УДК 004.056.55

Журавська І. М.,
канд. техн. наук, доцент кафедри інформаційних технологій і програмних систем, ЧДУ ім. Петра Могили, м. Миколаїв, Україна
Румянков Д. І.,
бакалаврант кафедри інтелектуальних інформаційних систем, ЧДУ ім. Петра Могили, м. Миколаїв, Україна

СТВОРЕННЯ МОДИФІКОВАНОГО БЛОЧНОГО МЕТОДУ ШИФРУВАННЯ НА БАЗІ ОПЕРАЦІЇ XOR ДЛЯ КОРПОРАТИВНОГО МЕССЕНДЖЕРА

У статті досліджено проблему створення модифікованого блочного методу шифрування повідомлень між співробітниками віддалених філій корпорації.

Актуальність роботи полягає в тому, що 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 стало невід'ємною частиною безпечного зв'язку.

У роботі пропонується модифікований блочний метод шифрування переданих повідомлень із використанням операції XOR. Описаний метод реалізований у програмному забезпеченні корпоративного мессенджера для співробітників територіально віддалених філій.

У процесі створення модифікованого методу шифрування використовується математичний апарат теорії інформації, систем числення, методів дискретної математики. Розробка логічних функцій, придатних для криптографічного перекодування інформації згідно з запропонованим підходом, базується на положеннях теорії логіки, криптографії.

Практичне значення роботи полягає в забезпеченні конфіденційного спілкування засобами чату співробітників віддалених філій корпорації без використання проміжних серверів, на яких існує загроза збереження та розшифрування перемовин.

Ключові слова: *блочний метод шифрування; операція XOR; корпоративний мессенджер*

Постановка проблеми

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.

Аналіз останніх досліджень і публікацій

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 одної 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 якості та вразливості існуючого програмного забезпечення (ПЗ), яке має реалізацію захисту від злому під час обміну повідомленнями між користувачами.

Одним з найбільш популярних є анонімний месенджер 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.

Створення мережі Tor почалося у 90-х роках минулого століття в дослідній лабораторії ВМС США, які до недавнього часу були активним спонсором проекту [8].

Але якщо розглянути дане ПЗ з точки зору законодавства, то тут є дуже багато речей, які необхідно мати на увазі. Так як Tor належав ВМС США, то виникає питання, а чи не є ці таємні адреси неофіційних сайтів власністю самих ВМС США? Звичайно, кожний розробник має усі відомості про архітектуру, знає про всі недоліки системи, навіть недоліки, які були закладені навмисно, а так як Tor – це механізм анонімайзера, тому ці дії можуть бути цілком непомітними й виконуватися віддалено іншими обчислювальними пристроями з прихованою від задіяних користувачів метою.

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].

Розглянемо таке усім відоме ПЗ, як Skype. Воно дозволяє кожному користувачу, який має встановлену програму та сторінку користувача, розмовляти, створювати конференції, а також передавати інформацію. Проаналізуємо, яку модель захисту інформації має Skype.

Прослухати Skype шляхом аналізу трафіку досить непросто за причини:

– протокол Skype має розподілену структуру (як, наприклад, той же BitTorrent);

– трафік пересилається в зашифрованому вигляді.

Але після того, як у 2011 р. цей VoIP-мессенджер купила корпорація Microsoft, було впроваджено багато функцій, які більш тісно прив'язують додаток до центральних серверів, і тому сьогодні вже говорити, що Skype – це в чистому вигляді розподілений протокол, не можна. Це теоретично спрощує аналіз трафіку, але на практиці це не дуже сильно допомагає саме прослуховувати Skype [11].

Здійснити перехоплення можна ще до того моменту, як дані стануть зашифрованими – для цього потрібно перехоплювати їх не в мережі, а на самому комп'ютері користувача. Звукові дані можна перехоплювати безпосередньо з мікрофона, текст – з клавіатури, а файли, знаючи їх назви, і зовсім отримати не складає труднощів. У стандартній для Windows програмі звукозапису є можливість вибрати в якості вхідного каналу «Stereo Mixer», який приймає всі звуки з мікрофона. Перехопити натискання на клавіатурі може який-небудь простий «клавіатурний шпигун» (keylogger) програмний або апаратний.

Тому роботодавці забороняють вести виробниче спілкування через Skype, щоб співробітники не розголошували комерційні таємниці корпорації

Також необхідно зазначити, що після того, як компанія Microsoft придбала Skype, вона обладнала клієнт Skype технологією законного прослуховування [12]. Тепер будь-якого абонента можна перемкнути на спеціальний режим, за якого ключі шифрування, які раніше генерувалися на телефоні чи комп'ютері абонента, будуть генеруватися на сервері. А отримавши доступ до сервера, можна прослуховувати розмови та

читати листування. Microsoft надає можливість користуватися цією технологією спецслужбам по усьому світу.

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 [14]. 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 [15].

Постановка завдання

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 перемовин 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 у попередньому розділі.

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 [15].

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 [15]. 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.

Виклад основного матеріалу

Метод злому алгоритму шифрування XOR. Оскільки XOR-шифрування – це симетричний алгоритм, то відкритий текст піддається операції «виключення або» разом з ключовим текстом для отримання шифротексту. Повторне застосування операції XOR відновлює оригінал для шифрування і дешифрування використовується одна і та ж функція.

Справжньою безпеки тут ніколи не було. Цей тип шифрування легко зламується, навіть без комп'ютера. Його злом на комп'ютері займає кілька секунд. Припустимо, що відкритий текст використовує англійську мову. Більш того, нехай довжина ключа будь невелике число байт. Нижче описано, як зламати цей шифр [16]:

1. Визначаємо довжину ключа за допомогою процедури, відомої як підрахунок збігів. Застосуємо операцію XOR до шифротексту, використовуючи як ключ сам шифротекст з різними зсувами, і підрахуємо співпадаючі байти. Якщо величина зсуву кратна довжині ключа, то співпаде понад 6 відсотків байтів. Якщо ні, то будуть збігатися менше ніж 0.4 відсотка (вважаючи, що звичайний ASCII текст кодується випадковим ключем, для інших типів відкритих текстів числа будуть іншими). Це називається показником збігів. Мінімальне зміщення від одного значення, кратного довжині ключа, до іншого і є довжина ключа.

2. Зміщуємо шифротекст на цю довжину і проведемо операцію XOR для зміщеного і оригінального шифротекст. Результатом операції буде видалення ключа та отримання відкритого тексту, підданого операції XOR з самим собою, зміщеним на довжину ключа. Оскільки в англійській мові на один байт доводиться 1,3 біта дійсної інформації, існуюча значна надмірність дозволяє визначити спосіб шифрування. Незважаючи на це, велика кількість постачальників ПЗ все ще нав'язують цей алгоритм у якості «майже такого ж безпечного як DES», вражає. Саме цей алгоритм (з 160-бітовим повторюваним ключем) National Security Agency (NSA) США зрештою дозволила використовувати в цифрових телефонних стільникових мережах для закриття голосу [17].

Тепер розглянемо алгоритм підрахунку «індексу збігу» [18].

Розглянемо текст, написаний на деякій мові. Алфавіт цієї мови будемо вважати що складається з *m* літер. Розглянемо досить довгий рядок $\vec{x}$ з *n* літер. Якщо f_i задає кількість *i*-ї літери алфавіту в рядку $\vec{x}$, то можна визначити індекс збігів як ймовірність збігу двох довільних букв в рядку:

$$I(\vec{x}) = \sum_i f_i \frac{f_i - 1}{n(n-1)}, \quad (1)$$

де *n* – кількість літер в повідомленні;

f_i – функція яка відображає закономірність повтору літери з індексом і в повідомленні.

Звідки при досить великих і визначенні як отримати наближену формулу індексу збігу:

$$I(\vec{x}) = \sum_i p_i^2, \quad (2)$$

де p_i – сума усіх ймовірностей збігу кожної літери в повідомленні.

Тепер, якщо припустити, що наш текст написаний природною мовою (наприклад, російською або англійською), є досить довгим і його характеристики відповідають відомим нам характеристикам цієї мови, то для нього можна отримати очікуваний індекс збігів (використовуючи відомі частоти появи окремих букв), наведений у табл. 1.

Таблиця1

Індекс збігу при використанні відповідної мови повідомлення

Мова	Індекс збігу
Російська	0,0553
Англійська	0,0644–0,0667
Українська	0,0678–0,0731
Італійська	0,0738
Іспанська	0,0775
Німецька	0,0762
Французька	0,0778

Для роботи методу індексу збігів важливо, що дана характеристика не змінюється, якщо текст мовою зашифрований з використанням моноалфавітного шифру, такого, як наприклад шифр Цезаря. Для випадкового рядку символів алфавіту це значення приблизно дорівнює:

$$I(\vec{x}) \approx \frac{1}{m}, \quad (3)$$

де *m* – кількість літер у відповідному алфавіті.

Тобто, індекс збігу дорівнює 0,03030 для російської мови, для української – 0.02941 (враховуючи апостроф) і відповідно 0,03856 для англійської мови.

Важливою властивістю є те, що індекс збігу для рядка не змінюється при шифруванні цього рядка моноалфавітним шифром.

Метод індексу збігів полягає в наступному [19]. Візьмемо рядок $\vec{y}$ і послідовно циклічно зміщуємо рядок на *m* / 2 позицій, побудуємо нові *m* / 2 – 1 рядків.

Після, знайдемо індекси взаємних збігів між вихідною рядком і кожної отриманої. Максимальний індекс збігів між двома рядками буде відповідати випадку використання однакових шифрів зсуву для відповідних букв, тобто у разі коли розмір зсуву кратний розміру ключового слова шифру Віженера.

Якщо рядок досить довгий (тобто статистика досить точна), то можна порівнювати проміжні значення зі значеннями з табл. 1 для визначення розміру зсуву та подальшої перевірки.

Повернемося до нашого алгоритму злому XOR-шифрування. Після того, як ми визначили довжину ключа, необхідно знайти сам ключ. Для цього виконуємо наступні кроки [17]:

1. Розбиваємо текст на групи символів.
2. Кількість груп дорівнює довжині ключа (Якщо у нас шифротекст «ciphertext» і ключ довжиною 3 символи, то в першу групу потраплять букви c, h, t, t; в другу: i, e, e; а в третю – p, r, x).
3. У кожну групу входять символи, які кодуються і-м символом ключа.
4. У кожній з груп виконуємо бітову операцію XOR із символами з найбільш поширеним в алфавіті символом (для англійської мови це пробіл).
5. Вважаємо частоти кожного отриманого символу серед групи.
6. Вибираємо в якості і-й літери ключа елемент з найбільшою частотою входження.

Ось, слідуючи такому простому алгоритму дій, можна провести злом шифротексту, який був зашифрований за допомогою функції XOR, й дізнатися зміст повідомлення.

Розробка модифікованого алгоритму. Оскільки операція XOR використовує деякий ключ (x), який можна визначити за допомогою підрахунку індексів збігу, тому початковим завданням є необхідність забезпечити непрацездатність використання цього алгоритму для його визначення.

У результаті проведених тестувань з математичними операціями, було прийнято рішення про введення для шифрування всього тексту повідомлення єдиного числового ключа, який утворюється за рахунок символьного (рис. 1).

Алгоритм було реалізовано на мові програмування C++, у середовищі QtCreator. QtCreator було обрано, оскільки він надає можливість кросплатформеності, й тим самим у подальшому можна встановлювати програму на інші операційні системи. Модернізований алгоритм виглядає таким чином:

1. Вводимо значення ключа.
2. Складаємо числовий ключ, кожного разу зміщуючи на один біт, після числового значення символу символьного ключа.
3. Після, виконуємо операцію «^» (XOR) до кожного символу повідомлення.
4. Отримуємо зашифроване повідомлення.

Для порівняння, розглянемо блок-схему створеного алгоритму (див. рис. 1) порівняно з класичним шифруванням операцією XOR (рис. 2).

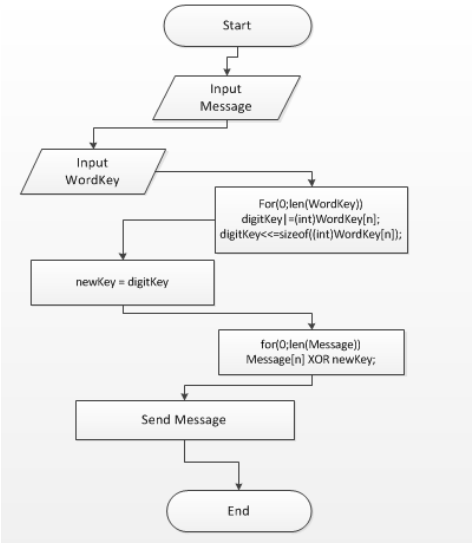

Рис. 1. Модифікований алгоритм шифрування з операцією XOR із застосуванням числового ключа

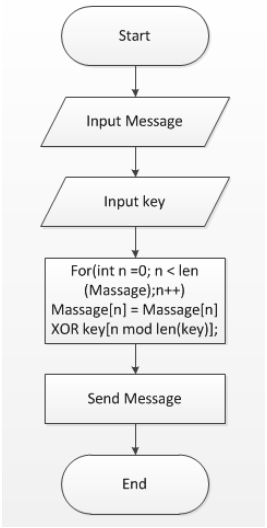

Рис. 2. Класичний алгоритм шифрування з операцією XOR

Тим самим було створено алгоритм функції створення унікального ключа на основі тієї ж операції XOR. Оскільки, вдалося забезпечили захист від описаного попередньо алгоритму злому. Але все ж позбутися того, що в алгоритмі присутня частота повтору відповідних символів, не вдалося, так як це властивість операції XOR. Тому із зазначеного вище алгоритму злому спрацьовує лише обрахування частоти повтору символів, за якою можливо визначити мову, на якій написано повідомлення (рис. 3).

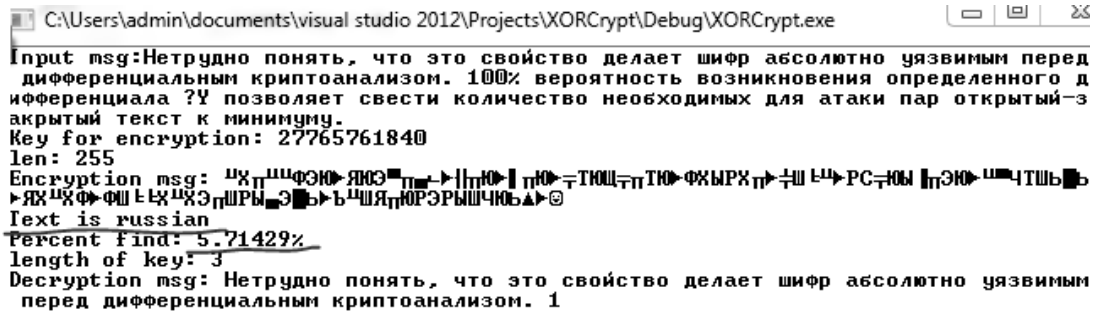

Рис. 3. Результат роботи алгоритму злому

Шифрування повідомлення. Для реалізації шифрування повідомлень, з забезпеченням захисту від підрахунку збігу індексів, необхідно було реалізувати геш-функцію. На цьому етапі розробки ПЗ, реалізуємо геш-функцію, про яку йшла мова в попередніх розділах, а саме беручи за основу операцію XOR-шифрування (рис. 4). 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 (рис. 5).

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 (рис. 6), 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 [19], навіть метод підрахунку збігів визначає мову неправильно.

Реалізація чату між двома ПК. Організацію чату було виконано у виродженій підмережі «точка-точка» в межах локальної мережі одного приміщення/ будинку, а також між ПК, розташованими в різних підмережах, поєднаних через Інтернет (рис. 7).

В останньому випадку користувачі можуть працювати в одній корпорації, філії якої територіально розташовані не тільки у різних містах, а навіть у різних країнах. Для тестування спілкування повідомленнями через мережу Інтернет було реалізовано механізм перенаправлення портів NAT [20] та виконане налаштування відповідних параметрів маршрутизатора фірми TP-Link [21].

Для впровадження запропонованого модифікованого методу шифрування з використанням операції XOR було розроблено програмну архітектуру чату,

розроблений дружній інтерфейс користувача чату (рис. 8).

Дана програма є кросплатформеною, протестована під керуванням ОС Linux Mint 16 Petra, Ubuntu, Windows 7 Ultimate x64, має також реалізацію під розрядність x32.

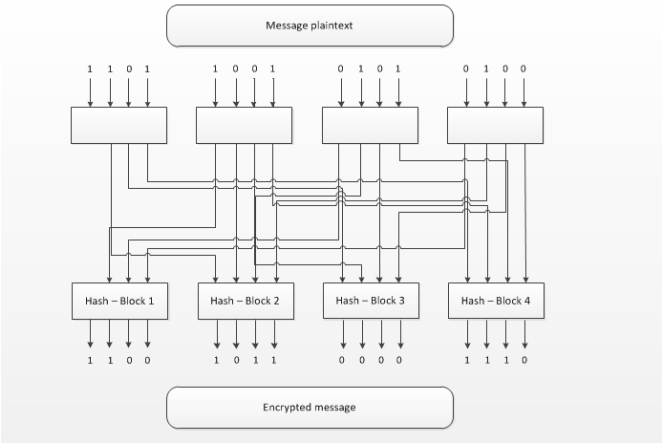

Рис. 4. Реалізація геш-функції на основі блочного алгоритму

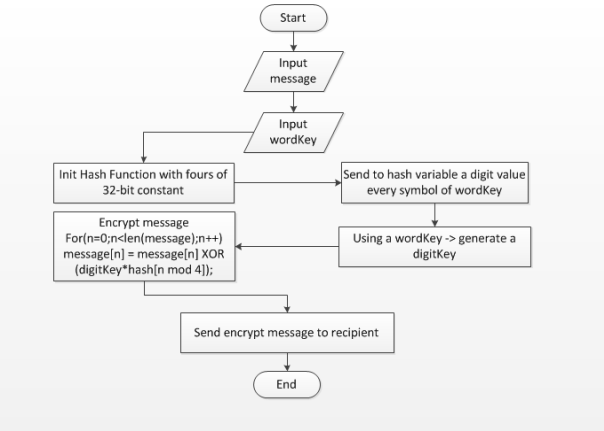

Рис. 5. Модифікований алгоритм шифрування з використанням геш-функції

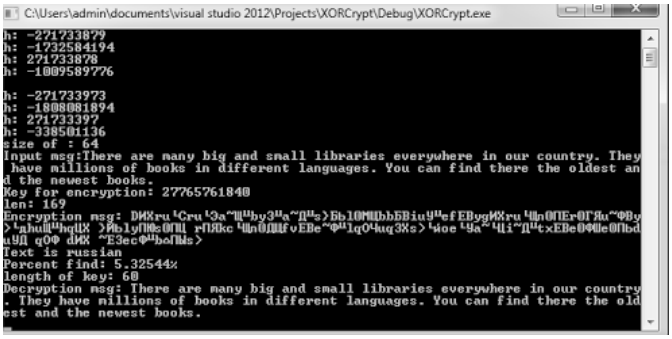

Рис. 6. Результат роботи алгоритму шифрування в поєднанні з операцією XOR та геш-функцією

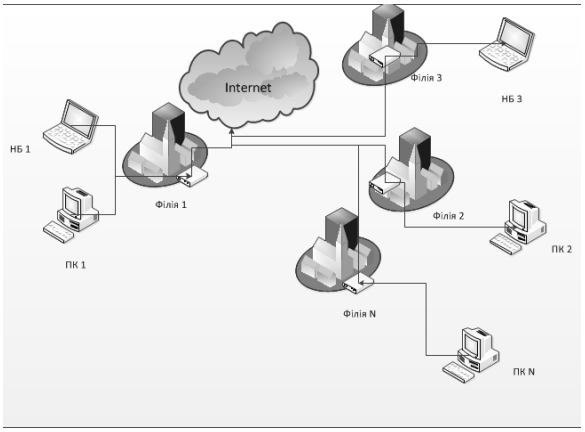

Рис. 8. NetDiagram розгалужених філій корпорації, поєднаних через Інтернет

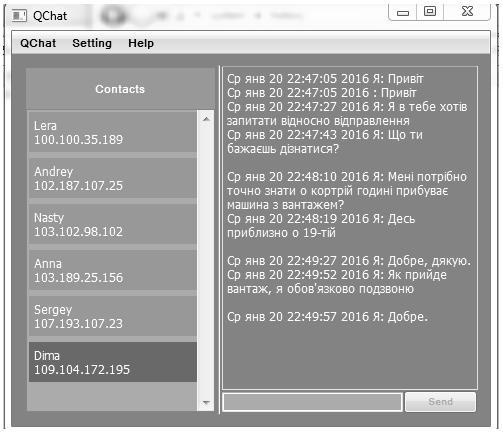

Рис. 9. Інтерфейс корпоративного мессенджера з шифруванням трафіка

Висновки

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.

ЛІТЕРАТУРА

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. Положение о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет : утв. Постановл. оперативно-аналит. центра при Президенте Республики Беларусь и Мин-ва связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 6/8 [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа : http://www.pravo.by/main.aspx?guid=12551&p0=T21503059&p1=1&p5=0. – Загл. с экрана.
10. 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.
11. 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.
12. Російські спецслужби отримали можливість відстежувати розмови у Skype [Електронний ресурс] / М. Костинян // Видання про Інтернет-бізнес в Україні. – 2013. – 15 бер. – Режим доступу : http://watcher.com.ua/2013/03/15/rosiyski-spetssluzhby-otrymaly-mozhlyvist-vidstezhuvaty-rozmovy-u-skype/. – Загол. з екрану.
13. Приложение Viber: описание, возможности [Электронный ресурс] // Официальный сайт компании Viber Media. – Режим доступа : http://www.viber.com/ru/about. – Загл. с экрана.
14. 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.
15. «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/im-confidential-experts/. – Загл. с экрана.
16. Хаггарти Р. Дискретная математика для программистов : [учеб. пособие для вузов] / Р. Хаггарти ; пер. с англ. ; под ред. С. А. Кулешова ; с доп. А. А. Ковалева. – М. : Техносфера, 2003. – 320 с.
17. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / пер. с англ. – М. : Триумф, 2002. – 816 с.
18. Ященко В. В. Введение в криптографию. Новые математические дисциплины : [учебник] / Под общ. ред. В. В. Ященко. – СПб. : Питер, 2001. – 288 с.
19. James M. Stewart, M. Chapple, and D. Gibson, (2015), CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 7th ed., John Wiley & Sons. Inc., Indianapolis, Indiana, 1080 p.
20. Абрамов В. О. Базові технології комп'ютерних мереж : [навч. посібник] / В. О. Абрамов, С. Ю. Клименко ; 2-ге вид. – К. : Видавнича група «А.С.К.», 2013. – 248 с.
21. Проброс портов на роутерах Asus, D-Link, TP-Link, Zyxel [Электронный ресурс] // Портал технических рекомендаций. – Режим доступа : http://pk-help.com/network/port-router-asus-d-link-tp-link-zyxel/. – Загл. с экрана.

Журавская И. Н., Румянков Д. И.,
Черноморский государственный университет им. Петра Могилы, г. Николаев, Украина

Создание модифицированного блочного метода шифрования на базе операции XOR для корпоративного мессенджера

В статье проведено исследование проблемы создания модифицированного блочного метода шифрования сообщений между сотрудниками удаленных филиалов компании.

Актуальность работы заключается в том, что информационная безопасность стала очень важным аспектом современных систем связи. Необходимость использования глобальной сети Интернет как среды

связи между территориально удаленными пользователями компьютерных систем создает постоянный риск для пользователей стать жертвами кражи передаваемых сообщений. В этом случае шифрование сообщений стало неотъемлемой частью безопасной связи.

В работе предлагается модифицированный блочный метод шифрования передаваемых сообщений с использованием операции XOR. Описанный метод реализован в программном обеспечении корпоративного мессенджера для сотрудников территориально удаленных филиалов.

В процессе создания модифицированного метода шифрования используется математический аппарат теории информации, систем счисления, методов дискретной математики. Разработка логических функций, пригодных для криптографического перекодирования информации в соответствии с предложенным подходом, базируется на положениях теории логики, криптографии.

Практическое значение работы состоит в обеспечении конфиденциального общения средствами чата между сотрудниками удаленных филиалов корпорации без использования промежуточных серверов, на которых существует угроза сохранения и расшифровки переговоров.

Ключевые слова: *блочный метод шифрования; операция XOR; корпоративный мессенджер*.

Zhuravska I. M., Rumiankov D. I.,
Petro Mohyla Black Sea State University, Mykolaiv, Ukraine

Creation of the modified block encrypt method based on XOR operation for corporate messenger

The problem of creating a modified block encryption method of messages between remote branch employees of the corporation is reseached in this article.

The relevance of the work is that information security has become a very important aspect of modern communication systems. Need to use for the Internet as a channel of communication between geographically remote users computer system creates a constant risk for users become victims of theft of posts. In this case, encryption of the messages has become an integral part of a secure connection.

The paper proposed a modified block encryption of messages transmitted using the logic operation XOR. This method is implemented in software corporate messenger for staff geographically remote branches.

In the process of creating a modified encryption method used mathematical tools of information theory, number systems, methods of discrete mathematics. Development of logic functions, suitable for cryptographic conversion information in accordance with the proposed approach is based on the theory of logic, cryptography.

The practical significance of the work lies in providing a confidential chat communication means staff remote branch offices of the corporation without intermediate servers, which threatens the preservation and decryption negotiations.

***Key words*:** *block encrypt method; XOR operation; corporate messenger*.

 Дата надходження статті до редколегії 24.11.2015