрійович (Київ).

Д.т.н., с.н.с., зав. відділом Інституту телекомунікацій і глобального інформаційного простору Національної академії наук України Стрижак Олександр Євгенович (Київ).

Проф., д.т.н., зав. кафедрою соціальних комунікацій та інформаційної діяльності Національного університету "Львівська політехніка" Пелещишин Андрій Миколайович (Львів).

Проф., д.т.н., зав. каф. АСУ Національного технічного університету «Харківський політехнічний інститут» Годлевський Михайло Дмитрович.

Проф., д.т.н., професор кафедри інженерії програмного забезпечення Національного аерокосмічного університету ім. Н.Є. Жуковського Шостак Ігор Володимирович.

Начальник відділу контролю космічного простору, підполковник Москаленко Сергій Станіславович НЦУВКЗ.

Начальник лабораторії збору і аналізу космічної обстановки, підполковник Краснощеков Олександр Євгенович НЦУВКЗ.

Ст. викл. каф. соціальної інформатики Харківського національного університету радіоелектроніки Данилов Андрій Дмитрович – **учений секретар.**

ПІДВИЩЕННЯ СТІЙКОСТІ КРИПТОАЛГОРИТМУ RSA ЗА РАХУНОК ВИКОРИСТАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ

Приймак А. В., Яремчук Ю. Є.
Вінницький національний технічний університет
(21000, Вінниця, Хмельницьке шосе, 95, каф. менеджменту та безпеки інформаційних систем, тел. (0432) 560 848)
e-mail: andrii.pryimak@live.com, факс: (093) 124-55-02

The research of the cryptographic algorithm RSA with regard to the possibility of increasing its stability by using genetic algorithm was made. The method of optimization of input message, that consists of 8 main steps, with the help of genetic algorithm is proposed. Using the three main properties of the genetic algorithm (selection, crossover and mutation), the input message is randomizing, which as a result of RSA encryption is transformed into a stochastic ciphertext, which is no longer deterministic and weak to attack based on selected ciphertext, and thus increases the cryptostability of this algorithm. The statistical testing of the proposed improvement of the algorithm, using the NIST STS test package, showed a high statistical reliability of this method, as the results of tests were inside 0.9-1 range. Comparison of the results of testing of the original RSA and the modified showed that the original algorithm shows worse performance compared to the proposed its modification. Ten of the fifteen tests showed that the modified RSA algorithm with the built-in proposed method for optimizing the input message has higher rates by 1-3%, which shows an increase of its cryptostability.

Для захисту інформації у мережі існує багато підходів, серед яких одним з найефективніших та найпопулярніших є криптографія. За допомогою криптографії вирішується питання забезпечення конфіденційності, цілісності і автентичності інформації (захищеного передавання даних, обміну інформацією чи її збереження) [1-2].

На даний момент одним з найвідоміших та найбільш поширених криптографічних асиметричних алгоритмів є – RSA. Даний алгоритм підтримується всіма версіями SSL/TLS, протоколами, які регулюють безпечний обмін даними в мережі Інтернет. Основними його недоліками є детермінованість шифротексту та вразливість до атаки на основі підібраного шифротексту [3-4]. Для вирішення вищезгаданих недоліків, в цій роботі було розроблено метод оптимізації вихідного повідомлення, використовуючи три основні властивості генетичного алгоритму (оператор відбору, схрещення та мутація). Даний метод складається із 8 таких кроків [5]:

1. Конвертація вихідного повідомлення в двійковий код.
2. Розбиття сконвертованого повідомлення на 2 рівні частини. Якщо вони нерівні, то дописуються нулі.
3. Генерація випадкової точка схрещення.
4. Схрещення двох частин за згенерованою точкою схрещення.

5. Об’єднання схрещених частин в одну послідовність біт для подальшого проведення процесу мутації.

6. Генерація 3 випадкових чисел. Ці числа є номерами бітів, які будуть замінені під час мутації. Всі 3 числа будуть зберігатись як одна послідовність R.

7. Операція мутації за вибраними числами з попереднього кроку. Результуюча послідовність $M^{''}$.

8. Формування вихідного повідомлення $m^{'}$ після процесу оптимізації генетичним алгоритмом, яке буде приймати подальшу участь в процесі шифрування алгоритмом RSA. Оптимізоване повідомлення матиме такий вигляд – $[M^{''}, S, R]$.

Для дослідження статистичної безпеки асиметричного алгоритму RSA з вбудованим запропонованим методом оптимізації вихідного повідомлення було використано пакет статистичних тестів NIST STS (рис. 1).

Основними параметрами для проходження тестів було обрано:

– довжина ключа –1024 біт;

– кількість тестів - 188.

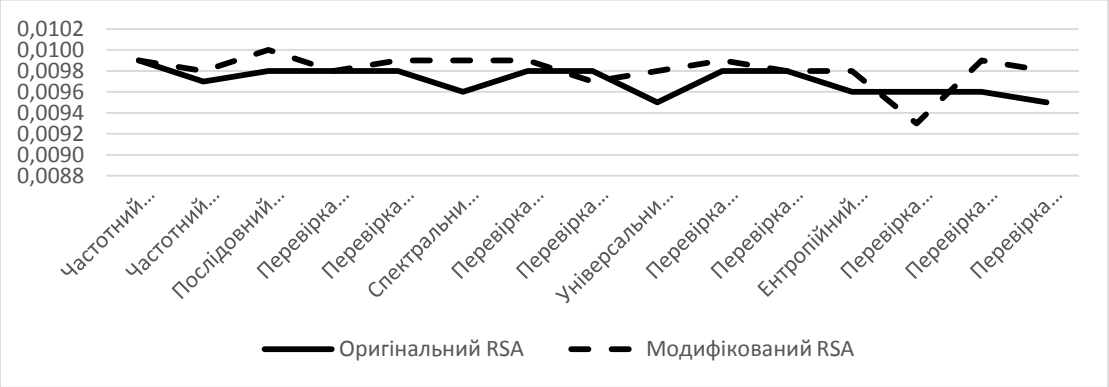

Рис. 1. Графічне порівняння результатів тестування

Алгоритм із вбудованим запропонованим методом оптимізації вихідного повідомлення показав кращі результати в десяти з п’ятнадцяти тестів на 1-3%, що свідчить про його вищий рівень статистичної безпеки.

1. Jana Bappaditya, Chakraborty Moumita, Tamoghna Mandal, Kule, Malay. An Overview on Security Issues in Modern Cryptographic Techniques. Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT) – 2018.

2. Joseph Charles, I.Carol, S.Mahalakshmi. Big Data Security an Overview. International Research Journal of Engineering and Technology (IRJET) – 2018 – 130-134. https://www.irjet.net/archives/V5/i2/IRJET-V5I232.pdf

3. R. Sivakumar, B. Balakumar, V. Arivu Pandeeswaran. A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security. International Research Journal of Engineering and Technology (IRJET) – 2018 – 4133-4137.

4. Joye M. Secure ElGamal-Type Cryptosystems Without Message Encoding. The New Codebreakers. Lecture Notes in Computer Science – 2016 – 470-478.

5. Приймак А., Яремчук Ю. Підвищення стійкості криптоалгоритму RSA за рахунок генетичної оптимізації вихідного повідомлення. Реєстрація, зберігання і обробка даних. – Т. 20, №6, 2018. – С. 76–84.