УДК 004.415.056.5
DOI https://doi.org/10.17721/ISTS.2020.4.71-80

С. В. Толюпа, orcid.org/0000-0002-1919-9174, **tolupa@i.ua**
В. С. Наконечний, orcid.org/0000-0002-0247-5400, **nvc2006@i.ua**
В. Г. Сайко, orcid.org/0000-0002-3059-6787, **vgsaiko@gmail.com**
М. Котов, orcid.org/0000-0003-1153-3198, **shunki2001@ukr.net**
В. Солодовник, orcid.org/0000-0002-8844-4348, **valeriamin6@gmail.com**
Київський національний університет імені Тараса Шевченка, Київ, Україна

ВИКОРИСТАННЯ СИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ ДЛЯ ПЕРЕДАЧІ СИГНАЛІВ У ПРИСТРОЯХ БЕЗДРОТОВОГО ВВЕДЕННЯ ДАНИХ

Нині існує безліч обчислювальних систем, які призначені для покращення, полегшення та вдосконалення життя людини. Оскільки з'являється все більше дослідників, які зацікавленні у сфері оброблення інформації, розвиток обчислювальних систем щороку набирає обертів. З розвитком інформаційних систем, не менш швидкими темпами розвиваються і можливі загрози, такі як порушення конфіденційності, цілісності та доступності інформації, що обробляється. З метою запобігання можливим втратам новітні системи захисту інформації постійно оновлюють і вдосконалюють. Оскільки неможливо створити абсолютно захищену систему, завжди є імовірність викрадення даних, тому проблема захисту інформаційних і телекомунікаційних систем набирає все більшої актуальності. Враховуючи те, що жодний захист не може бути досконалим, розроблено спосіб значного зменшення порушення конфіденційності даних. На сьогодні криптосистеми найбільше використовуються для захисту інформаційно-телекомунікаційних систем та інших технологій, зокрема і для захисту надважливої інформації держави, підприємства, особи або інших критично важливих даних, зокрема корпоративних таємниць, розвідувальних даних чи комерційних таємниць.

Презентовано способи використання симетричних алгоритмів для передавання сигналів у пристроях дистанційного введення даних. Подано інформацію про існуючі алгоритми шифрування й використання хеш-функцій. Проведено розмежування між одноключовим і двоключовим методами шифрування інформації. Детально розглянуто алгоритм AES його функції, робота раундів, схеми шифрування даних. Опис кожного алгоритму супроводжується прикладом, в якому пояснюються особливості його використання. Представлено математичну модель і приклад роботи блочного алгоритму шифрування. Висвітлено принципи роботи бездротових пристроїв. Розглянуто вразливості, пов'язані з бездротовими приладами та запропоновано рішення щодо їхнього захисту.

Ключові слова: *криптографія, шифрування, симетричне шифрування, блокове шифрування, шифрування сигналів, пристрої бездротового введення даних.*

1. ВСТУП

Нині існує безліч обчислювальних систем, які призначені для покращення, полегшення та вдосконалення життя людини. Оскільки з'являється все більше дослідників, які зацікавленні у сфері оброблення інформації, розвиток обчислювальних систем щороку набирає обертів. З розвитком інформаційних систем, не менш швидкими темпами розвиваються і можливі загрози, такі як порушення конфіденційності, цілісності та доступності інформації, що обробляється. З метою запобігання можливим втратам новітні системи захисту інформації постійно оновлюють і вдосконалюють. Оскільки неможливо створити абсолютно захищену систему, завжди є імовірність викрадення даних, тому проблема захисту інформаційних і телекомунікаційних систем набирає все більшої актуальності. Враховуючи те, що жодний захист не може бути досконалим, розроблено спосіб значного зменшення порушення конфіденційності даних.

Можливими способами захисту інформації є стеганографія та криптографія. Основна ціль стеганографії – приховування факту передавання чи зберігання інформації, а криптографії – приховування вмісту переданої інформації. Використовуючи сучасні криптографічні алгоритми шифрування інформації, можливо зберегти її конфіденційність навіть за умови несанкціонованого доступу до неї.

На сьогодні криптосистеми найбільше використовують для захисту інформаційно-телекомунікаційних систем та інших технологій, зокрема і для захисту надважливої інформації держави, підприємства, особи або інших критично важливих даних, зокрема корпоративних таємниць, розвідувальних даних чи комерційних таємниць.

2. ПОСТАНОВКА ПРОБЛЕМИ

Як відомо надійність криптосистем залежить від виконання таких вимог: зберігання ключів у таємниці, генерації псевдовипадкових чисел, алгоритм проведення шифрування тощо [1–5].

У розвиток криптографії значний внесок зробили в своїх працях такі автори: Кузнецов О. О., Горбенко І. Д., Кавальчук Л. В., Dan Boneh, Victor Shoup, Mohamed Barakat, Christian Eder, Timo Hanke, Steven D Galbraith, William Stallings [1–4]. Активно описували симетричне шифрування у своїх наукових працях Joseph Sterling Grah, Nigel Smart, Christof Paar, Jan Pelzl [7, 9, 11].

Питання застосування та функціонування шифру AES свого часу розглядали в своїх роботах Joan Daemen, Vincent Rijmen [12, 13]. Результати досліджень блочних алгоритмів шифрування викладено у працях А. В. Яковлева, А. А. Безбогова, В. В. Родіна, В. Н. Шамкіна, Roberto Avanzi, Bruce Schneier, Lars R, Knudsen Matthew, J.B. Robshaw [16, 18, 19, 20].

Останні події у світі підтвердили особливу важливість протидії порушникам і спробам ведення інформаційної боротьби з метою нанесення втрат. Достатньо детальний аналіз також підтвердив, що поряд з іншими методами і механізмами захисту інформації важливими є такі, що базуються на криптографічних перетвореннях інформації. Дійсно, при правильному виборі та застосуванні, відповідно до вимог криптографічних перетворень, досягається високий рівень безпеки, а також конфіденційність, цілісність, захист від НСД, доступність, неспростовність тощо.

У випадку криптографічного захисту інформації висуваються та повинні бути забезпечені криптографічна стійкість, цілісність, швидкодія криптографічних перетворень і вимоги, що висуваються додатками.

Зрозуміло, що криптографічна стійкість є безумовною вимогою, але поряд із нею швидкодія вже є також безумовною вимогою – потрібно захищати канали зі швидкістю від сотень мегабіт до десятків гігабіт за секунду, виконуючи операції в реальному часі. Указана вимога може бути виконана у разі застосування криптографічних перетворень типу блоковий симетричний шифр.

Тому проблема захисту інформації під час передавання сигналів у пристроях бездротового введення даних (ПБВД) є надзвичайно актуальною. Саме висвітленню та вирішенню цього питання й присвячена ця робота.

3. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Криптографія – наука, що розробляє методи використання складних математичних перетворень для приведення інформації, яка передається через канали поширення, у такій формі, в якій її не зможе отримати ніхто крім авторизованих і дозволених осіб.

Шифрування – ключовий об’єкт дослідження криптографів, це процес, під час якого змінюється форма інформації, що передається через відкриті канали передачі [1, 2].

Алгоритм шифрування – це набір зворотних математичних перетворень, що надають тексту шифрованого вигляду [1].

Існують три базові види шифрування даних [1]:

- шифрування з використанням двох ключів;
- шифрування з використанням одного ключа;
- безключове шифрування даних.

Принципова різниця між безключовими, одноключовими та двоключовими алгоритмами полягає у процесі шифрування вхідної інформації.

Безключові системи не використовують ключі у процесі криптографічного перетворення інформації. До безключових криптосистем належать хеш-функції та генератори псевдовипадкових чисел [5].

Хеш-функція – це функція що здійснює перетворення вхідного масиву даних довільної величини в бітовий рядок фіксованої довжини, та виконується за допомогою певного алгоритму [6, 7].

Як правило хеш-функції використовують [6, 7]:

- для побудови унікальних ідентифікаторів;
- для обчислення контрольних сум від даних для подальшого виявлення в них помилок, що виникають при зберіганні або передаванні даних;
- для пошуку дублікатів в серіях наборів даних;
- для побудови асоціативних масивів;
- для збереження паролів у системах захисту у вигляді хеш-коду. Відновлення такого пароля потребує функцію, яка буде зворотною до тої, що була використана для хешування паролів.

Одноключові системи у процесі криптографічного перетворення інформації використовують криптографічний ключ для шифрування та розшифрування даних. Ключ шифрування може складатись із чисел, слів або символів. Оскільки кожен, хто має доступ до ключа, може розшифрувати інформацію, то такий ключ має залишатися в таємниці, бути відомим лише для відправника й отримувача, щоб забезпечити стійкість шифрування [5].

Схему використання одноключової системи показано на рис. 1.

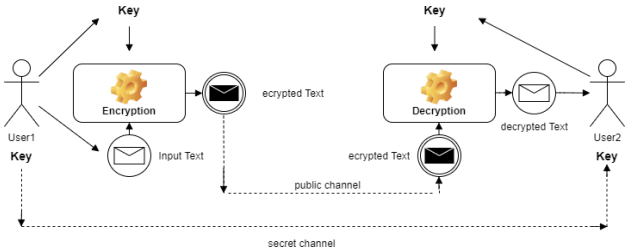

Рис. 1. Одноключове шифрування інформації

Двоключове шифрування інформації – спосіб шифрування даних, при якому використовуються два ключі шифрування: публічний і приватний. Головне досягнення асиметричного шифрування полягає у тому, що необхідність передавання ключа через спеціальний засекречений канал відпадає [5].

Схему використання асиметричної системи показано на рис. 2.

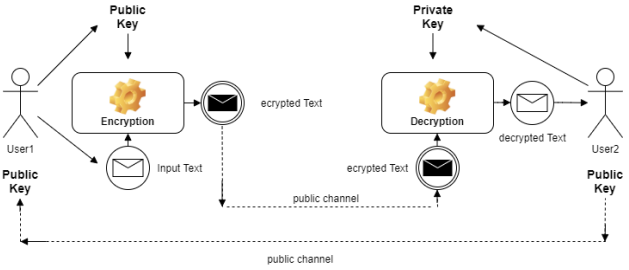

Рис. 2. Асиметричне шифрування інформації

Загалом суть асиметричних алгоритмів полягає в такому [5]: отримувач генерує два ключі – публічний і приватний. Після цього отримувач передає публічний ключ тому, хто надсилає повідомлення, а приватний залишає собі. Отримавши публічний ключ, перший користувач зашифровує інформацію, використавши цей ключ, та надсилає зашифрований текст.

Розшифрувати це повідомлення зможе лише той, хто має приватний ключ. За допомогою публічного ключа розшифрувати дане повідомлення – неможливо. Саме тому не потрібно використовувати засекречені канали зв'язку для передавання ключа.

Як зазначалося вище, алгоритми симетричного шифрування використовують лише один приватний ключ для шифрування вхідних даних. Якщо алгоритм шифрування достатньо криптостійкий, то єдиний спосіб зловмиснику розшифрувати інформацію – отримати секретний ключ.

Криптостійкість алгоритму шифрування визначається складністю розшифрування тексту методом грубої сили, тобто перебиранням усіх можливих комбінацій ключів. Алгоритм вважається нестійким, якщо вдалося перебрати половину усіх можливих комбінацій ключа. Ключ довжиною 128 біт, сучасні комп'ютери зможуть зламати лише через мільярди років, у свою чергу ключі довжиною 256 біт вважаються безпечними, теоретично спроможні встояти проти грубої атаки квантових комп'ютерів [8–11].

Як правило, для систем криптографічного захисту інформації, що практично використовуються, довжина повідомлення, що захищається за допомогою симетричного блокового шифру, значно перевершує довжину ключа шифрування. У цьому випадку не виконується критерій безумовної стійкості шифру, що використовується, і в таких умовах доцільне введення поліноміального критерію, що припускає наявність обмежень для обчислювальних ресурсів зловмисника та часу, протягом якого шифр залишається стійким. Поліноміальний критерій приводить до практичного критерію стійкості – неможливості реалізації атаки на шифр в умовах сучасної обчислювальної бази протягом тривалого строку.

Додатково, з огляду на можливість удосконалювання криптоаналітичних методів, вводиться критерій "запасу стійкості" до аналітичних атак – складність атаки на весь алгоритм має бути значно вищою складності силових атак.

Зазвичай цей критерій розглядає версію симетричного блокового алгоритму шифрування зі зменшеною кількістю циклів, що є уразливою проти криптографічного аналізу. Різниця в кількості циклів визначає запас стійкості алгоритму до конкретної криптоаналітичної атаки.

Для оцінювання криптографічної стійкості загальної конструкції шифру доцільно ввести ще один критерій, що розглядає можливість виключення яких-небудь операцій або заміни їх менш складними операціями (наприклад, на деяких наборах вхідних даних операція додавання за модулем 2^{32} близька або еквівалентна операції

додавання за модулем 2). У цьому випадку повноцикловий варіант спрощеного шифру повинен залишатися стійким до аналітичних атак.

Необхідно також враховувати, що більшість сучасних аналітичних атак, насамперед, таких як диференціальний і лінійний криптоаналіз, є статистичними. У процесі криптоаналізу для одержання ключа виконується велика кількість шифрувань і на підставі шифротекстів формуються варіанти підключів. Під час оброблення досить великої вибірки шифротекстів, сформованих на одному ключі, правильне значення ключових бітів зустрічається частіше інших варіантів.

Очевидно, що ймовірність знаходження правильної пари (що пропонує коректне значення ключа) залежить від статистичних властивостей шифру, і для збільшення складності криптоаналізу властивості криптограми повинні бути близькі до властивостей випадкової послідовності. Тому необхідною (але не достатньою) умовою стійкості шифру до аналітичних атак є забезпечення гарних статистичних властивостей вихідної послідовності (шифротекстів).

Для захисту шифру від алгебраїчних атак необхідно, щоб не існувало способу практичної побудови системи рівнянь, що зв'язують відкритий текст, криптограму та ключ шифрування, або не існувало способу розв'язання таких систем у поліноміальний час.

У побудові засобів криптографічного захисту необхідно враховувати можливість організації атак на реалізацію (зміна температурного режиму електронного пристрою, вхідної напруги, поява іонізуючого випромінювання, вимірювання струмів, що споживаються, ПЕМІН, час виконання тощо).

Такі атаки можуть бути ефективні проти всіх криптографічних алгоритмів, і захист від таких атак вимагає інженерних рішень уже на етапі проєктування засобів криптографічного захисту інформації.

4. РЕЗУЛЬТАТИ

Нині є два види симетричного шифрування [11]:

- блочний;
- поточний.

Свої назви, ці види дістали від способу оброблення вхідного тексту.

Блочні алгоритми шифрують текст блоками по 128 біт, шляхом застосування алгоритмів шифрування, до яких у свою чергу додається ключ довжиною 128, 192 або 256 біт.

Схему блочного шифру показано на рис. 3.

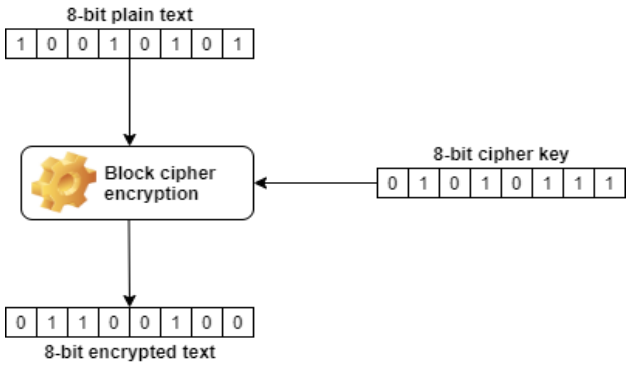

Рис. 3. Схема блочного шифру

Поточні шифри, у свою чергу, працюють із кожним бітом вхідного тексту та видають по біту вихідного, шифрованого тексту.

Схему поточного шифру показано на рис. 4.

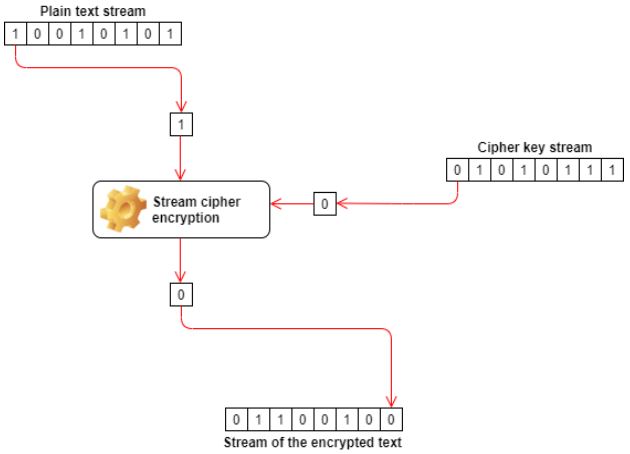

Рис. 4. Схема поточного шифру

Схема роботи AES показана на рис. 5.

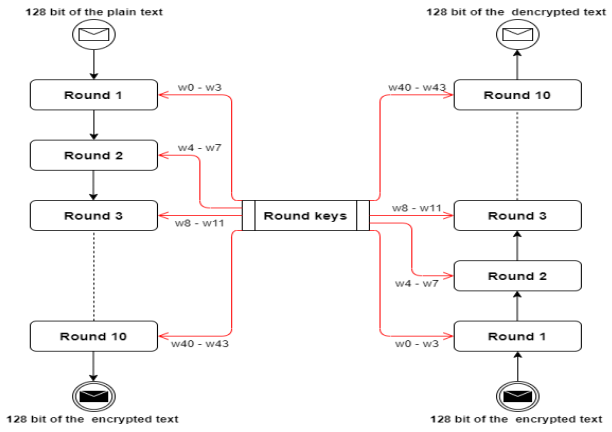

Рис. 5. Схема шифрування алгоритму AES

Відповідно до схеми на рис. 5 шифрування та дешифрування тексту відбувається протягом

десяти раундів, на кожному з раундів додається ключ раунду.

Нехай маємо 128 біт вхідного тексту A та 128 біт раундового ключа K, перед першим раундом, спочатку виконується операція AddRoundKey, це операція XOR вхідного тексту з ключем, тобто:

$$B = A \text{ XOR } K,$$

де B – 128 біт тексту після операції AddRoundKey [12].

Кожний раунд шифрування та дешифрування AES складається з чотирьох перетворень вхідної матриці [12]:

1. Для раунду шифрування виконують такі перетворення:

1) SubBytes – побайтова підстановка в S-BOX, з фіксованою таблицею замін.

2) ShiftRows – побайтове зрушення рядків матриці State.

3) MixColomns – перемішування байтів у колонках.

4) AddRoundKey – додавання ключа раунду.

2. Для раунду дешифрування виконуються такі перетворення:

1) InvShiftRows – зворотна операція до ShiftRows.

2) Inv SubBytes – зворотна операція до SubBytes.

3) AddRoundKey – додавання ключа раунду.

4) InvMixColomns – зворотна операція до MixColomns.

Останній раунд шифрування відрізняється від інших тим, що не активізує перетворення MixColomns [13].

На рис. 6 представлено схему перетворень у кожному раунді шифрування та дешифрування.

Відповідно до принципу Керкгоффса, оцінювати криптографічну стійкість алгоритму потрібно з урахуванням того, що зловмисник знає всі процедури перетворення вхідного тексту, які виконуються даним алгоритмом. Тобто в секреті залишається лише такий параметр – ключ шифрування [14, 15].

Зі сторони зловмисника, довжина ключа визначає доцільність виконання повного перебору всіх можливих його комбінацій, оскільки інформацію, що зашифрована довшим ключем, набагато складніше зламати атакою грубої сили.

Для прикладу візьмемо ключ довжиною 4 біти, використовуючи основні закони комбінаторики, можливо обчислити всі можливі варіанти перебору: S = 2 * 2 * 2 * 2 = 16. Таким чином, кількість можливих варіантів перебору становить S = 16.

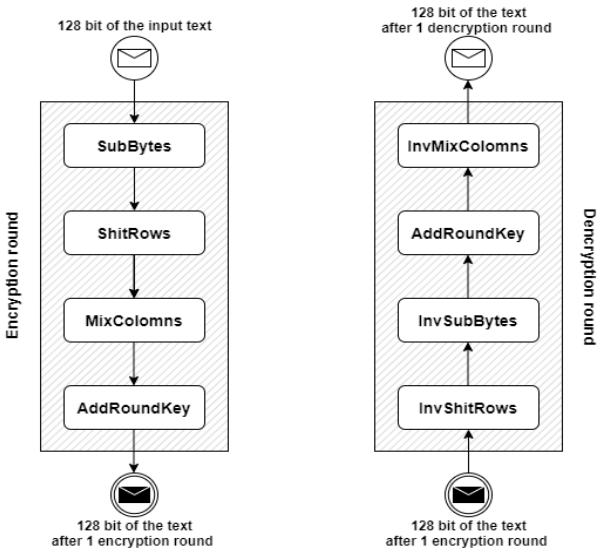

Рис. 6. Схема раундів алгоритму AES

Нехай маємо 10 000 машин, кожна перевіряє 1 000 000 комбінацій ключа шифрування за секунду, алгоритм вважається зламаним, якщо вдалось перебрати половину варіантів, на цій основі виконано табл. 1.

***Таблиця* 1**

Таблиця переборів ключів

Key size (bit)	Combinations	Time to check all combinations
1	2	2 * 10^(-10) sec
2	4	4 * 10^(-10) sec
4	16	1.6 * 10^(-9) sec
8	256	2.56 * 10^(-8) sec
16	65 536	6.5536 * 10^(-6) sec
32	4 294 967 296	0.4294967296 sec
56 (DES)	7.20575940 * 10^16	83.3999930995 days
64	1.84467441 * 10^19	58.4942417355 years
128 (AES)	3.40282367 * 10^38	1.07902831 * 10^21 years
192 (AES)	6.27710174 * 10^57	1.99045590 * 10^40 years
256 (AES)	1.15792089 * 10^77	3.67174306 * 10^59 years

Оцінивши результати обчислень з табл. 1, можна зробити висновок, що ключ довжиною 128 біт надійно шифрує інформацію. Ключ довжино 256 біт – теоретично стійкий до лобової атаки квантових комп'ютерів.

Блочним типом шифрування є система шифрування, яка залежно від алгоритму, обраного ще на початку своєї роботи, використовує його у кожному такті своєї роботи.

Відомо, що блочний алгоритм шифрування, по суті є шифром заміни, проте основна його особливість полягає в тому, що цей шифр має величезний алфавіт. Кожний алфавітний знак

представляє собою певну послідовність двійкових чисел 0 і 1, тобто двійкових даних, визначеного розміру [16–21].

Щоб краще уявити, як працює ця система, візьмемо блок розміру N (послідовність 0 і 1): $p = (p_0, p_1, p_2, \ldots, p_{N-1}) \in Z_{2,N}$, де p в $Z_{2,N}$ – це вектор, представлений у вигляді фіксованої довжини 0 і 1. Тоді двійкове подання числа ми отримаємо, підставивши дані у формулу

$$||p|| = \sum_{i=0}^{N-1} 2^{N-i-1} p_i. \quad (1)$$

Тоді очевидним стає те, що стійкість шифру напряму залежить від розмірів таблиць заміни, які неможливо фізично представити через величину їх обсягів.

Створимо таку таблицю. Для прикладу візьмемо значення N = 5, тоді табл. 1 виглядатиме таким чином:

***Таблиця* 2**

Таблиця заміни

(0,0,0,0,0)→0	(0,0,0,0,1)→1	(0,0,0,1,0)→2	(0,0,0,1,1)→3
(0,0,1,0,0)→4	(0,0,1,0,1)→5	(0,0,1,1,0)→6	(0,0,1,1,1)→7
(0,1,0,0,0)→8	(0,1,0,0,1)→9	(0,1,0,1,0)→10	(0,1,0,1,1)→11
(0,1,1,0,0)→12	(0,1,1,0,1)→13	(0,1,1,1,0)→14	(0,1,1,1,1)→15
(1,0,0,0,0)→16	(1,0,0,0,1)→17	(1,0,0,1,0)→18	(1,0,0,1,1)→19
(1,0,1,0,0)→20	(1,0,1,0,1)→21	(1,0,1,1,0)→22	(1,0,1,1,1)→23
(1,1,0,0,0)→24	(1,1,0,0,1)→25	(1,1,0,1,0)→26	(1,1,0,1,1)→27
(1,1,1,0,0)→28	(1,1,1,0,1)→29	(1,1,1,1,0)→30	(1,1,1,1,1)→31

Позначимо, що блоковий шифр виглядає таким чином:

$$\pi \in SYM(Z_{2,N});\ \pi: p \rightarrow q = \pi(p),$$

де $p = (p_0, p_1, p_2, \ldots, p_{N-1})$, $q = (q_0, q_1, q_2, \ldots, q_{N-1})$.

Як уже зазначалося, блоковий шифр є окремим випадком підстановки, тільки він має великий алфавіт, проте цей вид шифрів розглядається окремо, адже зараз вони широко використовуються і їх набагато легше і зручніше описати за допомогою алгоритмів.

Усі криптосистеми реалізовані за допомогою блокових шифрів, адже методика їхнього використання полягає в тому, що створюється ланцюг з уже зашифрованих даним алгоритмом байтів. Це дозволяє шифрувати інформацію, пакетний об'єм якої є необмеженим [16].

Вихідний текст шифрується за допомогою підстановки π, яку обирають із повної симетричної групи.

Тоді зловмисник, який займається проведенням атаки і робить спроби для знаходження відповідності між зашифрованим і вихідним текстом $p_i \leftrightarrow q_i$, $0 \le i \le m$, не може, навіть маючи ці відомості про шифр, визначити початковий текст, який має таку відповідність: $q \notin \{ q_i \}$ [20].

У цьому випадку правильно буде стверджувати, що блочний шифр є окремим випадком моноалфавітної підстановки, причому його алфавіт можна записати так:

$$Z_2^N = Z_{2,N}. \quad (2)$$

П[K] – ця підмножина є підмножиною симетричної групи $SYM(Z_{2,N})$ і ключовою системою блочних шифрів. Її індексація відбувається за допомогою параметра $k \in K$, де k є ключем, а K – простір ключів.

Математичним записом П[K] є вираз

$$П[K] = \{\pi\{k\} : k \in K\}. \quad (3)$$

Використовуючи принцип побудови таблиці при N = 5, розглянемо інший випадок. Нехай N = 64 і в такому разі кожен елемент $SYM(Z_{2,N})$ потенційно може розглядатися як підстановка, так, щоб $K = SYM(Z_{2,N})$.

Таким чином звідси випливає, що

– 2^{64} кількість блоків, розрядність яких – 64, проте атакуючий не має жодної можливості для підтримання каталогу, розмір якого становить $2^{64} \approx 1{,}8 \cdot 10^{19}$ рядків;

– спроба отримати ключ за кількості ключів рівній $(2^{64})!$ неможлива.

Неподільність систем шифрування з блочними шифрами пояснюється тим, що в них наявний алфавіт $Z_{2,64}$, простір ключів $K = SYM(Z_{2,64})$ і найголовніше те, що розмір каталогу частот появи символів для 64-розрядних блоків за умови того, що кількість ключів дорівнює 2^{64} або ж спроба отримати ключ зловмисником, виходить за межі його можливостей. У цей самий час атакуючий стикається з проблемою недостатньої кількості ресурсів, а це обмежує його можливості, тим самим забезпечуючи правильну роботу системи. Ця ситуація дуже схожа на ту, коли зловмисник намагається зробити криптоаналіз текстових даних.

Прикро усвідомлювати той факт, що і порушник і розробник мають однакову проблему. Причини цієї проблеми пояснюють такими факторами їхнього спричинення [16]:

- сам розробник не має можливості створити систему, де він міг би реалізувати $2^{64}!$ підстановок $SYM(Z_{2,64})$;
- атакуючий у свою чергу також не може перебрати всі ключі із цієї групи.

Формулювання вимог до блочного шифру можна записати так [16]:

- N – має мінімально дорівнювати 64, а ще краще бути більше за 64. Це робиться для ускладнення створення каталогу;
- простір ключів повинен бути якомога більшим, щоб виключити можливість його підбору;
- $\pi\{k, p\}: p \rightarrow y = \pi\{k, p\}$ – співвідношення вихідного і шифрованого тексту мають бути складними, щоб не можна було застосувати статистичні або аналітичні методи аналізу, на основі відповідності вихідного тексту або ключа.

Отже, бачимо, що використовуваний криптоалгоритм, за допомогою якого шифруються дані, повинен бути ідеально стійким, а це можна реалізувати тільки, якщо читання вихідних даних можливе за умови перебору всіх варіантів ключів, а доти повідомлення не буде таким, яке можна прочитати.

Якщо звернутися до теорії імовірності, тоді шуканий ключ, буде знайдений з імовірністю 0.5 після того, як буде здійснено перебір половини всіх ключів. У цьому випадку на злам такого криптоалгоритму, довжина ключа якого N, потрібно буде в середньому 2^{N-1} перевірок. Із цього випливає, що стійкість блочного шифру залежить виключно від довжини ключа, і це дає можливість експоненційного зростання стійкості шифру одночасно зі зростанням довжини ключа. І навіть, якщо можна було б припустити, що перебір ключів буде здійснюватися на спеціальній багатопроцесорній системі, то на злам ключа довжиною 128 біт, знадобиться занадто багато часу. Із цього факту випливає, що розшифрування методом лобової атаки стає не раціональним.

Звісно, усе це стосується виключно ідеальних за стійкістю шифрів, які неможливо реалізувати через різноманітні фізичні чинники [18].

Використання шифрування сигналів для пристроїв введення даних. Нині існує безліч пристроїв дистанційного введення даних. Під приладом дистанційного введення даних мається на увазі – пристрій бездротової передачі введених даних (ПБПВД) до обчислювальної машини. Прикладом таких приладів є: бездротові клавіатури, або миші, бездротова гарнітура, пристрої сенсорного введення даних тощо.

Пристрої ПБПВД передають інформацію за допомогою радіохвиль частотою від 27 MHz до 2.4 GHz. ПБПВД виконують свою функцію за допомогою двох приладів: передавача та приймача [22, 23].

Основною проблемою пристроїв, які передають інформацію на частоті 2.4 GHz є те, що немає єдиного стандарту щодо захисту інформації, яка передається.

У разі підключення таких пристроїв як бездротова комп'ютерна миша, автентифікація пристрою не використовується, що може призвести до перехоплення управління курсором.

У випадку бездротової клавіатури у деяких моделях використовується шифрування сигналів. Однак у більшості випадків захисту сигналів бездротових пристроїв не надається значної уваги. Відтак, наприклад, шифрування сигналів комп'ютерної миші, зазвичай не використовується, шифрування сигналів клавіатури також не проводиться. Завдяки чому зловмисники мають змогу перехопити сигнали, що може надати їм таку інформацію: особисті дані; дані банківських карт; логіни та паролі облікових записів; зміст листів особистого характеру; дані про стан здоров'я (під час онлайн консультацій лікарів, або ведення медичних карток онлайн); дані про фінансовий стан; дані про політичні вподобання; дані про короткострокові та довгострокові плани; інформацію про наукові розробки.

Навіть у разі шифрування сигналів клавіатури, отримання даних усе ще можливо. Прикладом методу отримання даних є MouseJack. Перед цією атакою не зможуть встояти товари навіть таких корпорацій-гігантів як Dell, Logitech, Microsoft, HP, Amazon, Gigabyte та Lenovo [24]. Ця атака може здійснюватися на відстанях до 100 м, а все, що потрібно мати зловмиснику, це USB-dongle [24–27].

Суть цієї атаки така: і бездротова клавіатура, і бездротова миша використовують два прилади для передавання сигналів (приймач та передавач) у ролі приймача виступає USB-dongle. Деякі моделі клавіатур шифрують сигнали, але комп'ютерні миші найчастіше цього не роблять.

У випадку з клавіатурами це працює таким чином [24]: ключ шифрування має лише USB-dongle, тобто тільки він має можливість розшифрувати сигнал, що несе в собі інформацію про введені клавіші, зловмисник, навіть якщо перехопить цей сигнал, то розшифрувати його не зможе.

На рис. 7 показано схему роботи 1–3 фаз указаної атаки.

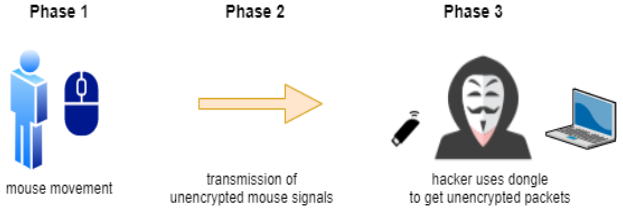

Рис. 7. Атака MouseJack (1–3 фази)

У ході перших трьох фаз відбувається таке: користувач задає зміну (x, y) координат положення миші, у свою чергу передавач, що міститься в миші, передає сигнал до USB-dongle, не шифруючи його, за допомогою радіосигналів. Зловмисник, використовуючи власний, налаштований USB-dongle, перехоплює незашифровані сигнали.

На рис. 8 зображено 4–6 фази атаки MouseJack [24].

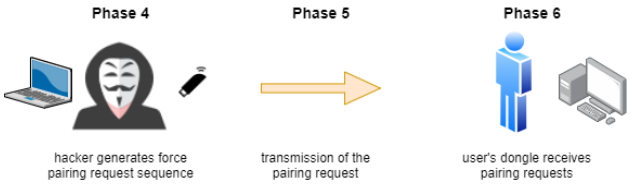

Рис. 8. Атака MouseJack (4–6 фази).

Виконуючи 4–6 фази, зловмисник надсилає послідовність запитів на підключення до USB-dongle користувача, у свою чергу USB-dongle користувача отримує послідовність цих запитів і під'єднується до пристрою користувача [24].

На рис. 9 зображено 7–9 фази атаки MouseJack.

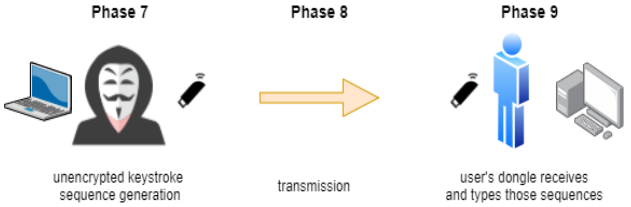

Рис. 9. Атака MouseJack (7–9 фази)

Під час виконання 7–9 фази зловмисник надсилає послідовність символів на комп'ютер користувача. Після виконання всіх зазначених фаз зловмисник має значні можливості маніпулювання над комп'ютером користувача [24].

Використання цієї вразливості можливе на всіх операційних системах, оскільки ця вразливість не відноситься до вразливостей приймача.

Застосовуючи дану вразливість, зловмисник має змогу встановити зловмисне програмне забезпечення, отримати доступ до даних комп'ютера, видаляти дані, порушувати їхню цілісність або доступність.

Отже способом захисту від цієї вразливості є шифрування сигналів ПБПВД, використовуючи надійні алгоритми шифрування, такі як розглянутий вище алгоритм AES. Слід установити однозначну ідентифікацію пристроїв, що намагаються відправляти пакети до USB-dongle.

Недоліком використання шифрування для сигналів ПБПВД є збільшення часу відгуку, тобто часу між уведенням даних користувачем та їхнім відображенням, а також зростання ціни приладів.

5. ВИСНОВКИ

Захист даних – першочергова справа для професіоналів у сфері інформаційної та кібербезпеки. Серед різноманіття атак і спроб вилучити конфіденційну інформацію, фахівцям усе важче досягати ефективного захисту критично важливої інформації. Не полегшують ситуацію і нові технології, які створені з одного боку для покращення функцій захисту, а з іншого – нею так само користуються і порушники, намагаючись зазіхнути на конфіденційність, цілісність і доступність даних у системі.

Ця стаття написана для ознайомлення з методами перехоплення та ранжуванням інформації під час введення її з пристроїв бездротового введення даних.

У роботі дано загальну характеристику алгоритму шифрування, як засобу захисту інформації. Прописано найбільш розповсюджені види шифрувань і відомості про них. Наведено приклади застосування таких методів під час захисту даних.

Ця робота описує симетричні алгоритми шифрування, а саме алгоритм AES, як найбільш широко застосованого алгоритму на теперішній час. Прописано його переваги, недоліки та сферу застосування.

Для порівняння розглянуто блочний алгоритм шифрування та побудовано його математичну модель. У цій частині роботи алгоритм розглядається як такий, що має певні переваги, а саме надійність. Проте він незначно поступається швидкості реалізації порівняно з методом поточного шифрування даних.

Висвітлення проблематики наукової роботи чітко розкриває суть необхідності застосування шифрування під час використання пристроїв дистанційного введення даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Dan Boneh, Victor Shoup, A Graduate Course in Applied Cryptography, version 0.4, Stanford University, September 2017.

[2] Mohamed Barakat, Christian Eder. An Introduction to Cryptography, September 20, 2018.

[3] Steven D Galbraith, Mathematics of Public Key Cryptography, version 2.0,

[4] William Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, November 16, 2005/

[5] Information on https://www.pvsm.ru/algoritmy/225093#begin.

[6] Information on https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84 %D1%83 %D0%BD%D0%BA%D1%86%D0%B8%D1%8F.
[7] Joseph Sterling Grah, Hash Functions In Cryptography, The University of Bergen, June 1, 2008.
[8] Information on https://www.binance.vision /security/what-is-symmetric-key-cryptography.
[9] Nigel Smart, Cryptography: An Introduction, 3rd edition, Mcgraw-Hill College, December 30, 2004.
[10] Information on https://en.wikipedia.org/wiki /Symmetric-key_algorithm.
[11] Christof Paar, Jan Pelzl, Understanding Cryptography, Springer-Verlag Berlin Heidelberg, 2010
[12] Joan Daemen, Vincent Rijmen, AES Proposal: Rijndael, October 1999.
[13] Joan Daemen, Vincent Rijmen, The Design of Rijndael, Springer-Verlag, November 26, 2001.
[14] Information on https://ru.wikipedia.org/wiki/%D0%9F%D1%80%84%D1%81%D0%B0.
[15] Information on https://dic.academic.ru/dic.nsf /ruwiki/12112.
[16] А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин, Криптографическая защита информации. Издательство ТГТУ, 2016.
[17] Information on https://studref.com/403682 /informatika/blochnye_shifry.
[18] Roberto Avanzi, A Salad of Block Ciphers, Munich, August 1, 2017.
[19] Bruce Schneier, A self-study course in block-cipher cryptanalysis, Cryptologia, January 2000.
[20] Information on https://sites.google.com/site/ anisimovkhv/learning/kripto/lecture/tema4.
[21] Lars R. KnudsenMatthew J.B. Robshaw, The Block Cipher Companion, Springer-Verlag Berlin Heidelberg, 2011.
[22] Information on https://techspirited.com/how-does-wireless-keyboard-mouse-work
[23] Information on https://compfonyk.com/kak-rabotaet-besprovodnaya-klaviatura-dlya-kompyutera/
[24] Information on https://xakep.ru/2016/02/25/ mousejack/
[25] Information on https://www.securitylab.ru/ news/381480.php
[26] Information on https://www.mousejack.com/faq
[27] Information on https://ru.wikipedia.org/ wiki/%D0%AD%D0%BB%D1%8E%D1%87

Стаття надійшла до редколегії 11.11.2020

Use of symmetric encryption algorithms for signal transmission in wireless data input devices

Today, there are many computer systems that are designed to improve, facilitate and improve human life. As more and more researchers become interested in information processing, the development of computer systems is gaining momentum every year. With the development of information systems, possible threats, such as breaches of confidentiality, integrity and availability of processed information, are developing at an equally rapid pace. In order to prevent possible losses, the latest information security systems are constantly updated and improved. Since it is impossible to create a completely secure system, there is always the possibility of data theft, so the problem of protection of information and telecommunications systems is becoming increasingly important. Given that no protection can be perfect, a way has been developed to significantly reduce data breaches. Today, cryptosystems are mostly used to protect information and telecommunications systems and other technologies, including the protection of critical information of the state, enterprise, person or other critical data, including corporate secrets, intelligence or trade secrets.This article presents ways to use symmetric algorithms for signal transmission in remote data input devices. Information on existing algorithms of encryption and use of hash functions is given. A distinction is made between single-key and two-key methods of information encryption. The AES algorithm of its function, work of rounds, schemes of data encryption are considered in detail. The description of each algorithm is accompanied by an example which explains the features of their use. A mathematical model and an example of a block encryption algorithm are presented. The principles of operation of wireless devices are highlighted. Vulnerabilities related to wireless devices are considered and solutions for their protection are proposed.

Keywords: *cryptography, encryption, symmetric encryption, block encryption, signal encryption, wireless data entry devices.*

Сергій Толюпа,
доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Serhii Toliupa,
Doctor of Technical Sciences, Professor, Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

Володимир Сайко,
доктор технічних наук, професор, професор кафедри прикладних інформаційних систем Київського національного університету імені Тараса Шевченка.

Volodymyr Saiko,
Doctor of Technical Sciences, Professor, Professor of the Department of Applied Information Systems, Taras Shevchenko National University of Kyiv.

Володимир Наконечний,
доктор технічних наук, старший науковий співробітник, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Volodymyr Nakonechnyi,
Doctor of Technical Sciences, Senior Research Fellow, Professor of the Department of Cybersecurity and Information Protection, Taras Shevchenko National University of Kyiv.

Максим Котов,
студент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Maxim Kotov,
student of the Department of Cyber Security and Information Protection of Taras Shevchenko National University of Kyiv.

Валерія Солодовник,
студентка кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Valeria Solodovnik,
student of the Department of Cyber Security and Information Protection of Taras Shevchenko National University of Kyiv.