Дробиш Р.С. магістр, Люта М.В., ст. викладач
Київський національний університет технологій та дизайну

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ ТА ШИФРУВАННЯ ІНФОРМАЦІЇ

Анотація. *В статті розглянуто види шифрування, розглянули відомі блочні шифри та принципи їх роботи.*

Ключові слова: *інформаційна безпека; простий шифр заміни; шифр зсуву; симетричне шифрування; асиметричне шифрування; криптографія.*

Drobysh R., Liuta M.
Kyiv National University of Technologies and Design

ANALYSIS OF EXISTING METHODS OF PROTECTION AND ENCRYPTION OF INFORMATION

Abstract. *The article considers the types of encryption, considered the known block ciphers and the principles of their operation.*

Keywords*: information security; simple replacement cipher; the shift cipher; symmetric encryption; asymmetric encryption, cryptography.*

Вступ. Криптографія в минулому використовувалася лише у військових цілях. Однак зараз, у міру утворення інформаційного суспільства, криптографія стає одним з основних інструментів, що забезпечують конфіденційність, авторизацію, електронні платежі, корпоративну безпеку та безліч інших важливих речей.

Криптографічні методи можуть застосовуватися для вирішення таких проблем безпеки: конфіденційність переданих/збережених даних; автентифікація; цілісності даних, що зберігаються і передаються; забезпечення справжності документів. Також ці методи застосовуються в базових методах перетворення інформації, якими є: шифрування (симетричне та несиметричне); обчислення хеш функцій; генерація електронного цифрового підпису; генерація послідовності псевдовипадкових чисел.

Шифрування – це оборотне перетворення даних з метою їх приховування від сторонніх. Багато методів шифрування використовують ключ шифрування – секретну кодову послідовність, використовувану у процесі перетворення інформації. Методів шифрування було винайдено безліч – від шифрів простої заміни до принципово нерозкривного шифру Вернама (двійкове додавання вихідного тексту з одноразово використовуваною випадковою послідовністю).

Шифр простої заміни – клас методів шифрування, які зводяться до створення за певним алгоритмом таблиці шифрування, в якій для кожної літери відкритого тексту існує єдина зіставлена їй літера шифр-тексту. Саме шифрування полягає у заміні букв згідно таблиці. Для розшифрування достатньо мати ту саму таблицю, або знати алгоритм, за якою вона генерується. До шифрів простої заміни належать багато способів шифрування, що виникли в давнину або середньовіччя, як, наприклад, Атбаш або Шифр Цезаря. Для розкриття таких шифрів використовується частотний криптоаналіз. Зазначимо, що шифр простої заміни не завжди має на увазі заміну літери на якусь іншу літеру. Допускається використовувати заміну літери на цифру.

Шифр Цезаря, також відомий як шифр зсуву – один із найпростіших і найвідоміших методів шифрування. Шифр Цезаря – це вид шифру підстановки, в якому кожен символ у відкритому тексті замінюється символом, що знаходиться на певному постійному чисельності позицій лівіше або правіше за нього в алфавіті. Наприклад, у шифрі зі зрушенням праворуч на 3, А була б замінена на Г, Б стане Д, і так далі. Симетричний метод шифрування полягає в тому, що обидві сторони-учасники обміну даними мають абсолютно однакові ключі для шифрування та розшифрування даних.

Симетричний метод шифрування можна реалізувати з урахуванням різних алгоритмів. Наприклад, часто використовуються алгоритми DES (Data Encryption Standard – стандарт шифрування даних), 3-DES (потрійний DES), RC2, RC4. Сьогодні найнадійнішим симетричним алгоритмом вважається розширений стандарт шифрування AES (Advanced Encryption Standard). Шифр AES передбачає певну кількість повторних циклів зміни коду, у результаті вихідний звичайний текст перетворюється на шифр. Кожен цикл складається з кількох етапів обробки, включаючи той, який залежить від ключа шифрування. Використовуючи той самий ключ шифрування, застосовується набір циклів у зворотній послідовності, щоб перевести шифр у простий текст. Коли сторони вирішують використовувати AES для шифрування даних, одна із сторін генерує пару симетричних ключів. Симетричний ключ є набором випадкових чисел, які задають послідовність зміни даних при шифруванні. Щоразу під час запуску роботи AES шифру генерується унікальна пара симетричних ключів.

Цей метод шифрування підтримує роботу ключів різної довжини – 128 біт, 192 біт, 256 біт і дослідники нещодавно почали говорити про 512-бітові ключі для AES. Логічно припустити, що чим довше значення ключа, тим більше часу знадобиться на його злом, і відповідно тим надійніший шифр. Без відповідного ключа AES-шифр дуже важко зламати. Крім того, цей алгоритм шифрування дуже швидкий, оскільки не потребує більших обчислювальних ресурсів. Але обом учасникам обміну даними потрібно мати за симетричним ключем. Тобто. один із учасників повинен відправити свій симетричний ключ іншому якимось чином. Механізм передачі ключа у відкритому вигляді легко вразливий, оскільки схильний до перехоплення даних. На просторах Інтернету під час передачі ключа може вклинитися якийсь шахрай і серйозно вплинути на обмін даних. Оскільки передавати ключ у відкритому вигляді небезпечно, його передають у зашифрованому вигляді. Для обміну ключами застосовують асиметричне шифрування. Використання разом симетричного та асиметричного методів шифрування даних називається гібридним шифруванням. Метод асиметричного шифрування (або метод відкритого ключа) передбачає використовувати в парі два різні ключі – відкритий та секретний. Відкритий ключ (publickey) вільно поширюється у мережі, тоді як секретний ключ (privatekey) завжди тримається у секреті. У асиметричному шифруванні ключі працюють у парі – якщо дані шифруються відкритим ключем, то розшифрувати їх можна лише відповідним секретним ключем і навпаки – якщо дані шифруються секретним ключем, то розшифрувати їх можна лише відповідним відкритим ключем. Використовувати відкритий ключ із однієї пари та секретний з іншого – неможливо. Кожна пара асиметричних ключів пов'язана з математичними залежностями. Метод асиметричного шифрування реалізують такі алгоритми, як RSA, алгоритм Діффі-Хеллмана (Diffie-Hellman), Elgamal, Rabin та інші. Усі алгоритми асиметричного шифрування базуються на складності розв'язання математичних задач. Наприклад, розкладання дуже великих чисел на співмножники (RSA) або логарифмічні завдання (метод еліптичних кривих). Сьогодні RSA вважається одним із найефективніших алгоритмів асиметричного шифрування. Очевидно, що чим довше ключ, тим вища стійкість має криптосистема.

Шифрування та розшифровування працює так само, як кейс, для якого використовую два ключі: одним кейс закривають, а іншим – відкривають. Асиметричне шифрування дозволяє розв'язати завдання з поширенням ключів (на відміну симетричного шифрування). Ви можете надсилати свій відкритий ключ усім, з ким хочете взаємодіяти, і не використовувати унікальні пари ключів для кожного випадку. Асиметричний шифр може забезпечити аутентифікацію залежно від використання алгоритму. Але асиметричні алгоритми приблизно тисячу разів повільніше, ніж симетричні, так як вони використовують складні математичні обчислення, що потребує

більше обчислювальних ресурсів. Розв'язанням задачі з продуктивністю асиметричних алгоритмом стали гібридні методи шифрування даних. Не всі форми криптографії однакові. Деякі системи можна легко обминути або зламати. Інші – досить стійкі навіть для тривалих атак. Здатність криптографічної системи захистити інформацію від атаки називається стійкістю. Криптографічна стійкість залежить від різних факторів, зокрема:

– Секретність ключа.

– Складність відгадування ключа або спроби перебору всіх можливих ключів (складність пошуку ключа). Як правило, чим довше ключ, тим складніше його підібрати.

– Складність обернути обчислення шифрувального алгоритму без знання ключа шифрування (злом шифрувального алгоритму).

– Існування (або відсутність) будь-яких «лазівок», або інших способів, якими можна легко отримати секретні дані без знання ключа.

– Можливість розшифрувати все зашифроване повідомлення, якщо ви знаєте спосіб, яким можна розшифрувати певний шматок повідомлення (називається атака з відомим текстом).

– Властивості вихідного тексту та знання цих властивостей зловмисником.

Наприклад, криптографічна система може бути вразливою до атак, якщо всі зашифровані повідомлення в цій системі починаються і закінчуються відомим фрагментом тексту. Ціль криптографічного проектування – створити алгоритм, за якого складно відтворити всі дії у зворотному порядку без відповідного ключа; для якого спроба вгадати ключ була б рівносильною послідовному підбору ключів один за одним. Такий шифр буде стійким, навіть якщо зломщик володіє якоюсь інформацією про зміст повідомлення, тому що в ньому лежать складні математичні обчислення.

Постановка завдання. Підвищення швидкості шифрування та дешифрування інформації Для досягнення мети необхідно виконати наступні завдання:

– виконати огляд існуючих методів та засобів шифрування та дешифрування інформації;

– розробити програмну реалізацію розробленого алгоритму.

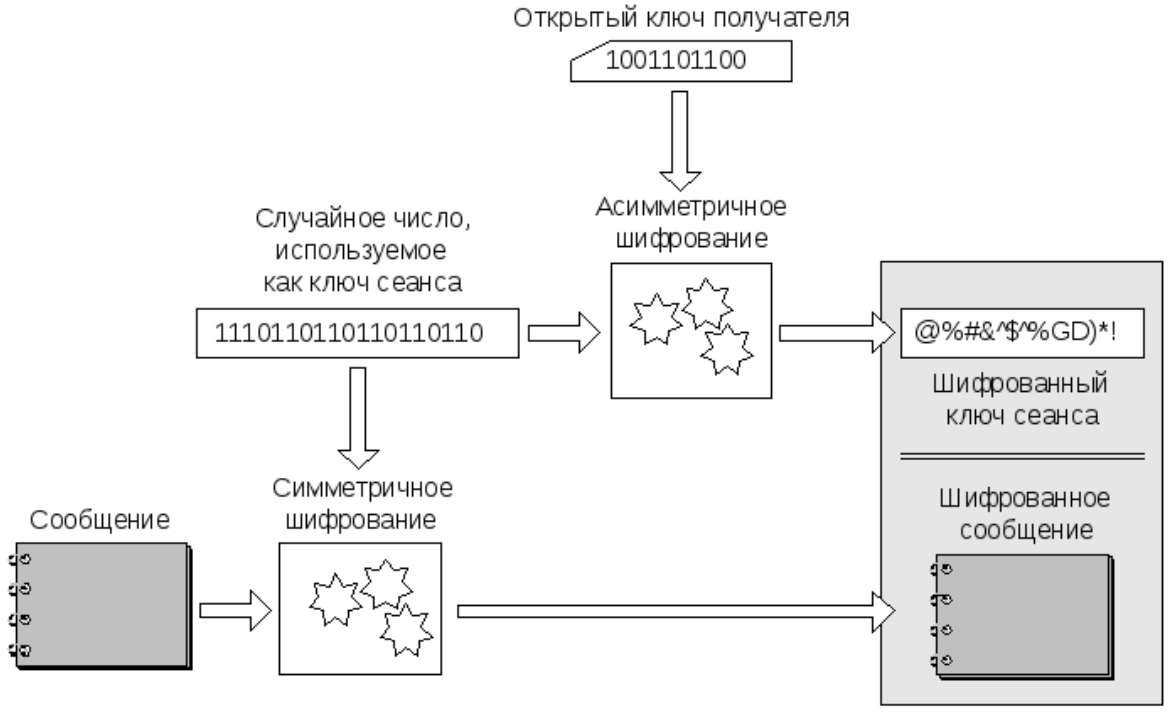

Рис. 1. **Схема асиметричного шифрування**

Результати досліджень. Використання алгоритму RSA в «чистому вигляді» не є найкращою ідеєю, так як швидкість обробки інформації буде дуже і дуже низькою, тобто. Для ключів великої довжини та значних за розміром файлів знадобиться значний час шифрування (розшифрування). Тому в прикладних програмах комбінують схеми асиметричного та блокового шифрування, використовуючи швидкість і надійність блокових шифрів та зручність розподілу ключів асиметричних систем.

Отримувач за допомогою свого секретного ключа розшифровує сеансовий ключ блокового шифрування, а потім за допомогою Blowfish розшифровує вже саме повідомлення. Таким чином, послідовність дій одержувача та відправника дзеркальні.

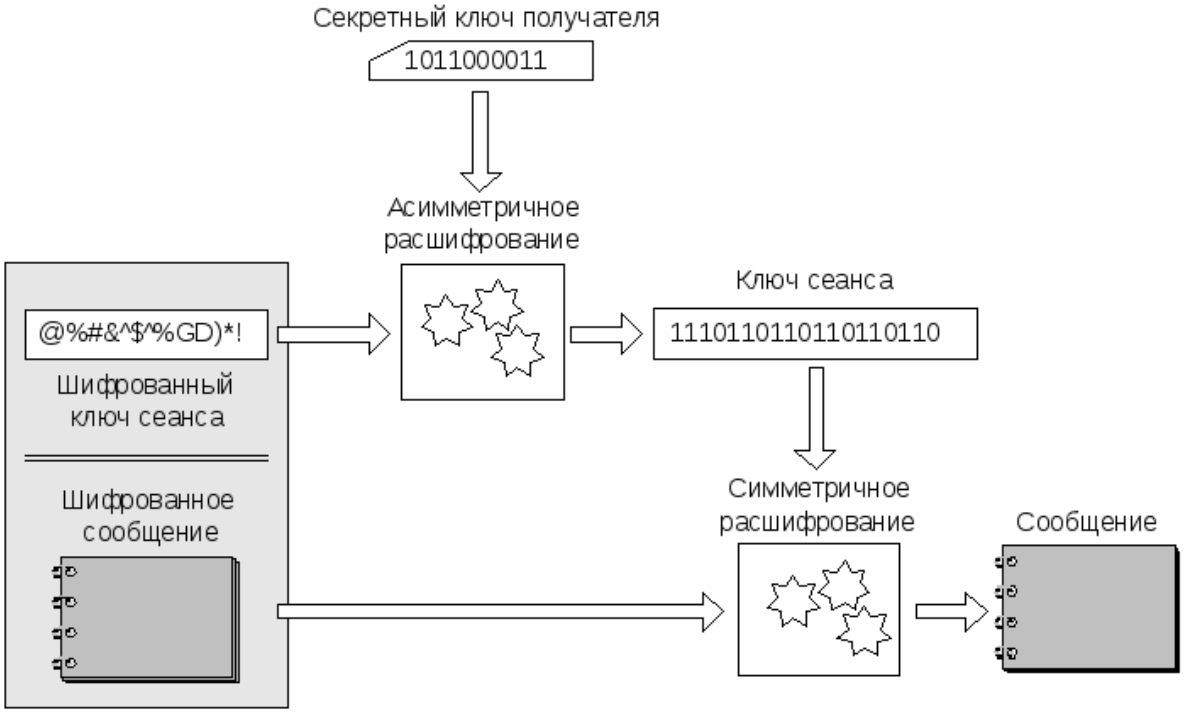

Рис. 2. **Схема асиметричного шифрування**

Висновки. Було досягнуто швидкості шифрування та дешифрування інформації. Для досягнення мети виконалися наступні завдання:

- огляд існуючих методів та засобів шифрування та дешифрування інформації;
- розробка програмної реалізації розробленого алгоритму.

Список використаної літератури

1. Алексенцев А. И. О составе защищаемой информации. *Безопасность информации*. 1999. No 2. С. 5–7.
2. Алферов А. П., Зубов А. Ю. и др. Основы криптографии: учеб. пособие. 2-е и зд., испр. и доп. М.: Гелиос АРВ, 2002. 480 с.
3. Анісімов А. В., Кулябко П. П. Інформаційні системи та бази даних: Навчальний посібник для студентів факультету комп'ютерних наук та кібернетики. Київ, 2017. 110 с.
4. Антоненко В. М., Мамченко С. Д., Рогушина Ю. В. Сучасні інформаційні системи і технології: управління знаннями: навч. посібник. Ірпінь: Нац. університет ДПС України, 2016. – 212 с.
5. Асиметричні_алгоритми_шифрування. URL: https://uk.wikipedia.org/wiki/
6. Бакут П. А. Информационные ресурсы – вопросы теории и практики. Научно-техническая информация. Серия: Организация и методика информационной работы. 2007. No. 11. С. 16–23.
7. Баранов А., Брыжко В., Базанов Ю. Права человека и защита персональных данных. К., 2000.
8. Библиотеки и информационные ресурсы в современном мире науки, культуры, образования и бизнеса. *Материалы 14-й Международной конференции "Крым 2007"* (Алушта, 9–17.06.2007). К.: НПБ Украины, 2007. 75 с.