УДК 316.74

Л. А. Рогозіна
О. О. Семенова

Шифрування інформації у системах передачі даних

Вінницький національний технічний університет

Анотація
В статті наведений спосіб захисту інформації від несанкціонованого доступу – шифрування, описані основні криптосистеми.
Ключові слова: шифрування, дешифрування, криптосистема, ключ, алгоритм, захист, несанкціонований доступ.

Abstract
Encryption, the way to protect information from unauthorized access, is presented in the paper. Basics cryptosystems are described as well.
Keywords: encryption, decipherment, cryptosystem, key, algorithm, protection, unauthorized access.

Шифрування – це кодування даних з метою захисту від несанкціонованого доступу. Процес кодування називається шифруванням, а процес декодування – розшифруванням. Саме кодоване повідомлення називається шифрованим, а застосований метод називається шифром.

Основна вимога до шифру полягає в тому, щоби розшифрування (і, можливо, шифрування) були можливі тільки при наявності санкцій, тобто деякої додаткової інформації (або пристрою), яка називається ключем шифру. Процес декодування шифровки без ключа називається дешифруванням.

Галузь знань про шифри, методи їх побудови та розкриття називається криптографією. Властивість шифру протистояти розкриттю називається криптостійкістю або надійністю і звичайно визначається складністю алгоритму дешифровки.

У практичній криптографії криптостійкість шифру оцінюється з економічних міркувань. Якщо розкриття шифру коштує (в грошовому еквіваленті, включаючи необхідні комп'ютерні ресурси, спеціальні пристрої тощо) більше, за саму зашифровану інформацію, то шифр вважається достатньо надійним [1].

Симетричні криптосистеми (симетричне шифрування) – спосіб шифрування, в якому для шифрування та дешифрування використовуються один й той самий криптографічний ключ.

Ключ шифрування має зберігатись у секреті обома сторонами та має бути обраним до початку обміну повідомленнями.

Процес розшифрування заключається в тому, щоби ще раз скласти шифровану послідовність з тією самою гамою шифру:

Описаний метод має суттєвий недолік. Якщо відома хоча б частина висхідного повідомлення, то все повідомлення може бути легко дешифроване.

Більшість симетричних шифрів використовують складну комбінацію великої кількості підстановок та перестановок. Багато таких шифрів виконуються у декілька (до 100) проходів, використовуючи на кожному проході ключ проходу. Множина «ключів проходів» для всіх проходів називається розкладом ключів. Зазвичай, він утворюється з ключа шляхом виконання над ним певних операцій, в тому числі перестановок та підстановок.

Найважливішими параметрами всіх алгоритмів симетричного шифрування є:

- стійкість;
- довжина ключа;
- кількість раундів;
- довжина блоку, якій оброблюється;
- складність апаратно/програмної реалізації;
- складність перетворень.

До переваг симетричної системи можна віднести:

- порівняно високу швидкість (приблизно на 3 порядки вищу ніж у асиметричних систем);
- простота реалізації (за рахунок більш простих операцій);
- менша необхідна довжина ключа для відповідної стійкості;

Але є також суттєві недоліки, які практично призводять до того, що дана система майже не використовується на даний час.

- складність керування ключами у великій мережі. Це означає квадратичне збільшення кількості ключів, які необхідно генерувати, зберігати, передавати та знищувати у мережі. Для мережі з 10 абонентів потрібно 45 ключів, для 100 – вже 4950, для 1000 – 499500;
- складність обміну ключами. Для застосування симетричної системи необхідно вирішити проблему надійної передачі ключів до кожного абонента, тому що необхідний секретний канал для передачі кожного ключа обом сторонам [2].

Криптографічна система з відкритим ключем (або асиметрична криптосистема, асиметричне шифрування) – це система шифрування, при якій відкритий ключ передається по відкритому (тобто не захищеному) каналу зв'язку та використовується для шифрування повідомлень. Для розшифрування повідомлень використовується секретний (або приватний) ключ.

Наявність двох ключів – відкритого та закритого – й робить цю систему асиметричною. Відкритий ключ розсилається всім, хто бажає відправляти повідомлення адресату, а приватний ключ зберігається адресатом і не повинен нікому відправлятись. Навіть якщо знати відкритий ключ та все відправлене розшифроване повідомлення, неможливо знайти приватний ключ.

До переваг асиметричної криптосистеми можна віднести:

- не потрібно передавати закритий ключ будь-якими каналами зв’язку;
- на противагу симетричній криптосистемі, секретний ключ зберігається тільки у одній стороні;
- у симетричній криптосистемі варто змінювати ключ після кожного сеансу передачі даних, у асиметричній ключі можна тримати незміненими достатньо довгий час;
- у більшості мереж кількість ключів при асиметричному шифруванні набагато менша, ніж при симетричному.

Недоліки:

- хоча повідомлення шифруються надійно, але самі сторони «засвічуються» самим фактом передачі (на чому може бути побудована атака);
- асиметричні алгоритми використовують набагато довші ключі ніж симетричні;
- у чистому вигляді асиметричні системи вимагають значних обчислювальних ресурсів, тому на практиці вони частіше використовуються разом з іншими алгоритмами [3].

Також асиметрична система з відкритим ключем використовується у системах цифрових підписів. Цей процес ґрунтується на властивості комутативності операцій шифрування та розшифрування [4]:

$$M = (M^e)^d \bmod n = M^{ed} \bmod n = M^{de} \bmod n = (M^d)^e \bmod n = M.$$

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1. Тема 23. Шифрування [Електронний ресурс] / http://oim.asu.kpi.ua/ – Режим доступу до ресурсу: http://oim.asu.kpi.ua/files/DM/23_Cryptography.pdf.
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – Санкт-Петербург: БХВ-Петербург, 2009 – 576 с.
3. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. – М.: Аст, Астрель, 2006 – 447 с.
4. Мао В. Современная криптография. Теория и практика. – М.: Вильямс, 2005 – 763 с.

Науковий керівник: Семенова Олена Олександрівна – к.т.н., доцент кафедри телекомунікаційних систем та телебачення, Вінницький національний технічний університету, м. Вінниця.

Рогозіна Лідія Альбертівна – студентка групи ТКт-12б, факультет радіотехніки, зв'язку та приладобудування, Вінницький національний технічний університет, м. Вінниця, e-mail: coolida@bk.ru.

Supervisor: Semenova Olena – Candidate of Engineering Sciences, Associate Professor at the Department of Telecommunication Systems and Television, Vinnytsia National Technical University, Vinnytsia.

Lidiia Rohozina – group TKt-12, Faculty for Radio Engineering, Telecommunication and Electronic Instrument Engineering, e-mail: coolida@bk.ru.