Захист інформації від несанкціонованого доступу шляхом шифрування даних

Є.О. Філіп'єв, *студент,*
О.Л. Левошко, *викладач*
Кіровоградський національний технічний університет

Проблема захисту інформації шляхом її перетворення, що виключає доступ до неї сторонньою особою, хвилювала людський розум з давніх часів.

Історія криптографії - ровесниця історії людської мови. Більш того, спочатку писемність сама по собі була криптографічною системою, тому що в древніх суспільствах нею володіли лише обрані. Священні книги Стародавнього Єгипту, Стародавньої Індії тому приклади.

З широким поширенням писемності, криптографія стала формуватися як самостійна наука.

Поширення писемності викликало потребу саме в криптографії. Основними типами класичних шифрів є перестановочні шифри, які змінюють порядок літер в повідомленні, та підстановочні шифри, які систематично замінюють літери або групи літер іншими літерами або групами літер.

Одним із ранніх підстановочних шифрів був шифр Цезаря, в якому кожна літера в повідомленні замінювалась літерою через декілька позицій із абетки. Цей шифр отримав ім'я Юлія Цезаря, який його використовував, зі зсувом в 3 позиції, для спілкування з генералами під час військових кампаній.

Шифротексти, отримані від класичних шифрів (та деяких сучасних), завжди видають деяку статистичну інформацію про текст повідомлення, що може бути використано для злому. Після відкриття частотного аналізу, майже всі такі шифри стали більш-менш легко зламними досвідченим фахівцем. Майже всі шифри залишались беззахисними перед криптоаналізом з використанням частотного аналізу до винаходу поліалфавітного шифру. Інновація даного методу полягала в тому, щоб використовувати різні шифри для різних частин повідомлення.

В поліалфавітному шифрі Віженера, алгоритм шифрування використовує ключове слово, яке керує підстановкою літер в залежності від того, яка літера ключового слова використовується. В середині 18 ст., Чарльз Беббідж показав, що поліалфавітні шифри цього типу залишились частково беззахисними перед частотним аналізом.

На початку 20-го століття, було створено і запатентовано багато механічних шифрувально/ дешифрувальних приладів, серед них роторні машини — найвідомішою серед них є Енігма, автомат, що використовувався Німеччиною з кінця 20-тих і до кінця Другої світової війни. Шифри, реалізовані прикладами покращених варіантів, призвели до істотного підвищення криптоаналітичної складності.

Поява цифрових комп'ютерів та електроніки після Другої світової війни зробило можливим появу складніших шифрів. Більше того, комп'ютери дозволяли шифрувати будь-які дані, які можна представити в комп'ютері у двійковому виді, на відміну від класичних шифрів, які розроблялись для шифрування письмових текстів. Це зробило непридатними для застосування лінгвістичні підходи в криптоаналізі.

Однак, комп'ютери також знайшли застосування у криптоаналізі, що, в певній мірі, компенсувало підвищення складності шифрів. Тим не менше, гарні сучасні шифри залишались попереду криптоаналізу; як правило, використання якісних шифрів дуже ефективне (тобто, швидке і вимагає небагато ресурсів), в той час як злам цих шифрів потребує набагато більших зусиль ніж раніше, що робить криптоаналіз настільки неефективним та непрактичним, що злам стає практично неможливим.

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що передбачають використання обчислювальних засобів. Відомо більше десятка перевірених алгоритмів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму криптографічно стійкі.

Насьогодні, розрізняють два типи шифрів: симетричні та несиметричні.

До алгоритмів симетричного шифрування належать методи шифрування, у яких ключ шифрування, та ключ дешифрування однакові, або один із них легко обчислюється з іншого та навпаки.

Симетричні алгоритми шифрування можна розділити на потокові та блочні. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Блочні алгоритми працюють з блоками фіксованого розміру. Як правило, довжина блоку дорівнює 64 бітам, але, в алгоритмі AES використовуються блоки довжиною 128 біт.

До найвідоміших блочних шифрів належать DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 та ін.

Шифри Data Encryption Standard (DES) та Advanced Encryption Standard (AES) є стандартами блочних шифрів затверджених урядом США (однак, стандартизацію DES було скасовано після прийняття стандарту AES). Не зважаючи на те, що стандарт DES було визнано застарілим, він (та особливо його все ще дійсний варіант triple-DES) залишається досить популярним; він використовується в багатьох випадках, від шифрування в банкоматах до забезпечення приватності електронного листування та безпечному доступі до віддалених терміналів.

Симетричні алгоритми шифрування не завжди використовуються самостійно. В сучасних криптоситемах, використовуються комбінації симетричних та асиметричних алгоритмів, для того, аби отримати переваги обох схем. До таких систем належить SSL, PGP та GPG. Асиметричні алгоритми використовуються для розповсюдження ключів швидших симетричних алгоритмів.

В основному, симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні. На практиці, це означає, що якісні асиметричні алгоритми в сотні або в тисячі разів повільніші за якісні симетричні алгоритми. Недоліком симетричних алгоритмів є необхідність мати секретний ключ з обох боків передачі інформації. Так як ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації під час розповсюдження.

Проблемою симетричного шифрування є необхідність передачі ключа, для розшифрування інформації, таким чином ключ може бути перехоплений кимось іншим. Будь хто, знаючий секретний ключ, може розшифрувати інформацію. Тоді як в асиметричному шифруванні є два пов'язаних ключа -- пара ключів. Відкритий ключ -- публічний, до нього повинні мати доступ всі ті, хто матиме потребу зашифрувати інформацію. Тоді як закритий ключ -- приватний ключ, повинен бути в секреті, і доступний лише тому хто має право розшифрувати інформацію.

Будь яку інформацію, зашифровану за допомогою відкритого ключа можна розшифрувати лише застосовуючи той самий алгоритм, але з використанням відповідного приватного ключа. Також всю інформацію, зашифровану за допомогою

приватного ключа, можна розшифрувати лише за допомогою відповідного відкритого ключа.

Це означає, що немає необхідності хвилюватись за передачу ключа, відкритий ключ повинен бути публічним. Але асиметричне шифрування є значно повільнішим від симетричного. Також потребує значно більше обчислювальної потужності як для шифрування, так і для розшифрування інформації.

До даного методу належать такі алгоритми як DES та Elgamal.

Через недоліки в швидкодії асиметричного методу даний методи доводиться використовувати разом з симетричним (асиметричні методи на 3 - 4 порядки повільніші). Так, для рішення задачі ефективного шифрування з передаванням секретного ключа, використаного відправником, інформація спочатку симетрично зашифровується випадковим ключем, потім цей ключ зашифровують відкритим асиметричним ключем одержувача, після чого повідомлення і ключ відправляються по мережі.

Сучасний захист інформації передбачає постійне вдосконалення системи відповідно до зростання ризиків несанкціонованого доступу до інформації. Даний процес безперервний і полягає в реалізації сучасних методів та шляхів вдосконалення систем інформаційної безпеки, постійному контролі, виявленні її слабких місць і потенційних каналів для викрадення інформації. Безперервне вдосконалення систем обумовлене появою нових способів доступу до інформації ззовні

Сучасний захист інформації характеризується за допомогою таких методів:

- криптографічний захист різного ступеня конфіденційності при передачі інформації;
- управління інформаційними потоками, як у локальній мережі, так і при передачі каналами зв'язку на різні відстані;
- застосування механізмів обліку спроб доступу ззовні, подій в інформаційній системі і друкованих документів;
- забезпечення цілісності програмного забезпечення та інформації;
- впровадження засобів відновлення сучасної захисту інформації;
- здійснення фізичної охорони та обліку техніки і магнітних носіїв;
- створення спеціальних служб інформаційної безпеки.

Систематичне застосування всіх перерахованих вище методів і засобів сучасної захисту інформації, збільшує надійність системи безпеки і запобігає розголошення конфіденційної інформації.

Список літератури

1. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. — М.: Гелиос АРВ, 2002. — 240 с. — 3000 экз.
2. С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. — М.: Горячая линия — Телеком, 2002. — 175 с. — (Специальность. Для высших учебных заведений). — 3000 экз.
3. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный мир, 2004.
4. Вильям Столлингс. Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001. ISBN 5-8459-0185-5.
5. Ухлинов А. М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1996.
6. Мафтик С. Механизмы защиты в сетях ЭВМ. М.: Мир, 1993.
7. Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997.