КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.216223
УДК 004.056

Кулібаба Сергій Олександрович
студент 3 курсу кафедри програмних систем і технологій
факультету інформаційних технологій
Київського національного університету імені Тараса Шевченка, Київ, Україна.
ORCID ID: 0000-0002-7316-1214
kulibseryyy@gmail.com

Курченко Олег Анастасійович
кандидат технічних наук, доцент кафедри програмних систем і технологій
факультету інформаційних технологій
Київського національного університету імені Тараса Шевченка, Київ, Україна.
ORCID ID: 0000-0002-3507-2392
kurol@ukr.net

КРИПТОГРАФІЧНИЙ МЕТОД ШИФРУВАННЯ ДАНИХ PATTERN REVERSE MULTIPLICATION

Анотація. У даній роботі розглядається задача розробки власного криптографічного метода шифрування шляхом використання допоміжних та вже існуючих засобів розробок. Процес захисту даних відбуватиметься шляхом зміни внутрішньої структури даних. Вже існуючі криптографічні методи висвітлені в інтернет-джерелах, тому було прийнято рішення відобразити принцип утворення власного метода шифрування для будь-яких даних. Процес обробки може займати значну кількість часу для достатніх об'ємів даних, тому в даній роботі буде продемонстрований процес обробки із використанням ресурсів пристрою. Дана модифікація підвищить ефективність використання запропонованої методології підвищення рівня захисту даних. Завдяки власним підходам, особи, які намагаються отримати інформацію не легальним шляхом, будуть мати меншу ймовірність до успішного отримання дійсних даних. Застосування методології може використовуватись у різних цифрових напрямках зокрема засобах комунікації, загальний обмін даними, захист пакетів, які надсилаються по мережі.

Ключові слова: ключ; шифрування; розшифрування; ресурси пристрою; швидкість обробки.

ВСТУП

Доступ до інтернету є у більшості осіб. Завдяки інтернету користувачі відповідних комунікаційних та інших систем можуть обмінюватись інформацією між собою. Обмін інформацією не завжди може бути захищеним та конфіденційним [1].

Існують зловмисники, у яких є бажання отримати відповідну інформацію від певних організацій, тому до технологій підвищення рівня захисту збереження даних повинно приділятись достатньо уваги, щоб відповідні особи не змогли отримати інформацію нелегальним шляхом [2, 3]. Прикладом може бути нещодавна подія – інформаційний напад на державні сервіси, в наслідок чого була можливість отримати доступ до персональних даних громадян України.

Криптографічні технології захисту даних широко використовуються в інформаційних технологіях. Значна кількість компаній використовують певні засоби захисту даних у власне розроблених програмних забезпеченнях.

Використання подібних технологій зумовлена тим, щоб зберігати конфіденційність та надавати високу якість обслуговування обробки даних користувачів систем, а також залучати їх до використання їхніх засобів надання послуг.

АНАЛІЗ ПУБЛІКАЦІЙ ТА ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

У статті розглядається методологія утворення власного метода криптографічного шифрування. Підвищення рівня захисту відбуватиметься зміною внутрішньої структури даних, яка вміщає в собі відповідну інформацію методом Pattern Reverse Multiplication (далі PRM).

Для побудови власного метода слід знати властивості криптографічних шифрувань [4]. Основою методів є конфіденційність, незмінність та джерело. Конфіденційність залишається для усіх користувачів відповідних систем, де використовуються відповідні методи захисту даних. Незмінність свідчить про те, що дані, які вже відправлені у систему, не можуть змінюватись для майбутньої верифікації джерела. Підтвердженням відправлених даних може бути саме джерело – користувач системи, який надсилає дані.

Існують декілька типів шифрувань, які можуть ідентифікувати себе по ознакам – симетричні та асиметричні методи. Основою симетричних методів – єдиний ключ для отримання дійсних даних, який має назву «публічний» [5, 6]. Він може надсилатись із захищеними даними або може залишатись у системі, щоб отримувач міг розшифрувати дані [7]. В асиметричних методах шифрування використовується два ключі – публічний та приватний [8]. Принцип подібний симетричному, але із модифікацією – обробка публічного ключа приватним, який не повинен відображатись зовні у системі.

Зміна внутрішньої структури відбувається завдяки редагуванню символів й спеціальних символів, які знаходяться у структурі даних [9]. При використанні певних засобів розробок можна отримати відразу десяткове число, яке дасть можливість проводити операції над ним [10].

Метою даної роботи є дослідження, які спрямовані на розробку методу шифрування, який дозволяє підвищити швидкість обробки даних за допомогою використання ресурсів пристрою, на якому відбувається шифрування та розшифрування.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

АЛГОРИТМ РОБОТИ МЕТОДА PRM

Для опрацювання даних потрібно отримати усі внутрішні символи цих даних (табл. 1). В даній роботі буде запропонованим опрацювання десяткового коду, тому потрібно конвертувати їх після отримання (1).

$$\sum_{k=1}^{m} \left(n_k \times 2^{m-k}\right)_{10} \qquad (1)$$

Таблиця 1

Частина кодувальних символів ASCII

Символ	2-й код	Символ	2-й код
	00100000	a	01100001
!	00100001	b	01100010
"	00100010	c	01100011
#	00100011	d	01100100
$	00100100	e	01100101
%	00100101	f	01100110
&	00100110	g	01100111
‘	00100111	С	11010001
(	00101001	Т	11010010
)	00101010	У	11010011
*	00101011	Ф	11010100
+	00101100	Х	11010101
,	00101101	Ц	11010110
-	00101110	Ч	11010111
0	00110000	H	01001000
1	00110001	I	01001001
2	00110010	J	01001010
3	00110011	K	01001011
4	00110100	L	01001100
5	00110101	M	01001101
6	00110110	N	01001110

Обробка та підвищення рівня захисту повинна відбуватись завдяки відповідному шаблону – ключу. Шаблон може бути створений індивідуально під власне розроблений алгоритм, адже підхід до опрацювання даних дає можливість реалізувати дану задачу [11].

Дані, які отримані, повинні взаємодіяти із ключем. Алгоритм опрацювання може бути будь-яким. В даному методі використовується наступний алгоритм:

1. Утворення ключа із довжиною $9 \leq N$.
2. Зворотній запис ключа.
3. Отримання конвертованих даних.
4. Відповідне число множиться на довжину ключа.
5. Результат добутку розділяється на окремі числа.
6. Кожне число береться, як індекс із ключа.
7. Формування захищених даних.
8. Відправка захищених даних по мережі / системі.
9. Відправка початкової форми ключа.

Відправка ключа по мережі / системі може відбуватись тоді й тільки тоді, коли над ним проводяться певні операції по відповідному алгоритму, внаслідок чого буде утворений асиметричний метод шифрування [12]. При цьому можна робити генерацію ключів, де застосовується симетричний метод – це може підвищити рівень захищеності даних.

ISSN 2663 - 4023

В запропонованому методі довжина повинна бути не менше 9. Це через те, що результат розділеного числа, які утворився від добутку, може бути від 0 до 9.

Надійність вихідних даних може залежати від довжини ключа – кількість ітерацій на обробку. При використанні мінімальної довжини можна отримати менш надійний захист й більш швидку обробку, але при використанні достатньо складного алгоритму, дані можуть мати достатній рівень захисту.

КОМПРЕСІЯ ДАНИХ

При використанні подібного алгоритму може виникнути проблема із підвищенням початкового розміру даних у декілька разів. Через те, що заміна одного символу може бути декількома, тому внаслідок чого можна отримати вихідні захищені дані із розміром у 3 – 4 рази більші, ніж за оригінал. Рішенням може бути зміна алгоритму або використати компресії для вихідних даних.

Є декілька типів стискань – із втратами та без втрат [13, 14]. Стискання із втратами може відображати втрату деяких символів. Але завдяки алгоритмам компресії – дані повертаються до дійсного вигляду після їх розпакування.

Рекомендацією до утворення власних технологій по запропонованому алгоритму слід використовувати стискання із втратами – це дасть можливість ефективно зберігати й надсилати дані по мережі / системі.

Для підвищення швидкості обробки можна на початку використати компресію для даних, потім їх обробити по алгоритму для підвищення рівня захисту. Деякі дані можуть не зменшити об’єм, тому дана технологія може використовуватись лише після обробки даних. Також можна поєднувати стискання даних – до початку й після.

ПРИСКОРЕННЯ ШВИДКОСТІ ОБРОБКИ

Подібні алгоритми можуть опрацьовувати дані повільно. Рішенням проблеми може бути оптимізаційне конструювання програми зокрема використання ресурсів пристрою, де буде використовуватись метод підвищення конфіденційності. В даній роботі буде розглянутий спосіб підвищення швидкості обробки даних шляхом використання ресурсів пристрою.

Існують різні допоміжні технології, які надають можливість швидко обробляти дані. Принцип роботи усіх – потоки процесора та головний носій.

Розділення вхідних даних на декілька частин й відправка їх на опрацювання до потоків, допомагають швидко обробляти дані. При цьому тактова частота процесора повинна бути достатньо потужною – впливає на швидкість обробки. Використання технологій, які дають можливість реалізувати використання потоків – робота їх може бути не стабільною. Слід використовувати черги до подання даних на обробку для отримання дійсних вихідних результатів.

Швидкість обробки даних завдяки використанню потоків процесора є окремим випадком до прискорення обробки. При використанні пам’яті головного носія доступність до оброблених даних стає швидшою, внаслідок чого можна отримати приріст швидкості обробок у декілька разів, ніж за звичайне використання потоків процесора [15].

Для використання ресурсів пристрою слід враховувати потужність, де буде використовуватись алгоритм підвищення захисту даних. Не достатньо потужні пристрої

також можуть надавати прискорення швидкості, але він буде відрізнятись від швидкості на потужному пристрої.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Криптографічні методи шифрування застосовуються у значній кількості систем, зокрема засобах комунікації, різноманітних сервісах тощо. Використання вже існуючих методів підвищення рівня захисту та конфіденційності осіб системи надають лише достатній рівень надійності даних.

В даній роботі був запропонований алгоритм обробки будь-яких даних методом PRM. Завдяки використанню сучасних технологій та допоміжних засобів розробок можна отримати дані, рівень яких може підвищитись у декілька разів. Алгоритм побудови власного метода надає можливість змінити його структуру – опрацювання над ключем. При опрацюванні ключа по іншим алгоритмам – можна отримати асиметричний метод шифрування, який буде залишати частину інформації у системі, та підвищувати рівень захищеності даних на високий.

При використанні складних алгоритмів до опрацювання даних може виникнути проблема із збереженням / передачею даних по мережі. Рішенням може бути компресія даних – отримання вихідного об’єму наближений до об’єму оригінальних даних.

Прискоренням швидкості обробки даних може бути використання ресурсів пристрою, на якому використовується алгоритм для реалізації конфіденційності даних користувачів відповідних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Sharma, M. K., Somwanshi, D. (2018). Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique. У 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE). IEEE. https://doi.org/10.1109/icraie.2018.8710434.

2 Gupta, S., Isha, Bhattacharya, A., Gupta, H. (2021). Analysis of Social Engineering Attack on Cryptographic Algorithm. У 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE. https://doi.org/10.1109/icrito51393.2021.9596568.

3 Chaudhary, P., Gupta, R., Singh, A., Majumder, P. (2019). Analysis and Comparison of Various Fully Homomorphic Encryption Techniques. У 2019 International Conference on Computing, Power and Communication Technologies (GUCON) (с. 58–62).

4 Comon-Lundh, H., Cortier, V., Zălinescu, E. (2010). Deciding security properties for cryptographic protocols. application to key cycles. ACM Transactions on Computational Logic, 11(2), 1–42. https://doi.org/10.1145/1656242.1656244.

5 Gitanjali, J., Jeyanthi, N., Ranichandra, C., Pounambal, M. (2014). ASCIi based cryptography using unique id, matrix multiplication and palindrome number. У 2014 International Symposium on Networks, Computers and Communications (ISNCC). IEEE. https://doi.org/10.1109/sncc.2014.6866509

6 Zaw, T. M., Thant, M., Bezzateev, S. V. (2019). Database Security with AES Encryption, Elliptic Curve Encryption and Signature. У 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). IEEE. https://doi.org/10.1109/weconf.2019.8840125.

7 Yu, L., Wang, Z., Wang, W. (2012). The Application of Hybrid Encryption Algorithm in Software Security. У 2012 4th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE. https://doi.org/10.1109/cicn.2012.195.

8 Rad, N. B., Shah-Hosseini, H. (2008). GBHE: Grid-Based Cryptography with AES Algorithm. У 2008 International Conference on Computer and Electrical Engineering (ICCEE). IEEE. https://doi.org/10.1109/iccee.2008.36.

9 Atmaja, I. M. A. D. S., Astawa, I. N. G. A., Wisswani, N. W., Nugroho, I. M. R. A., Sunu, P. W., Wiratama, I. K. (2020). Document Encryption Through Asymmetric RSA Cryptography. У 2020 International Conference on Applied Science and Technology (iCAST). IEEE. https://doi.org/10.1109/icast51016.2020.9557723.

10 Lin, C., Ran, J., Deng, D., Zhang, N., Wang, J. (2020). Research on Key-bytes Encryption Technology of SDH Channel. У 2020 International Conference on Robots & Intelligent System (ICRIS). IEEE. https://doi.org/10.1109/icris52159.2020.00059.

11 Alshahrani, A. M., Walker, S. (2014). A novel encryption solution for real time applications. У 2014 Third International Conference on e-Technologies and Networks for Development (ICeND). IEEE. https://doi.org/10.1109/icend.2014.6991356.

12 Keerthi, K., Surendiran, B. (2017). Elliptic curve cryptography for secured text encryption. У 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT). IEEE. https://doi.org/10.1109/iccpct.2017.8074210.

13 Yue Shen, Hanwen Zhang, Guohai Liu, Hui Liu, Wei Xia, Hongxuan Wu. (2014). Power quality data compression based on sparse representation and compressed sensing. У 2014 11th World Congress on Intelligent Control and Automation (WCICA). IEEE. https://doi.org/10.1109/wcica.2014.7053666.

14 Atar, E., Ersoy, O. K., Ozyilmaz, L. (2016). Character/text data compression and encryption by compressive sensing and hybrid cryptography. У 2016 24th Signal Processing and Communication Application Conference (SIU). IEEE. https://doi.org/10.1109/siu.2016.7495753

15 Daemen, J., Claesen, L., Genoe, M., Peeters, G., Govaerts, R., Vandewalle, J. (1993). A cryptographic chip for ISDN and high speed multi-media applications. У IEEE Workshop on VLSI Signal Processing. IEEE. https://doi.org/10.1109/vlsisp.1993.404507.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

Serhii Kulibaba
3-th year student of the Department of Software Systems and Technologies,
Faculty of Information Technology,
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
ORCID ID: 0000-0002-7316-1214
kulibseryyy@gmail.com

Oleg Kurchenko
Candidate of Technical Sciences, Associate Professor of Software Systems and Technologies
Faculty of Information Technology
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
ORCID ID: 0000-0002-3507-2392
kurol@ukr.net

CRYPTOGRAPHY DATA ENCRYPTION METHOD PATTERN REVERSE MULTIPLICATION

Abstract. The task of unlocking a private cryptographic method of encryption using a path of victories of additional and already essential tools is considered. The process of defending data is to change the internal structure of data. Existing cryptographic methods are covered on the Internet, so it was decided to show the principle of establishing a public encryption method for any data. The processing process can take a significant amount of time for sufficient amounts of data, so this paper will demonstrate the processing process using the resources of the device. This modification will increase the efficiency of the proposed methodology to increase the level of data protection. Due to their own approaches, people who try to obtain information illegally will be less likely to successfully obtain valid data. The application of the methodology can be used in different digital areas, individual means of communication, general data exchange, security packages contained in the network.

Keywords: key; encryption; decryption; device resources; processing speed.

REFERENCES

1 Sharma, M. K., Somwanshi, D. (2018). Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique. In 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE). IEEE. https://doi.org/10.1109/icraie.2018.8710434.

2 Gupta, S., Isha, Bhattacharya, A., Gupta, H. (2021). Analysis of Social Engineering Attack on Cryptographic Algorithm. In 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE. https://doi.org/10.1109/icrito51393.2021.9596568.

3 Chaudhary, P., Gupta, R., Singh, A., Majumder, P. (2019). Analysis and Comparison of Various Fully Homomorphic Encryption Techniques. In 2019 International Conference on Computing, Power and Communication Technologies (GUCON) (p. 58–62).

4 Comon-Lundh, H., Cortier, V., Zălinescu, E. (2010). Deciding security properties for cryptographic protocols. application to key cycles. ACM Transactions on Computational Logic, 11(2), 1–42. https://doi.org/10.1145/1656242.1656244.

5 Gitanjali, J., Jeyanthi, N., Ranichandra, C., Pounambal, M. (2014). ASCIi based cryptography using unique id, matrix multiplication and palindrome number. In 2014 International Symposium on Networks, Computers and Communications (ISNCC). IEEE. https://doi.org/10.1109/sncc.2014.6866509

6 Zaw, T. M., Thant, M., Bezzateev, S. V. (2019). Database Security with AES Encryption, Elliptic Curve Encryption and Signature. In 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF). IEEE. https://doi.org/10.1109/weconf.2019.8840125.

7 Yu, L., Wang, Z., Wang, W. (2012). The Application of Hybrid Encryption Algorithm in Software Security. In 2012 4th International Conference on Computational Intelligence and Communication Networks (CICN). IEEE. https://doi.org/10.1109/cicn.2012.195.

8 Rad, N. B., Shah-Hosseini, H. (2008). GBHE: Grid-Based Cryptography with AES Algorithm. In 2008 International Conference on Computer and Electrical Engineering (ICCEE). IEEE. https://doi.org/10.1109/iccee.2008.36.

9 Atmaja, I. M. A. D. S., Astawa, I. N. G. A., Wisswani, N. W., Nugroho, I. M. R. A., Sunu, P. W., Wiratama, I. K. (2020). Document Encryption Through Asymmetric RSA Cryptography. In 2020 International Conference on Applied Science and Technology (iCAST). IEEE. https://doi.org/10.1109/icast51016.2020.9557723.

10 Lin, C., Ran, J., Deng, D., Zhang, N., Wang, J. (2020). Research on Key-bytes Encryption Technology of SDH Channel. In 2020 International Conference on Robots & Intelligent System (ICRIS). IEEE. https://doi.org/10.1109/icris52159.2020.00059.

11 Alshahrani, A. M., Walker, S. (2014). A novel encryption solution for real time applications. In 2014 Third International Conference on e-Technologies and Networks for Development (ICeND). IEEE. https://doi.org/10.1109/icend.2014.6991356.

12 Keerthi, K., Surendiran, B. (2017). Elliptic curve cryptography for secured text encryption. In 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT). IEEE. https://doi.org/10.1109/iccpct.2017.8074210.

13 Yue Shen, Hanwen Zhang, Guohai Liu, Hui Liu, Wei Xia, Hongxuan Wu. (2014). Power quality data compression based on sparse representation and compressed sensing. In 2014 11th World Congress on Intelligent Control and Automation (WCICA). IEEE. https://doi.org/10.1109/wcica.2014.7053666.

14 Atar, E., Ersoy, O. K., Ozyilmaz, L. (2016). Character/text data compression and encryption by compressive sensing and hybrid cryptography. In 2016 24th Signal Processing and Communication Application Conference (SIU). IEEE. https://doi.org/10.1109/siu.2016.7495753

15 Daemen, J., Claesen, L., Genoe, M., Peeters, G., Govaerts, R., Vandewalle, J. (1993). A cryptographic chip for ISDN and high speed multi-media applications. In IEEE Workshop on VLSI Signal Processing. IEEE. https://doi.org/10.1109/vlsisp.1993.404507.