УДК 519.72

М.О. Чугаєва
Сумський державний педагогічний університет ім. А.С. Макаренка

КРИПТОСИСТЕМИ З ВІДКРИТИМ ТА ЗАКРИТИМ КЛЮЧЕМ

У будь-якому суспільстві люди передають, зберігають та переробляють інформацію. Повідомлення по радіо, телебаченню, дзвоники на заняття у школі, сигнали світлофора – все це приклади передачі інформації. Записи у щоденниках, бібліотеки, архіви, музеї, книги, платівки, диски – це сховища інформації. Під час обчислень, пошуку потрібної довідки, написанні реферату або статті відбувається переробка інформації. Усі дії з інформацією називають інформаційними процесами, а науку про вимірювання та передачу інформації – теорією інформації. Однією з найважливіших проблем теорії інформації є проблема передачі інформації. Процес передачі інформації можна подати у вигляді схеми (рис. 1).

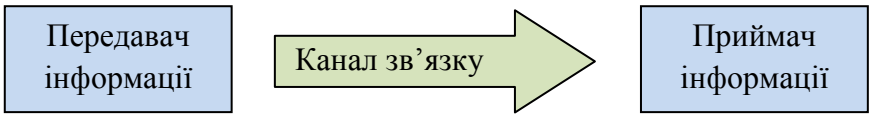

Рис. 1. Схема передачі інформації

Зрозуміло, що найбільше проблем при передачі інформації виникає саме у каналі зв'язку. Це, насамперед, проблеми, пов'язані з надійністю та часом передачі інформації, перетворенням інформації, її цілісністю та захистом.

Повідомлення, надіслані по радіо, телебаченню, через супутник чи комп'ютерні мережі можуть бути спотворені внаслідок різного роду шумів або перехоплені сторонніми особами. Щоб не допустити можливості отримання інформації (або її спотворення) сторонніми особами, повідомлення змінюють так, щоб приховати оригінал. У зв'язку з цим широкого використання набула *криптологія* – наука про створення й аналіз систем безпеки зв'язку. Криптологію умовно можна розділити на дві пов'язані між собою галузі: криптографію та криптоаналіз.

Криптографія вивчає методи забезпечення секретності та ідентичності (достовірності) інформації при її передачі через канал зв'язку чи при зберіганні. До основних понять криптології відносять поняття кода та шифра. Кодом називають правило для заміни одиниць інформації. Шифром (або криптосистемою) – алгоритм засекречування інформації [3].

Повідомлення шифрується для того, щоб стати незрозумілим, а кодується для того, щоб бути зрозумілим навіть після часткового спотворення внаслідок природних перешкод у каналі зв'язку. У типовій ситуації текст повідомлення закодовують (наприклад, у двійкову послідовність), потім шифрують і знову

кодують так, щоб можна було виявити та виправити помилки після отримання. Отриманий текст підлягає декодуванню та дешифровці.

Криптоаналіз – наука про методи розкриття (зламування) або підробки даних. Тобто, криптографія та криптоаналіз спрямовані на розв'язання взаємообернених задач.

Задачі криптології змінювалися упродовж її розвитку. Спочатку вона слугувала лише для забезпечення секретності інформації, що передавалась по військових та дипломатичних каналіх зв'язку.

Історія шифрів сягає часів Геродота (484 – 425рр. до н.е.), коли секретні повідомлення на дерев'яних табличках, покритих воском, попередили спартанців про вторгнення персів на їх територію. У II ст. до н.е. поширення набув квадратний шифр Полібія; пізніше (100 – 44рр. до н.е.). Юлієм Цезарем був винайдений ще один спосіб шифрування, який полягав у зсуві латинського алфавіту на кілька літер. Перші спроби викласти основні ідеї криптології були зроблені у середні віки абатом Тритеміусом (1462-1516 рр), Б. Віженером (1523-1596 рр.) та Дж. Кардано (1501-1576 рр.). У XX ст. поштовхом до розвитку криптології стали праці К.Шеннона.

При шифруванні даних відправник і отримувач інформації повинні узгодити процедуру шифрування та розшифровки. Як правило, вона складається із загального метода та ключа. Ключ забезпечує специфічну інформацію, що разом із загальним методом дозволяє відправнику легко зашифрувати, а отримувачу розшифрувати повідомлення. Отже, щоб зашифрувати повідомлення необхідно застосувати ключ, який може бути відомий як усім (так званий *відкритий ключ*), так і секретний, який відомий лише відправнику та отримувачу (*закритий ключ*). Для обох вказаних методів шифрування існує досить велика кількість різноманітних способів зашифрувати інформацію [4; 3, 23].

Особливістю криптосистем із закритим (секретним) ключем є використання однакового ключа для шифрування та дешифрування, тому іноді дані схеми називають симетричними. У цьому випадку за відсутності ключа кожен, хто перехопив повідомлення, не повинен (навіть маючи у розпорядженні потужні обчислювальні ресурси) за прийнятний час мати змогу дешифрувати повідомлення. Якщо згадати шифр Цезаря, в якому використовується ключ довжиною не більшою, ніж кількість букв у римському алфавіті, то при сучасних технологічних можливостях підібрати значення ключа дуже легко. Тому для даних схем використовуються більш довгі ключі. Якщо стороння людина дізнається про метод шифрування, то для підбору ключа довжиною 128 біт необхідно дуже багато часу, навіть при використанні комп'ютерних методів, бо кількість можливих комбінацій дорівнює $3{,}4 \cdot 10^{38}$. Тому методи шифрування, які використовують державні служби безпеки відкриті для загалу. Прикладами найвідоміших алгоритмів шифрування з секретним ключем є:

- DES – стандарт шифрування (Data Encryption Standard), що використовується урядом США.

- Skipjack – секретний алгоритм симетричного ключа (був зламаний у 1998 році), який застосовують в обладнанні. Розроблений Агенством державної безпеки США.
- Triple-DES – стандарт DES, який застосовують тричі для підвищення складності зламування.
- RC2, RC4, RC5 та RC6 – комерційні шифри, які створює та ліцензує компанія RSA Security, Inc. Наприклад, компанія Microsoft використовує для власного програмного забезпечення шифр RC4.
- AES – алгоритм AES є новим федеральним стандартом обробки інформації, який застосовують для визначення криптографічного алгоритму в організаціях уряду США для захисту секретної інформації.

Перевагою алгоритмів шифрування за допомогою відкритого ключа є їх швидкість та ефективність. Недоліки – ключ повинен знати отримувач, якщо ж їх декілька, ймовірність розкриття конфіденційності збільшується.

Розглянемо більш детально шифрування з відкритим ключем, тобто криптосистему, в якій ключ відомий, а метод шифрування залишається секретним. Іноді таке шифрування називають асиметричним, адже отримувач та відправник не обов'язково мають користуватися однаковим ключем.

Однією з перших криптосистем з відкритим ключем є криптосистема Р.Рівеста, А.Шаміра і Л.Едлемана, яка стала відомою під назвою RSA. В основі цієї схеми лежить піднесення до степеня по заданому (досить великому) модулю при фіксованій експоненті [3,93].

Розглянемо деяку комунікаційну мережу з великою кількістю абонентів, які бажають налагодити між собою довірливе спілкування. Вважатимемо, що інформація якою вони обмінюються закодована цілими числами ω, $0 \le \omega < N$. На практиці число N має від 200 до 600 десяткових знаків. Кожен користувач мережі обирає два досить великі прості числа p і q так, щоб їх добуток $n = pq$ був більшим від N. Обидва ці числа необхідно тримати в таємниці, а от число n можна відкрито публікувати в каталогах абонентів мережі. Додатково необхідно опублікувати випадково вибране число e, яке є взаємно простим як з $p-1$, так і з $q-1$ (того самого порядку, що й число n). Таким чином, відкритим ключем буде пара чисел (n,e).

Якщо ми бажаємо відправити таємне повідомлення ω, то знаючи відкритий ключ, обчислюємо остачу s від ділення ω^e на n і відсилаємо її. Щоб дешифрувати дане повідомлення необхідно скористатись таємним ключем. Ним є довільне число d, для якого $de \equiv 1 (\mathrm{mod}\, p-1)$ і $de \equiv 1 (\mathrm{mod}\, q-1)$. Таке число d можна легко обчислити, застосовуючи розширений алгоритм Евкліда до пари чисел e і $(p-1, q-1)$. Далі слід знайти остачу від ділення s^d на n, яка й збігатиметься з вихідним повідомленням ω. Справді, $s^d \equiv (\omega^e)^d = \omega^{ed} (\mathrm{mod}\, n)$,

тому враховуючи умову $de \equiv 1(\mathrm{mod}(p-1)(q-1))$ та застосовуючи теорему Ейлера, дістанемо $\omega^{ed} \equiv \omega(\mathrm{mod}\, n)$ [1].

Складність дешифрування отриманого криптотексту ворогом, навіть якщо в нього є відкритий ключ (n,e) полягає в тому, що без знання множників p і q не існує напевно можливого способу знаходження дешифруючого ключа d, який відповідає за оборотність відображення $\omega \to \omega^e(\mathrm{mod}\, n)$. Крім того, не існує інших методів дешифрування. Проте, останні два твердження залишаються недоведеними. Можна сказати, що задача зламування шифру RSA ймовірно має ту ж складність, що й задача розкладання числа n на множники.

Для прикладу виберемо числа $p=29$ і $q=31$. Тоді $n=29\cdot 31=899$, $\varphi(n)=(p-1)(q-1)=28\cdot 30=840$. Також виберемо число $e=17$. Тобто, відкритий ключ матиме вигляд: $(899,17)$. Знайдемо тепер таке число d, щоб $17d \equiv 1(\mathrm{mod}\, 840)$. Цю умову задовольняє $d=593$, оскільки

$$593\cdot 17 = 10081 = 12\cdot 840 + 1.$$

Тоді відкритий текст повідомлення $m=100$ при шифруванні матиме вигляд: $c=100^{17}(\mathrm{mod}\, 899)=101$. Справді, $101^{593}(\mathrm{mod}\, 899)=100$.

Зрозуміло, що знаючи алгоритм шифрування, стороння особа може точно відтворити відкритий текст повідомлення m, тобто вона може так само, як і відправник знайти шифр C та порівняти його з отриманим криптотекстом. Враховуючи можливість вичерпуючого пошуку така загроза є досить небезпечною, якщо кількість можливих текстів порівняно невелика. Якщо додавати до коротких повідомлень випадкові байти, то цю загрозу можна в деякій мірі подолати [2].

Таким чином, кожен з наведених способів шифрування (з відкритим та закритим ключами) мають свої недоліки та переваги. А саме, шифрування з відкритим ключем є більш безпечним, але більш повільнішим у порівнянні з асиметричними системами. Але для аутентифікації, шифрування й відправки ключа для симетричних шифрів RC4 або AES використовують шифрування з відкритим ключем. Отримувач спочатку розшифровує симетричний ключ, який далі використовує для розшифрування корисних даних.

Найпопулярніші зараз стандарти SSL/TLS і IPSec, які застосовують для шифрування даних в Інтернеті, комбінують алгоритми асиметричного та симетричного шифрування з метою використання переваг кожного. Комбінування методів шифрування підвищує загальний рівень безпеки системи передачі інформації. У деяких системах програмне забезпечення обирає симетричний ключ випадково, таким чином розкриття одного ключа сеансу зв'язку не впливає встановлення наступного сеансу.

Література

1. Андрійчук В.І. Вступ до дискретної математики / В.І. Андрійчук, М.Я. Комарницький, Ю.Б. Іщук– Львів: ВЦЛНУ ім. І.Франка. – 2003. – 255 с.

2. Брассар Дж. Современная криптология/ Дж. Брассар. – М.: ПОЛИМЕД, 1999. – 176 с.
3. Галуев Г.А. Математические основы криптологии: Учебно-методическое пособие / Г.А. Галуев. – Таганрог: Изд-во ТРТУ 2003. – 120 с.
4. Коробейников А.Г. Математические основы криптологии. Учебное пособие / А.Г. Коробейников., Ю.А. Гатчин. – Спб: Спб ГУ ИТМО, 2004. – 106 с.
5. Фомичев В.М. Дискретная математика и криптология. Курс лекцій / Под общ. Ред. д-ра физ-мат. н. Н.Д. Подуфалова. – М.: ДИАЛОГ– МИФИ, 2003. – 400 с.

Анотація. *Чугаєва М.О. Криптосистеми з відкритим та закритим ключем. У статті висвітлюються питання щодо застосування шифрів для передачі, збереження й обробки даних. Описуються два основні методи шифрування, їх застосування у сучасному світі. Розглядаються недоліки і переваги шифрування з секретним і з відкритим ключами.*

Ключові слова: *інформація, шифрування, дешифрування, ключ шифрування, криптосистема.*

Аннотация. *Чугаева М.А. Криптосистемы с открытым и закрытым ключом. В статье освещаются вопросы, касающиеся использования шифров для передачи, сохранения и обработки информации. Описываются два основных метода шифрования, их применение в современном мире. Рассматриваются недостатки и преимущества шифрования с секретным и с открытым ключами.*

Ключевые слова: *информация, шифрование, дешифрование, ключ шифрования, криптосистема.*

Summary. *Chugaeva M.O. Cryptosystems with public and private keys. The article highlights the issue of the use of codes for transmission, storage and processing. Two basic encryption methods and their application in the modern world are described. The advantages and disadvantages of secret encryption and public key are considered.*

Keywords: *information, encryption, decryption, encryption key cryptosystem.*