Харченко М.М.,

студентка 5 курсу
фізико-математичного факультету
Науковий керівник: Вакалюк Т.А.
кандидат педагогічних наук, доцент кафедри
прикладної математики та інформатики
Житомирський державний університет імені Івана Франка

МЕТОДИ ШИФРУВАННЯ ДАНИХ

Інформаційна безпека стала дуже важливим аспектом сучасних систем зв'язку. Необхідність використання глобальної мережі Інтернет як середовища зв'язку між територіально віддаленими користувачами комп'ютерних систем створює постійний ризик для користувачів стати жертвами крадіжки переданих повідомлень. У цьому випадку шифрування повідомлень стає невід'ємною частиною концепції безпечного зв'язку. Для перетворення (шифрування) зазвичай використовується деякий алгоритм чи пристрій, що має реалізацію заданого алгоритму, при чому вони можуть бути відомі широкому колу осіб. Наприклад, геш-функція MD2 використовується в стандартах захисту електронної пошти. Загальна модель управління процесом шифрування здійснюється за допомогою періодичної зміни ключа шифрування, який забезпечує кожного разу оригінальне представлення інформації при використанні одного й того ж алгоритму або пристрою [1]. Втім, накопичений досвід використання загальновживаних алгоритмів шифрування підвищує кваліфікацію зловмисників, які полюють на корпоративну інформацію з метою або порушення її конфіденційності, або цілісності, або доступності. Тому актуальним є створення нових або модифікація існуючих алгоритмів шифрування з метою підвищення криптостійкості таких алгоритмів, але з обов'язковою умовою збереження їх швидкодії.

Процес шифрування передбачає узгодження ключа між користувачами і використання його в процесі обміну та шифрування даних [2]. Технічна особливість шифрування така, що зловмисник, не маючи унікального ключа, який використовувався користувачами, не зможе отримати миттєвий доступ до інформації.

Шифрування буває симетричним і асиметричним. Кожне з них має свої переваги та недоліки.

У ході симетричного шифрування використовується лише один ключ, заздалегідь відомий двом користувачам. Перевагою даного виду шифрування є те, що швидкість створення зашифрованого документу та його відкриття займає небагато часу, а ось недоліком є те що, симетричне шифрування передбачає використання захищеного каналу зв'язку для передачі ключа між користувачами.

При асиметричному шифруванні використовуються два ключі – відкритий і секретний. Відкритий ключ використовується для зашифровки повідомлення, а для розшифровки – секретний. Асиметричне шифрування має перевагу в тому, що використовується два ключа в загальному вигляді схеми, а це створює достатньо надійний захист інформації. Але недоліком цього виду шифрування є низька швидкодія через складну реалізацію та велику кількість обчислень. Тому проблема забезпечення високої швидкодії алгоритмів шифрування пояснює більшу поширеність симетричних алгоритмів. Фактично, асиметричні алгоритми використовуються лише для передачі ключів шифрування, які потім використовуються у симетричному шифруванні. Однак, блокові симетричні шифри, які забезпечують високий рівень стійкості, є надлишково складними в реалізації, тому доцільно їх полегшення шляхом зменшення складності криптографічних перетворень. Підвищена таким чином швидкодія шифрування надає змогу використовувати малопотужні засоби (переносні комунікатори) для поточного обміну повідомленнями між співробітниками однієї організації [3].

Дослідження сучасних вчених-криптографів свідчать, що при збереженні потрібного рівня криптостійкості можливо використовувати спрощені алгоритми, що забезпечить підвищення швидкості шифрування [4; 5]. Тому у багатьох сучасних методах шифрування застосовуються прості логічні операції (наприклад, XOR), і потреби в більш витончених алгоритмах не виникає, оскільки XOR вже забезпечує абсолютну стійкість. Зрозуміло, що це можливо тільки в тому випадку, якщо виконуються три необхідні й достатні умови стійкого ключа, сформульовані Клодом Шенноном [6].

Розглянемо позитивні та негативні сторони існуючого програмного забезпечення (ПЗ), яке має реалізацію захисту від злому під час обміну повідомленнями між користувачами. Одним з найбільш популярних є анонімний мессенджер Tor Messenger, котрий забезпечує анонімність співрозмовників шляхом пропускання всього Інтернет-трафіку через ланцюг 3400 проміжних серверів [7]. Крім того, існує близько тисячі неофіційних вузлів, адреси яких тримаються в таємниці. Їх вкрай важко відстежити, тому що всередині Tor їх справжні IP-адреси маскуються.

Зважаючи на вищенаведене, розширюється перелік країн – Білорусія, Китай, Росія, Україна та ін., – в яких на законодавчому рівні розглядається заборона використання споживачами телекомунікаційних послуг анонімайзерів, використання неіснуючих мережеві ідентифікаторів або

таких, що належать іншим особам. Така заборона пов'язана не тільки з цензурою, а й з можливістю використання ідентифікаторів споживачів, хто вступив до таких анонімних мереж, з метою, не узгодженою з самими споживачами та проти їх волі [8–10].

За останні два роки дуже швидко набрав популярності мессенджер під назвою Viber. Дане ПЗ працює на ПК-платформах (Windows, Unix-подібні ОС), а також може бути встановлено на портативний пристрій, наприклад, смартфон з ОС Android, iOS, BlackBerry, Symbian або S40 [13]. Слабким місцем в реалізації Viber є те, що розмови зберігаються на загальному сервері в незашифрованому вигляді, – так стверджують експерти [13]. Історія розмов користувачів Viber на ОС Windows зберігається два тижні в загальнодоступному місці, до якого може звернутися будь-який користувач.

Як говорять експерти, їм вдалося перехопити трафік на комп'ютерах з ОС Windows 7 й дізнатися адреси посилань, за якими можна звернутися й отримати усі дані, якими користувачі обмінювались під час розмови. Тому використання Viber, під час ділових чи конфіденційних розмов також неприпустиме, як і використання Skype, оскільки це ставить під загрозу комерційні таємниці фірми [13].

Особливу увагу необхідно приділити захисту інформації, що передається відкритими каналами зв'язку через Інтернет. Зважаючи на те, що кожна фірма надає перевагу власному ПЗ (або створеному на замовлення ПЗ особисто для фірми) для внутрішніх розмов ніж загальновживаному, за мету роботи була поставлена розробка модифікованого блочного метода шифрування каналу зв'язку, який би забезпечив конфіденційні перемовини між двома користувачами мережі, та створення програми-мессенджера, яка б здійснювала захищений чат з використанням цього методу. За прототип було взято відому програму Skype, про яку йшла мова вище.

Як заявляє сама компанія Skype, її системи використовують алгоритм шифрування RSA для обміну ключами і 256-ти бітовий AES для масової кодування. Однак Skype не публікує ні свої ключові алгоритми обміну, ні свій мережевий протокол, і, незважаючи на постійні запити, відмовляється розкрити принцип, що лежить в основі ідентифікаційної системи своїх сертифікатів, або здійснення шифрування [13]. Тому можна зробити припущення, що всередині реалізація алгоритмів шифрування даних є досить великою й знаходиться на віддаленому сервері, тому за основу необхідно було взяти простий алгоритм, який задовольнить вимогам швидкого шифрування й розшифрування тексту. Найпростішим і одним із найефективніших (при внесенні до реалізації відповідних модифікацій використанні) є алгоритм шифрування з використанням простої логічної функції XOR [13]. Тому було прийнята спроба реалізувати алгоритм з використанням XOR й розглянути усі його переваги та недоліки, щоб зрозуміти, наскільки є захищеним канал зв'язку з таким шифруванням.

Ідея була покладена на «клієнт-серверну» технологію зі створенням чату, який має відповідну модифікацію з шифруванням повідомлення відповідною геш-функцією, заснованою на операції XOR.

При дотриманні перерахованих умов, які зазначив Клод Шеннон для абсолютно стійкого алгоритму шифрування [6], для злому алгоритму шифрування XOR необхідно буде витратити досить багато часу. Хоча, звичайно, замість XOR тут можна використовувати і який небудь інший алгоритм. Але оскільки XOR є одним із найшвидших (обчислювально ефективних алгоритмів), це дає можливість без затримок швидко отримувати й розшифровувати інформацію, яка надходить до отримувача. Таке застосування можна реалізовувати не тільки при створенні мессенджера, а й наприклад при шифруванні даних для БПЛА, де важлива швидкість отримання вказівок щодо траєкторії переміщення апарату.

Шифрування повідомлення. Для реалізації шифрування повідомлень, з забезпеченням захисту від підрахунку збігу індексів, необхідно було реалізувати гешфункцію. На цьому етапі розробки ПЗ, реалізуємо геш-функцію, а саме беручи за основу операцію XOR шифрування. Алгоритм, схожий на AES, реалізовується досить просто. Крім того, одна функція виконує як шифрування, так і дешифрування, що впливає на швидкість обміну та використання алгоритмів шифрування повідомлень. Результатом створення даної функції стало те, що її застосування приходиться на частину числового ключа. Тобто ми генеруємо числовий ключ, як і раніше, але після ініціалізуємо геш-функцію з 32-бітними константами. Після ініціалізації виконуємо комбінування значень кожного символу ключа з цими константами, яких чотири. Наступним кроком є те що, ми організовуємо шифрування використовуючи операцію XOR, як і раніше але шифруємо циклічно кожну літеру повідомлення відповідною константою геш-функції.

У результаті внесення до алгоритму шифрування деякої геш-функції ми отримали те, що метод, який раніше визначав, на якій мові написано повідомлення, вже не спрацьовує, а якщо спрацьовує, – то кожного разу помиляється з визначенням мови та приблизною довжиною ключа.

Як видно з результатів експерименту застосування методів злому, які були запропоновані й віднайдені в мережі [13], навіть метод підрахунку збігів визначає мову неправильно.

Під час виконання роботи було розглянуто криптостійкість алгоритмів та механізмів шифрування даних в таких відомих програмах, як Tor, Skype та Viber. Також було проведено аналіз на стійкість до злому криптосистеми, яка базується на алгоритмі швидкого шифрування XOR. За результатами досліджень був запропонований новий модифікований блочний метод шифрування з використанням операції XOR. Розроблений метод було покладено в основу створення корпоративного мессенджера з шифруванням повідомлень, який забезпечує захищене спілкування засобами чату як між співробітниками в локальній мережі, так і для обміну

повідомленнями між територіально розосередженими філіями одної корпорації. Програма є кросплатформеною, протестована під керуванням ОС Linux Mint 16 Petra, Ubuntu, Windows 7 Ultimate x64, має також реалізацію під розрядність x32. Створений мессенджер (на відміну від загальновживаних програм Skype, ICQ, Tor Massenger й т. п.) не залишає даних про розмову в мережі Інтернет за рахунок встановлення прямого зв'язку між двома користувачами без проміжних серверів, які могли б зберігати дані та історію перемовин.

Список використаних джерел:

1. Горбенко, І. Д. Захист інформації в інформаційно-телекомунікаційних системах / І. Д. Горбенко, Т. О. Гріненко. Харків : ХНУРЕ, 2004. – 222 с.
2. Криптография и безопасность сетей : [учеб. пособие] / Б. А. Фороузан ; пер. с англ. под ред. А. Н. Берлина. – М. :Интернет-ун-т информ. технологий ; БИНОМ. Лаборатория знаний, 2010. – 784 с.
3. Горбенко І. Д. Аналіз блокових симетричних шифрів міжнародного стандарту ISO/IEC 29192-2 / І. Д. Горбенко, А. В. Самойлова // Прикладная радиоэлектроника (Харьк. нац. ун-т радиоэлектроники). – 2013. – Том 12 – № 2. – С. 247–249.
4. Лужецький В. А. Блоковий шифр на основі псевдовипадкової послідовності криптопримітивів / В. А. Лужецький, А. В. Остапенко // Системи обробки інформації : зб. наук. пр. – 2010. – Вип. 3(84). – С. 136.
5. Sravan Kumar D. A Block Cipher Using Rotation and Logical XOR Operations / D. Sravan Kumar, CH. Suneetha, and A. Chandrasekhar // IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011, pp. 142–147.
6. Шеннон К. Работы по теории информации и кибернетике / пер. с англ. – М. : Изд-во иностранной литературы, 1963. – 830 с.
7. Создатели сети Tor выпустили анонимный мессенджер [Электронный ресурс] // Интернет-газета «Вести». – 2015. – 30 окт. – Режим доступа : http://hitech.vesti.ru/news/view/id/7984. – Загл. с экрана.
8. Разбор полётов: Кто его раздевает, тот слёзы проливает [Электронный ресурс] // TJournal – новое медиа. – 2015. – 7 февр. – Режим доступа : https://tjournal.ru/p/unblockable-tor. – Загл. с экрана.
9. Правила надання та отримання телекомунікаційних послуг : затв. постановою Кабінету Міністрів України від 11 квітня 2012 р. № 295 [Електронний ресурс] // Офіційний веб-портал Верховної Ради України. – Режим доступа : http://zakon4.rada.gov.ua/laws/show/295-2012-%D0%BF. – Загол. з екрана.
10. Передача голоса по IP-протоколу и безопасность программы Skype [Электронный ресурс] / С. Л. Гарфинкель // Независимый информационный ресурс. – Режим доступа : http://www.skypeclub.ru/skype_security.htm. – Загл. с экрана.

11. Приложение Viber: описание, возможности [Электронный ресурс] // Официальный сайт компании Viber Media. – Режим доступа : http://www.viber.com/ru/about. – Загл. с экрана.

12. Viber не использует шифрование для защиты данных [Электронный ресурс] // Информационный портал по безопасности. – 2014. – 25 апр. – Режим доступа : http://www.securitylab.ru/news/452203.php. – Загл. с экрана.

13. «Одинаково не доверяю всем мессенджерам»: эксперты о конфиденциальности приложений для общения [Электронный ресурс] / В. Волков // Портал о цифровой реальности. – 2015. – 21 апр. – Режим доступа : https://digital.report/imconfidential-experts/. – Загл. с экрана.