КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.14.176185
УДК 004.056.5:004.7

Гнатюк Сергій Олександрович
доктор технічних наук, професор,
заступник декана факультету кібербезпеки, комп'ютерної та програмної інженерії
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Смірнова Тетяна Віталіївна
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-5093-1581
sm.tetyana@gmail.com

Бердибаєв Рат Шиндалійович
PhD,
керівник науково-технічного центру проблем інформаційної безпеки імені Турганбека Омара
Алматинський університет енергетики та зв'язку, Алмати, Казахстан
ORCID ID: 0000-0002-8341-9645
r.berdybaev@aues.kz

Бурмак Юлія Анатоліївна
здобувач НДЛ протидії кіберзагрозам в авіаційній галузі
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0002-5410-6260
julburmac@gmail.com

Оспанова Дінара Манапівна
PhD докторант
Казахський гуманітарно-юридичний інноваційний університет, Семей, Казахстан
ORCID ID: 0000-0002-2206-7367
odm-1778@mail.ru

УДОСКОНАЛЕНИЙ МОДУЛЬ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Анотація. Сучасні методи й засоби шифрування даних гарантують надійний захист (зокрема, конфіденційність та цілісність даних), проте розвиток методів криптоаналізу спонукає до розробки й впровадження нових, більш ефективних, криптоалгоритмів. Крім того, на формування нових вимог до методів і засобів криптографії впливає розвиток сучасних інформаційно-комунікаційних технологій (LTE/5G/6G). З огляду на це, у роботі було проаналізовано відомі програмні модулі криптографічного захисту даних, які сьогодні використовуються в месенджерах і інших застосунках. Цей аналіз дозволив виявити переваги, недоліки і шляхи удосконалення (зокрема, за рахунок використання сучасних процедур безпеки) модулів криптографічного захисту даних. Обрано прототип та удосконалено модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в інформаційно-комунікаційних системах та мережах. Для ефективного використання удосконаленого методу важливим є вибір стійких методів шифрування та гешування, а також синхронізація секретного ключа. У якості зазначених процедур можуть використовуватись відомі криптографічні методи і засоби, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих

видів криптоаналізу. У подальших роботах планується зосередити увагу на практичних дослідженнях удосконаленого модуля криптографічного захисту інформації з використанням різних методів шифрування і гешування, зокрема тих, що були запропоновані авторами у своїх попередніх дослідженнях.

Ключові слова: захист інформації, криптографія, конфіденційність, цілісність, модуль шифрування, інформаційно-комунікаційні системи та мережі, месенджер.

1. ВСТУП

Сьогодні серед множини методів захисту інформації особливе місце займають криптографічні методи [1]. На відміну від інших, ці методи спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її оброблення, передавання і зберігання. Широке використання і постійне збільшення об'єму інформаційних потоків, а також розвиток інформаційно-комунікаційних технологій (LTE/5G/6G), викликають постійне зростання інтересу до криптографії. Останнім часом збільшується відповідно роль програмних криптографічних засобів захисту інформації, які не потребують великих фінансових витрат порівняно з апаратними криптосистемами. Сучасні методи й засоби шифрування гарантують надійний захист (зокрема, конфіденційність та цілісність даних), проте розробка й реалізація нових методів криптоаналізу ставить під загрозу стійкість використовуваних криптоалгоритмів.

Вимоги до рівня захисту інформації почали зростати зі збільшенням кількості атак від зловмисників не тільки на великі технологічні компанії, але і на пересічних користувачів. Після викриття Е. Сноуденом фактів прослуховування спецслужбами пересічних громадян США всі, хто користуються мобільними месенджерами, відразу стали приділяти увагу захисту особистої інформації. Саме тому, на ринку з'явилась низка месенджерів, які використовують повне або часткове шифрування передаваних текстових повідомлень, файлів, фотографій або відео. Крім власне шифрування, також з'явилася опція самознищення повідомлень і цілих чатів, та навіть блокування можливостей для скріншотів.

2. АНАЛІЗ ПУБЛІКАЦІЙ ТА ПОСТАНОВКА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Розглянемо більш детально відомі програмні модулі криптографічного захисту даних, які сьогодні використовуються в месенджерах і інших застосунках.

1. MTProto 1.0 [2] – модуль, який використовується для шифрування повідомлень при передаванні клієнтами Telegram. Протокол поділяється на три фактично незалежні компоненти: 1) компонент високого рівня (мова запиту API): визначає спосіб, за допомогою якого API запити та відповіді перетворюються на двійкові повідомлення; 2) криптографічний (авторизаційний) рівень: визначає спосіб шифрування повідомлень перед передаванням транспортним протоколом; 3) транспортний компонент: визначає метод для клієнта та сервера для передавання повідомлень за допомогою іншого існуючого мережевого протоколу (наприклад, http, https, tcp, udp).

2. Signal Protocol [3] – використовується для шифрування миттєвих повідомлень Facebook Messenger. Функція доступна в розділі Secret Conversations (секретне листування). У цих чатах діє повне або наскрізне шифрування (end-to-end encryption), при якому прочитати повідомлення можуть тільки користувачі, які беруть участь в

листуванні, а провайдери, хакери, урядові відомства та інші сторонні особи не можуть отримати доступ до ключів, необхідних для розшифрування повідомлень. Зашифрувати можна персональні чати з текстом і стікерами, але відео або анімовані картинки вони не підтримують. Протокол поєднує в собі Double Ratched Algorithm, Prekeys та розширений протокол потрійного обміну ключами Діффі-Хеллмана (3-DH) і використовує Curve25519, AES-256 та HMAC-SHA256. Signal Protocol також підтримує шифрування групових чатів.

3. TLS Skype [4] – для миттєвих повідомлень використовується TLS (безпека на рівні транспорту) для шифрування повідомлень між клієнтом Skype та службою чату, коли вони надсилаються безпосередньо між двома клієнтами Skype. Більшість повідомлень надсилаються двома способами, однак у майбутньому вони будуть надсилатися лише через хмару вендора, щоб забезпечити оптимальну роботу користувачів. Голосові повідомлення шифруються, коли вони доставляються клієнтам. Однак після того, як клієнт прослухав голосові повідомлення, вони передаються з серверів на місцевий комп'ютер, де він зберігається як незашифрований файл. Skype використовує AES (Rijndael), який рекомендований та використовується урядом США для захисту конфіденційної інформації. Користувацькі ключі сертифіковані сервером Skype за допомогою 1536 або 2048-бітних сертифікатів RSA.

У табл. 1 відображено порівняльний аналіз розглянутих модулів захисту інформації у сучасних інформаційно-комунікаційних системах та мережах (ІКСМ). за такими критеріями, як використовувані криптоалгоритми, швидкість роботи (ШР), зручність для користувачів (ЗК) і кросплатформеність (КП).

Таблиця 1

Порівняльний аналіз програмних модулів захисту інформації

№ з/п	Модулі	Месенджери, що використовують	Криптоалгоритм	ШР	ЗК	КП
1.	MTProto 1.0	Telegtam	SHA-256, AES-256	+	+	+/-
2.	Signal Protocol	Fasebook Messanger, WhatsApp, Signal	Curve25519, AES-256, HMAC, SHA256	+/-	+	+
3.	TLS Skype	Skype	AES-256, RSA	+/-	-	+/-

Як показав аналіз, розглянуті програмні модулі мають низку недоліків і можуть бути удосконалені за рахунок використання сучасних процедур безпеки. Зважаючи на зазначене, *метою цієї роботи* є удосконалення модуля криптографічного захисту інформації для забезпечення конфіденційності та цілісності даних у сучасних ІКСМ.

3. ОСНОВНА ЧАСТИНА ДОСЛІДЖЕННЯ

3.1. Теоретичне обґрунтування удосконалення модуля захисту

З огляду на результати проведеного аналізу, прототипом було обрано розглянутий модуль MTProto Mobile Protocol v.1.0 [2], порівняно з яким було змінено наступне:

1. Змінені вхідні та вихідні дані. На вході приймаються і обробляються наступні дані: повідомлення M, інформацію про ідентифікатор користувача та ідентифікатор сесії S, інформацію про час відправлення і довжину повідомлення ID та порядковий номер повідомлення PD. На виході тільки отримуємо $mHash$ – геш значення DB ($DB = (S, ID, M)$) та $EncP$ – зашифроване повідомлення P.

2. Замість використання геш функції SHA-1 введено використання певної криптостійкої геш функції F_{hash}. Слід зауважити, що у якості F_{hash} може бути використана функція гешування, що побудована на основі одного із методів [5-7].

3. Замість використання блокового шифру AES введено використання функції F_{enc}. Слід зауважити, що у якості F_{enc} може бути використаний певний криптостійкий алгоритм шифрування, побудований на основі блокових, потокових шифрів чи геш функцій тощо [8-10].

4. У якості *authKey*, ввдено використання заздалегідь узгодженого секретного ключа користувачів, наприклад за допомогою протоколів асиметричної криптографії.

3.2. Опис удосконаленого модуля криптографічного захисту інформації

Нехай маємо повідомлення M, $M \in V_m$, $V_m \in \{0,1\}^m$, яке потрібно зашифрувати для передавання. Тоді готується наступне повідомлення (містить окрім повідомлення M, інформацію про ідентифікатор користувача та ідентифікатор сесії (S, $S \in V_s$, $s \in Z_+$), інформацію про час відправлення і довжину повідомлення (ID, $ID \in V_{id}$, $id \in Z_+$) та порядковий номер повідомлення (PD, $PD \in V_{pd}$, $pd \in Z_+$)):

$$P = (S, ID, M, PD),$$

де $P \in V_p$, $p = m + s + id + pd$.

Алгоритм зашифрування. Розглянемо поетапно більш детально схему роботи *алгоритму зашифрування* (рис. 1).

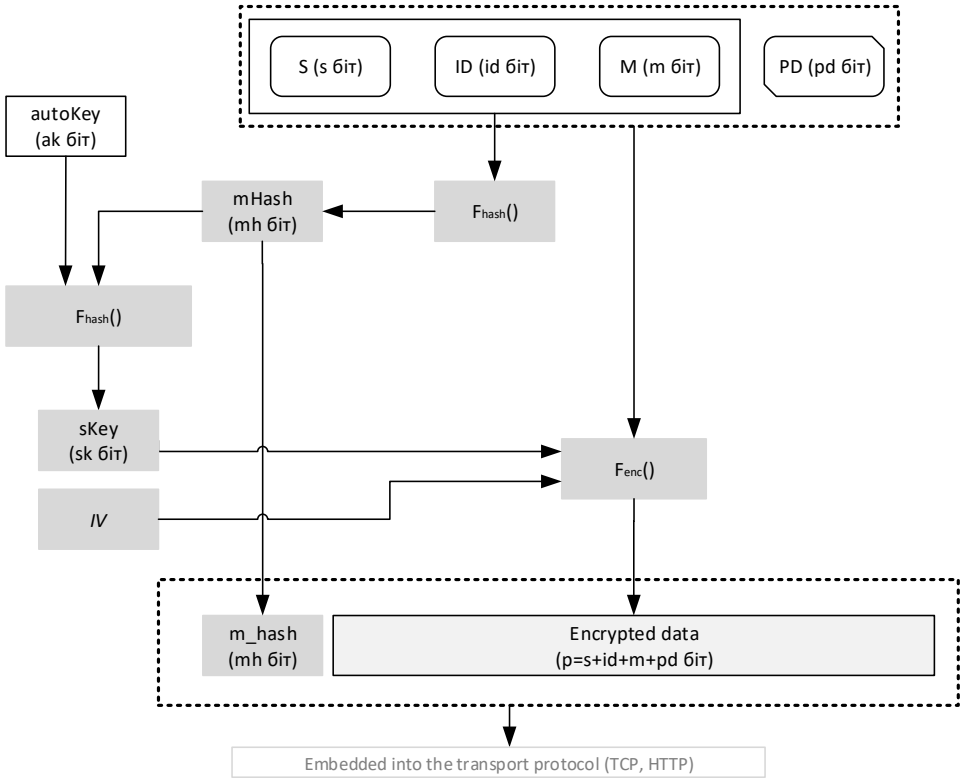

Рис. 1 . Схема роботи удосконаленого модуля криптографічного захисту інформації

Етап 1. *Формування блоку даних* DB *для обрахунку геш значення:*

$$DB = (S, ID, M),$$

де $DB \in V_{db}$, $db = m + s + id$, S – ідентифікатор користувача та ідентифікатор сесії, $S \in V_s$, $s \in Z_+$, ID – інформація про час відправлення і довжину повідомлення, $ID \in V_{id}$, $id \in Z_+$, M – саме повідомлення, $M \in V_m$.

Етап 2. *Формування геш значення повідомлення* DB:

$$mHash = F_{hash}(DB),$$

де $mHash$ – геш значення DB, $DB \in V_{db}$, $mHash \in V_{mh}$, $mh \in Z_+$, $F_{hash}(x)$ – деяка функція гешування.

Етап 3. *Формування ключа сеансу* $sKey$:

$$sKey = F_{hash}(authKey, mHash),$$

де $sKey$ – сеансовий ключ, $sKey \in V_{sk}$, $sk \in Z_+$, $authKey$ – секретний ключ автентифікації (користувачам потрібно заздалегідь узгодити даний ключ, наприклад за допомогою протоколів асиметричної криптографії), $authKey \in V_{ak}$, $ak \in Z_+$, $F_{hash}(x)$ – деяка функція гешування.

Етап 4. *Шифрування за допомого криптографічного алгоритму:*

$$EncP = F_{enc}(P, sKey, IV),$$

де $EncP$ – зашифроване повідомлення P, $EncP \in V_p$, P – повідомлення із додатковою інформацією, $P \in V_p$, $sKey$ – сеансовий ключ, $sKey \in V_{sk}$, IV – вектор ініціалізації, $IV \in V_{iv}$, $iv \in Z_+$, $F_{enc}(P, sKey, IV)$ – функція шифрування (може бути побудована на основі блокових і потокових шифрів, геш функцій тощо).

Етап 5. *Формування кінцевого повідомлення:*

$$EncMes = (mHash, EncP),$$

де $EncMes$ – кінцеве зашифроване повідомлення, $EncMes \in V_{p+mh}$, $mHash$ – геш значення DB, $DB \in V_{db}$, $EncP$ – зашифроване повідомлення P, $EncP \in V_p$.

Алгоритм розшифрування. Розглянемо поетапно більш детально схему роботи *алгоритму розшифрування*.

Етап 1. *Розкладання отриманого зашифрованого повідомлення на частини:*

$$(mHash, EncP) = EncMes,$$

де $EncMes$ – отримане зашифроване повідомлення, $EncMes \in V_{p+mh}$, $mHash$ – геш значення DB, $DB \in V_{db}$, $EncP$ – зашифроване повідомлення P, $EncP \in V_p$.

Етап 2. *Формування ключа сеансу* $sKey$ *:*

$$sKey = F_{hash}\left(authKey, mHash\right),$$

де $mHash$ – геш значення DB, $DB \in V_{db}$, $mHash \in V_{mh}$, $mh \in Z_+$, $sKey$ – сеансовий ключ, $sKey \in V_{sk}$, $sk \in Z_+$, $authKey$ – секретний ключ автентифікації (користувачам потрібно заздалегідь узгодити даний ключ, наприклад за допомогою протоколів асиметричної криптографії), $authKey \in V_{ak}$, $ak \in Z_+$.

Етап 3. *Розшифрування за допомого криптографічного алгоритму:*

$$P = F_{dec}\left(EncP, sKey, IV\right),$$

де $EncP$ – зашифроване повідомлення P, $EncP \in V_p$, P – повідомлення із додатковою інформацією, $P \in V_p$, $sKey$ – сеансовий ключ, $sKey \in V_{sk}$, IV – вектор ініціалізації, $IV \in V_{iv}$, $iv \in Z_+$, $F_{dec}\left(EncP, sKey, IV\right)$ – функція розшифрування обернена до $F_{enc}\left(P, sKey, IV\right)$.

Етап 4. *Розкладання блоку даних* P *на частини:*

$$\left(S, ID, M, PD\right) = P,$$

де $P \in V_p$, $p = m + s + id + pd$, S – ідентифікатор користувача та ідентифікатор сесії, $S \in V_s$, $s \in Z_+$, ID – інформація про час відправлення і довжину повідомлення, $ID \in V_{id}$, $id \in Z_+$, M – повідомлення, $M \in V_m$, порядковий номер повідомлення PD, $PD \in V_{pd}$, $pd \in Z_+$).

Етап 5. *Формування перевірочного блоку даних* DB' *для обрахунку геш значення:*

$$DB' = \left(S, ID, M\right),$$

де $DB' \in V_{db}$, $db = m + s + id$, S – ідентифікатор користувача та ідентифікатор сесії, $S \in V_s$, $s \in Z_+$, ID – інформація про час відправлення і довжину повідомлення, $ID \in V_{id}$, $id \in Z_+$, M – саме повідомлення, $M \in V_m$.

Етап 6. *Формування перевірочного геш значення повідомлення* DB':

$$mHash' = F_{hash}\left(DB'\right),$$

де $mHash'$ – перевірочне геш значення DB', $DB' \in V_{db}$, $mHash \in V_{mh}$, $mh \in Z_+$.

Етап 7. *Перевірка* $mHash'$ та $mHash$:

$$mHash' == mHash$$

Якщо $mHash'$ і $mHash$ рівні – це значить повідомлення не було змінено зловмисником.

Етап 8. *Перевірка системних даних:* отриманий ідентифікатор користувача та ідентифікатор сесії, інформацію про час відправлення і довжину повідомлення,

порядковий номер повідомлення. Якщо ці дані істині та коректні, то повідомлення надіслав легітимний користувач, і можемо прочитати повідомлення M .

Для використання цього модуля на практиці потрібно визначитись з функціями гешування F_{hash} та шифрування F_{enc} .

4. ВИСНОВКИ

У цій роботі удосконалено модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволяє забезпечити конфіденційність і цілісність даних в ІКСМ.

Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа $authKey$. У якості функцій F_{enc} та F_{hash} можуть бути використані зокрема й алгоритми, запропоновані авторами у своїх попередніх роботах [6, 8-10], або інші відомі криптоалгоритми [5, 7, 11-13], стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

У подальших роботах планується зосередити увагу на практичних дослідженнях удосконаленого модуля криптографічного захисту інформації з використанням різних методів шифрування і гешування, зокрема тих, що були запропоновані авторами у своїх попередніх дослідженнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Oppliger, R. (2021). *Cryptography 101: From Theory to Practice.* Artech.
2 Job J, Naresh V & Chandrasekaran, K. (2015). A modified secure version of the Telegram protocol (MTProto). У *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. IEEE. https://doi.org/10.1109/conecct.2015.7383884
3 D. van D. (2019). *Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol.* Radboud University.
4 *TLS and SRTP for Skype Connect Technical Datasheet*. (2011). Skype.
5 Wu, Q. (2015). A Chaos-Based Hash Function. У *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (p. 1–4).
6 Gnatyuk, S., Kinzeryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., & Odarchenko, R. (2019). Secure Hash Function Constructing for Future Communication Systems and Networks. У *Advances in Artificial Systems for Medicine and Education II* (с. 561–569). Springer International Publishing. https://doi.org/10.1007/978-3-030-12082-5_51.
7 Rajeshwaran, K., Anil Kumar, K. (2019). Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function. У *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE. https://doi.org/10.1109/icecct.2019.8869146
8 Iavich, M., Iashvili, G., Gnatyuk, S., Tolbatov, A., Mirtskhulava, L. (2021). Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. *Communications in Computer and Information Science,* 1486, 185-193, 2021.
9 Gnatyuk, S., Iavich, M., Kinzeryavyy. V., Okhrimenko, T., Burmak, Y., Goncharenko, I. (2020). Improved secure stream cipher for cloud computing. *CEUR Workshop Proceedings,* 2732, 183-197.
10 Gnatyuk, S., Akhmetov, B., Kozlovskyi, V., Kinzeryavyy, V., Aleksander, M., Prysiazhnyi, D. (2020). New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis. *Advances in Intelligent Systems and Computing,* 1126, 93-104.
11 Kuznetsov, A., Horkovenko, I., Maliy, O., Goncharov, N., Kuznetsova, T., & Kovalenko, N. (2020). Non-Binary Cryptographic Functions for Symmetric Ciphers. У *2020 IEEE International Conference on*

Problems of Infocommunications. Science and Technology (PIC S&T). IEEE. https://doi.org/10.1109/picst51311.2020.9467982.

12 Jintcharadze, E., & Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. У *2020 IEEE East-West Design & Test Symposium (EWDTS)*. IEEE. https://doi.org/10.1109/ewdts50664.2020.9224901.

13 Lee, T. R., Teh, J. S., Jamil, N., Yan, J. L. S., Chen, J. (2021). Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes. *IEEE Access*, 9, 134052-134064. https://doi.org/10.1109/ACCESS.2021.3116468.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Sergiy O. Gnatyuk
DSc, Professor,
Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua,

Tetiana V. Smirnova
PhD, Associate Professor,
Associate Professor of Academic Dept of Cybersecurity and Software
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-5093-1581
sm.tetyana@gmail.com

Rat Sh. Berdibayev
PhD,
Chair of Scientific and Technical Center of Information Security Problems n.a. Turganbek Omar
Almaty University of Power Energy and Telecommunication, Almaty, Kazakhstan
ORCID ID: 0000-0002-8341-9645
r.berdybaev@aues.kz

Yuliia A. Burmak
PhD degree applicant in NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-5410-6260
julburmac@gmail.com

Dinara M. Ospanova
PhD Student
Kazakh Humanitarian Juridical Innovative University, Semey, Kazakhstan
ORCID ID: 0000-0002-2206-7367
odm-1778@mail.ru

IMPROVED MODULE FOR DATA CRYPTOGRAPHIC SECURITY IN MODERN INFORMATION-COMMUNICATION SYSTEMS AND NETWORKS

Abstract. Up-to-date methods and means of data encryption guarantee reliable security (in particular, data confidentiality and integrity), but the development of cryptanalysis methods encourages the development and implementation of new, more efficient, cryptoalgorithms. In addition, the formation of new requirements for cryptographic methods and means is influenced by the development of modern information and communication technologies (LTE/5G/6G). With this in mind, in the paper well-known software modules of cryptographic data protection were analyzed, which are currently used in messengers and other applications. This analysis revealed the advantages, disadvantages and ways to improve (in particular, through the use of modern security procedures) modules of cryptographic data protection. A prototype was selected and the cryptographic information security module was improved. This module fixes information about the user ID, session ID, sending time, message length and serial number, as well as uses a new session key generation procedure for encryption. It allows to ensure the data confidentiality and integrity in information-communication systems and networks. To effectively use the advanced method, it is important to choose secure encryption and hashing methods, as well as secret key synchronization. Known cryptographic methods and tools secure against linear, differential, algebraic, quantum and other known types of cryptanalysis can be used there. Further work will focus on practical research of the advanced module for data cryptographic security using various methods of encryption and hashing, in particular those proposed by the authors in their previous research studies.

Keywords: information security, cryptography, confidentiality, integrity, encryption module, information-communication systems and networks, messenger.

REFERENCES

1 Oppliger, R. (2021). *Cryptography 101: From Theory to Practice.* Artech.
2 Job J, Naresh V & Chandrasekaran, K. (2015). A modified secure version of the Telegram protocol (MTProto). У *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*. IEEE. https://doi.org/10.1109/conecct.2015.7383884
3 D. van D. (2019). *Analysing the Signal Protocol. A manual and automated analysis of the Signal Protocol.* Radboud University.
4 *TLS and SRTP for Skype Connect Technical Datasheet*. (2011). Skype.
5 Wu, Q. (2015). A Chaos-Based Hash Function. У *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (p. 1–4).
6 Gnatyuk, S., Kinzeryavyy, V., Kyrychenko, K., Yubuzova, K., Aleksander, M., & Odarchenko, R. (2019). Secure Hash Function Constructing for Future Communication Systems and Networks. У *Advances in Artificial Systems for Medicine and Education II* (с. 561–569). Springer International Publishing. https://doi.org/10.1007/978-3-030-12082-5_51.
7 Rajeshwaran, K., Anil Kumar, K. (2019). Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function. У *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. IEEE. https://doi.org/10.1109/icecct.2019.8869146
8 Iavich, M., Iashvili, G., Gnatyuk, S., Tolbatov, A., Mirtskhulava, L. (2021). Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. *Communications in Computer and Information Science,* 1486, 185-193, 2021.
9 Gnatyuk, S., Iavich, M., Kinzeryavyy. V., Okhrimenko, T., Burmak, Y., Goncharenko, I. (2020). Improved secure stream cipher for cloud computing. *CEUR Workshop Proceedings,* 2732, 183-197.
10 Gnatyuk, S., Akhmetov, B., Kozlovskyi, V., Kinzeryavyy, V., Aleksander, M., Prysiazhnyi, D. (2020). New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis. *Advances in Intelligent Systems and Computing,* 1126, 93-104.
11 Kuznetsov, A., Horkovenko, I., Maliy, O., Goncharov, N., Kuznetsova, T., & Kovalenko, N. (2020). Non-Binary Cryptographic Functions for Symmetric Ciphers. У *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE. https://doi.org/10.1109/picst51311.2020.9467982.
12 Jintcharadze, E., & Iavich, M. (2020). Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. У *2020 IEEE East-West Design & Test Symposium (EWDTS)*. IEEE. https://doi.org/10.1109/ewdts50664.2020.9224901.
13 Lee, T. R., Teh, J. S., Jamil, N., Yan, J. L. S., Chen, J. (2021). Lightweight Block Cipher Security Evaluation Based on Machine Learning Classifiers and Active S-Boxes. *IEEE Access,* 9, 134052-134064. https://doi.org/10.1109/ACCESS.2021.3116468.