МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ДЕРЖАВНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

**В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, В.А. Мухачьов,
В.І. Андрєєв, В.П. Щербина, Ю.Є. Яремчук**

КОМП'ЮТЕРНА КРИПТОГРАФІЯ

Лабораторний практикум для студентів, що навчаються з напрямків підготовки "Інформаційна безпека" і "Комп'ютерні системи та мережі".

Київ 2003

УДК 681.322:621.391
Х 87

Рецензенти:
В.П. Тарасенко, доктор технічних наук, професор
Л.М. Осинський, доктор технічних наук, професор

Затверджено Ученою радою Інституту інформаційно-діагностичних систем Національного авіаційного університету Міністерства освіти і науки України (протокол № 11 від 17.06.2003 р.)

Хорошко В.О., Азаров О.Д., Шелест М.Є., Андрєєв В.І., Мухачьов В.А., Щербина В.П., Яремчук Ю.Є.

Х87 Комп'ютерна криптографія. Лабораторний практикум. – Київ: НАУ, 2003. – 94 с.

У матеріалах лабораторного практикуму розглянуті сучасні методи та засоби криптографічного захисту інформації в лабораторних роботах та характерних практичних задачах.

Рекомендується для студентів і аспірантів, що навчаються з напрямку підготовки "Інформаційна безпека" і "Комп'ютерні системи та мережі" а також для фахівців, що працюють в галузі захисту інформації.

УДК 681.322:621.391

ЗМІСТ

ПЕРЕДМОВА

Розвиток і широке впровадження сучасних інформаційних технологій значно підвищили вразливість інформації, що циркулює в інформаційно-телекомунікаційних системах. Однією з причин цього є масове використання для обробки інформації засобів обчислювальної техніки з програмним забезпеченням, що дозволяє порівняно легко спотворювати, копіювати або знищувати оброблювану інформацію, а також змінювати штатні алгоритми накопичення, оброблення та передавання інформації каналами зв'язку. Розвиток нових інформаційних технологій створив наукові, технологічні та економічні передумови для появи таких понять, як «інформаційна війна» та «інформаційна зброя». Об'єктивні процеси масового впровадження подібних технологій в Україні висувають на перший план інформаційну складову такого загального поняття, як «національна безпека».

Відомим недоліком систем, створених на основі «відкритої архітектури», є принципова можливість доступу до інформації з боку осіб, для яких вона не призначена. Забезпечення адекватної і випереджальної протидії загрозам безпеки інформації є, у кінцевому рахунку, однією з найважливіших умов забезпечення політичної, економічної, оборонної та інших складових національної безпеки держави.

В даний час методи захисту інформації відіграють величезну роль у кредитно-фінансовій сфері, бізнесі, під час зберігання конфіденційної інформації та її передавання незахищеними каналами зв'язку, застосовуються в системах електронного документообігу та електронної комерції, використовуються під час забезпечення безпеки польотів і навіть можуть сприяти для з'ясування істини в ході судового розгляду. Протидія загрозам безпеки інформації повинна здійснюватися комплексно. Захист інформації необхідно забезпечувати на всіх етапах її накопичення, оброблення, зберігання та передавання. Надійно захистити інформацію в зовнішніх каналах зв'язку можна лише за допомогою криптографічних методів, до яких, зокрема, відноситься перетворення інформації з використанням секретних параметрів (шифрування). Криптографічні методи дозволяють, крім забезпечення конфіденційності, забезпечити цілісність та справжність інформації, організувати процедуру автентифікації абонентів, які обмінюються інформацією, реалізувати (без

розголошення) синхронне формування однакових псевдовипадкових даних на обох кінцях лінії зв'язку і т.д. Криптографічні методи базуються на тонких і не до кінця досліджених властивостях математичних об'єктів. У їхній основі лежить ідея використання математичних перетворень, побудова обернених до яких, без додаткових даних, обчислювально нереалізовна. Подібні перетворення називаються криптографічними. Відповідні додаткові дані (якщо вони є секретними параметрами) називаються ключами. Побудова криптографічних перетворень як і реалізація методів, що базуються на їх основі, не тривіальні. Тому знайомство з основами криптографії не тільки необхідно для повноцінної технічної освіти, але й корисно для практичних застосувань, у тому числі, в комерційній і фінансовій сферах.

ВСТУП

Проблема захисту інформації шляхом перетворення, що дозволяє уникнути її сприйняття сторонніми, хвилювала людський розум з давніх часів. Цій проблемі зобов'язана своїм народженням криптологія (kryptos – таємний, logos – наука) – наука, яка вивчає проблеми теорії і практики секретного зв'язку. Вона розділяється на два напрямки – криптографію і криптоаналіз – дисципліни, що у своєму розвитку переслідують прямо протилежні цілі. Криптографія займається пошуком і дослідженням математичних методів перетворення інформації, тобто криптографи намагаються забезпечити безпеку листування, винаходячи все нові і нові системи шифрування повідомлень. Сфера інтересів криптоаналізу – дослідження можливості розшифрування інформації без знання ключів, тобто криптоаналітики вирішують обернену задачу, розкриваючи шифри або підробляючи шифровані повідомлення, заміняючи істинний відкритий текст помилковими даними. Історія криптографії – однолітка історії людської мови. Більш того, спочатку писемність сама по собі була криптографічною системою, тому що в давніх суспільствах нею володіли тільки обрані. Священні книги Давнього Єгипту, Давньої Індії тому приклади. Із широким поширенням писемності криптографія стала формуватися як самостійна наука. Перші криптосистеми зустрічаються вже на початку нашої ери. Так, Цезар у своєму листуванні використовував шифр, який отримав його ім'я. Бурхливий розвиток криптографічні системи отримали в роки першої і другої світових війн. Починаючи з післявоєнного часу і по цей день поява обчислювальних засобів прискорила розробку й удосконалювання криптографічних методів. Чому проблема використання криптографічних методів в інформаційних системах стала в даний момент особливо актуальною? З одного боку, розширилося використання комп'ютерних мереж, зокрема, глобальної мережі Інтернет, якою передаються великі об'єми конфіденційної інформації і яка не допускає можливість несанкціонованого доступу. З іншого боку, поява нових потужних комп'ютерів, технологій мережних і нейронних обчислень, уможливило дискредитацію криптографічних систем, які ще недавно вважалися такими, які практично неможливо розкрити.

У наведених нижче лабораторних роботах основна увага приділена криптографічним методам захисту інформації. Сучасна криптографія містить у собі чотири загальних розділи:

1. Симетричні криптосистеми.
2. Криптографічні системи з відкритим ключем.
3. Криптографічні протоколи.
4. Керування ключами.

Широковідомим є використання криптографічних методів для передавання конфіденційної інформації каналами зв'язку (наприклад, в електронній пошті), під час встановлення справжності повідомлень, що передаються, а також для зберігання інформації (документів, баз даних) у зашифрованому вигляді на зовнішніх носіях. Криптографія дає можливість перетворити інформацію таким чином, що її прочитання (відновлення) можливо лише при знанні ключа.

Інформація, яка підлягає шифруванню і розшифруванню, представляється різними способами, найчастіше, у вигляді текстів, записаних у деякому алфавіті. Ці терміни розуміються так. Алфавіт – скінченна множина використовуваних для кодування інформації знаків. Текст – упорядкований набір з елементів алфавіту. Як приклади алфавітів, використовуваних у сучасних інформаційних системах можна, привести такі:

– алфавіт Z33 – 32 букви російського алфавіту і пропуск;
– алфавіт Z256 – символи, які входять у стандартний код ASCII, KOI-8;
– бінарний алфавіт – $Z2 = \{0,1\}$;
– вісімковий алфавіт або шістнадцятковий алфавіт.

Шифром називається множина обернених перетворень текстів повідомлень, що виробляються з метою приховування від зловмисника (противника) інформації, яка міститься в них. Перетворення тексту (повідомлення) за допомогою конкретно вибраного перетворення називається його шифруванням. Цей процес полягає в тому, що вихідний текст, який носить також назву відкритого тексту, замінюється шифрованим текстом. Процес застосування оберненого перетворення до отриманого шифрованого повідомлення називається розшифруванням. З використанням ключа шифрований текст перетвориться у вихідний. Ключем шифру називається сукупність даних, які визначають вибір

конкретного перетворення з усієї множини перетворень, що реалізуються шифром. По суті, ключ – це секретна інформація, необхідна для безперешкодного шифрування і розшифрування текстів. Найчастіше ключ являє собою послідовність, складену з букв алфавіту. Відновлення відкритих текстів повідомлень за умови, що ключі застосованих перетворень невідомі, називають дешифруванням. Криптографічні системи розділяються на симетричні і асиметричні (з відкритим ключем). У симетричних криптосистемах для шифрування і для розшифрування використовується той самий ключ. У системах з відкритим ключем використовуються два ключі – відкритий і закритий (секретний, особистий), які математично зв'язані один з одним, але не обчислюються один через одного за оглядовий час. Інформація для одержувача шифрується за допомогою відкритого ключа, який доступний усім бажаючим, а розшифровується за допомогою особистого ключа, відомого тільки одержувачу повідомлення. Терміни «розподіл ключів» і «керування ключами» відносяться до процесів системи обробки інформації, змістом яких є складання і розподіл ключів між користувачами. (Очевидно, ключі не повинні бути доступні стороннім). Криптографічні протоколи призначені для забезпечення взаємодії віддалених користувачів, у результаті чого формуються умови для коректного виконання процедур оброблення інформації. При цьому, коректність процедур оброблення інформації не можуть порушити ні сторонні, ні самі користувачі. Прикладом криптографічного протоколу може служити процедура перевірки авторства (справжності) повідомлення на основі електронного підпису. Електронним (цифровим) підписом документа називається результат особливого криптографічного перетворення, зробленого над документом його власником. При отриманні документа з підписом одержувач перевіряє деяке математичне співвідношення, істинність якого може забезпечити тільки власник документа. Роль криптографії полягає в неможливості формування підпису сторонніми, наприклад при внесенні в документ перекручувань.

Теоретично, існують шифри, які не піддаються дешифруванню. Поняття стійкості шифру розглядалося К. Шенноном у його роботі «Теорія зв'язку в секретних системах», опублікованій в 1949 році. Прийнято вважати, що ця робота сповістила початок ери наукової криптології. Шеннон назвав «нерозкривні шифри» ідеальними,

зауваживши, однак, що під час їхнього створення виникають нездоланні перешкоди. З цього він зробив висновок, що оцінка стійкості шифрів повинна спиратися на практичну складність їхнього розкриття. Криптостійкістю називається характеристика шифру, яка визначає міру складності його дешифрування. Ефективність шифрування з метою захисту інформації залежить, насамперед, від секретності ключа. У той же час, секретність алгоритму суттєвою не визнається. Є кілька показників криптостійкості, такі, як загальна кількість усіх можливих ключів; середній час, затрачуваний для визначення ключа; необхідний об'єм пам'яті. Процес криптографічного перетворення даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак їй притаманні й переваги: висока продуктивність, простота, захищеність і т.д. Програмна реалізація більш практична і допускає відому гнучкість у використанні. Для сучасних криптографічних систем захисту інформації є загальні вимоги, частина з яких наводиться нижче:

- зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;
- кількість операцій, необхідних для визначення ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинна бути не менша загальної кількості можливих ключів;
- кількість операцій, необхідних для розшифровування інформації шляхом перебору всіх можливих ключів, повинна мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень та прогнозу зростання потужності обчислювальних засобів);
- знання алгоритму шифрування не повинно впливати на надійність криптографічного захисту;
- незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- довжина шифрованого тексту повинна бути близькою довжині вихідного тексту;

– не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;
– алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

Нижче показано проходження інформації в системі секретного зв'язку, що відповідає класичній симетричній криптосистемі.

Відкритий текст M передається від передавача до приймача в зашифрованому вигляді. Шифрування проводиться за допомогою оберненого перетворення T_k, що вибирається з скінченної множини відображень за індексом k, який є ключем. Кожному ключу відповідає апріорна ймовірність його вибору. Таким чином, генератор ключів є пристроєм, який вибирає одне з відображень $T_1, T_2, ..., T_m$ з ймовірностями $p_1, ..., p_m$ відповідно. Шифртекст $E = T_k M$ передається незахищеним каналом зв'язку, де він може бути перехоплений. На прийомному кінці шифртекст розшифровується за допомогою оберненого перетворення T_k^{-1}, вибираного за допомогою усе того ж ключа k. Таким чином, криптографічна система є сімейством обернених відображень $\{T_i\}$ множини можливих повідомлень у множину криптограм. При цьому ймовірність зашифрування чергового повідомлення за допомогою відображення T_i дорівнює p_i.

Криптографічну систему часто називають секретною системою, загальною системою або просто системою. Зазвичай вважається, що множина можливих відкритих повідомлень $M_1, ..., M_n$ скінченна і ці повідомлення мають апріорні ймовірності $q_1, ..., q_n$. Дві системи збігаються,

якщо в них однакові множини відкритих повідомлень, криптограм і ключів, причому розподіли ймовірностей ключів рівні. Вибір ключа відбувається випадково, відповідно до розподілу ймовірностей ключів $p_1,\ldots,p_m$.

Під час створення криптографічної системи криптографи зазвичай враховують в яких умовах вона буде використовуватися, на який потік повідомлень розрахований канал зв'язку, за спливанням якого часу інформація втрачає свою цінність, тобто може бути розсекречена та інше. З цього випливає, що застосування дорогих систем шифрування, які мають високу стійкість, в багатьох випадках не виправдано, тобто на криптосистеми зі зниженою стійкістю також є попит.

Цикл лабораторних робіт дозволить познайомитися з деякими системами шифрування на конкретних прикладах, починаючи з таких класичних шифрів, як шифри заміни та перестановки і закінчуючи алгоритмами блокового шифрування та відкритого розподілу ключів, а також особливостями еліптичної криптографії, яка останнім часом бурхливо розвивається. Крім того будуть розглянуті генератори випадкових чисел та сучасні методи і засоби комп'ютерної стеганографії.

ЛІТЕРАТУРА

1. Организация и современные методы защиты информации. – М.: Концерн «Банковский Деловой Центр», 1998. – 465 с.

2. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электроинформ, 1997. – 364 с.

3. Шеннон К.Э. Теория связи в секретных системах / Работы по теории информации и кибернетики. – М.:И.Л., 1963. – С.333–402.

4. Введение в криптографию / Под общей ред. В. В. Ященко. - СПб.: Питер, 2001. - 288 с.

5. Брюс Шнайер. Прикладная криптография. Протоколы алгоритмы и исходные тексты на языке С. 2-е издание. Пер. с англ. - М.: Мир, 1996. – 562 с.

6. Manazes A., van Oorschot, S. Vanstone. Handbook of Applied Cryptography. – CRC Press, 1996. – 782 p.

7. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1997. – 335 с.

8. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія: Підручник. - Київ, 2002. – 504 с.

9. А. Саломаа. Криптография с открытым ключом: Пер. с англ. - М.: Мир, 1995. - 318 с.

10. Анохин М.И., Варнавский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М.: МИФИ, 1997. – 358 с.

11. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. – М.: ТЭИС, 1994. – 203 с.

12. Хоффман Л.Д. Современные методы защиты информации. - М.: Сов.радио, 1980. - 264 с.

13. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. Защита информации в персональных ЭВМ. – М.: Радио и связь, 1992. – 192 с.

14. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии. –М.: МЭИ, 2000. –100 с.

15. Клопов В.А., Мотуз О.В. Основы компьютерной стеганографии // Информационно-методический журнал «Защита информации. Конфидент». – 1997. – №4. – С.43–48.

16. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 143 с.

17. Закон України “Про електронний цифровій підпис”.
18. Закон України “Про електронні документи та електронний документообіг”.

Навчальне видання

Хорошко Володимир Олексійович
Азаров Олексій Дмитрович
Шелест Михайло Євгенович
Мухачьов Вячеслав Андрійович
Андрєєв Володимир Іванович
Щербина Володимир Парфирович
Яремчук Юрій Євгенович

КОМП'ЮТЕРНА КРИПТОГРАФІЯ

Лабораторний практикум

Оригінал-макет підготовлено Яремчуком Ю.Є.
Редактор В.О. Дружиніна
Технічний редактор Н.К. Ніколаєва

Видавництво НАУ
Свідоцтво Держкомінформу України
серія ДК № 977 від 05.07.2002 р.
03058, м. Київ, проспект Космонавта Комарова, 1, НАУ

Підписано до друку 27.06.2003 р.
Формат 60×84/16
Друк різографічний
Тираж 300 прим.
Зам. №287/111

Гарнітура Times New Roman
Папір офсетний
Умовн. друк. арк. 6,04

Віддруковано в видавництві НАУ
серія ДК № 977 від 05.07.2002 р.
03058, м. Київ, проспект Космонавта Комарова, 1