Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет

ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Підручник

Вінниця
ВНТУ
2011

УДК 004.056.55(075)
ББК 32.973я73
О 75

Автори:
Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук

Затверджено Міністерством освіти і науки, молоді та спорту України як підручник для студентів вищих навчальних закладів, які навчаються за напрямом підготовки «Управління інформаційною безпекою». Лист № 1/11-7280 від 04.08.2011 року.

Рецензенти:
Г.Ф. Конахович, доктор технічних наук, професор
В.Ю. Богданович, доктор технічних наук, професор
Г.В. Кузнєцов, доктор технічних наук, професор

Основи криптографічного захисту інформації : підручник /
О75 Г. М. Гулак, В. А. Мухачов, В. О. Хорошко, Ю. Є. Яремчук — Вінниця : ВНТУ, 2011. — 199 с.
ISBN 978-966-641-430-7

У підручнику розглядаються питання організації та функціонування надійних систем криптографічного захисту інформації. Наведено методику генерації та оцінювання якості псевдовипадкових послідовностей, а також методи генерації псевдовипадкових простих чисел.

Наводяться характеристики стійкості розповсюджених блокових шифрів та асиметричних криптоалгоритмів, описані криптографічно стійкі генератори псевдовипадкових чисел, викладено принципи організації, функціонування та забезпечення надійності інфраструктури відкритих ключів.

Підручник призначено для студентів вищих навчальних закладів та аспірантів, а також фахівців, які займаються криптографією.

УДК 004.056.55(075)
ББК 32.973я73

ISBN 978-966-641-430-7

ЗМІСТ

ВСТУП

На сучасному етапі розвитку індустріально-інформаційного суспільства все більшого значення набувають автоматизовані системи передачі, зберігання і обробки інформації, основані на використанні комп'ютерних технологій.

Такі системи вимагають постійного вдосконалення, а їх поширення в глобальних масштабах приводить до необхідності уніфікації принципів побудови і вживання відповідних технічних засобів.

З розвитком телекомунікацій стали доступними зручні засоби, які реалізовують обмін електронними даними, що привело до формування сфери електронного документообігу.

При побудові систем електронного документообігу на основі каналів зв'язку загального призначення виникають специфічні вимоги, пов'язані з необхідністю захисту інформації, такі як забезпечення конфіденційності, цілісності, авторства даних і так далі. Ці вимоги ускладнюються за умови недовіри учасників інформаційного обміну один до одного.

Крім того, захист інформації необхідний для забезпечення працездатності самих автоматизованих систем.

Не випадково необхідність впровадження засобів криптографічного захисту інформації (КЗІ) є одним з положень Закону України «Про електронні документи і електронний документообіг».

Слід зазначити, що стандарти, які на сьогодні діють в Україні, в області криптографічного захисту інформації не покривають весь спектр необхідних криптоалгоритмів і криптопротоколів, наприклад, відсутні стандарти на асиметричну криптосистему і систему узгодження симетричних ключів.

З іншого боку, необхідні криптоалгоритми і криптопротоколи можна побудувати на основі окремих положень вітчизняних і міжнародних стандартів, з подальшою процедурою сертифікації.

Це зумовлює до необхідність аналізу вимог і обмежень, встановлених нормативно-правовими документами, і вимагає об'єктивної оцінки можливостей організації відносно реалізації відповідних технологій.

У запропонованому навчальному посібнику розглядаються питання організації і функціонування надійних систем криптографічного захисту інформації. Викладені принципи побудови криптосистем різного типу, наведена методика генерації і оцінки якості псевдовипадкових послідовностей, а також методи генерації псевдовипадкових простих чисел.

Особлива увага приділена генерації якісних ключів на основі криптографічних генераторів псевдовипадкових послідовностей.

Наводяться описи і характеристики стійкості блокових шифрів ГОСТ 28147-89, Rijndael і асиметричних криптоалгоритмів, розглянуті принципи організації, функціонування і забезпечення надійності інфраструктури відкритих ключів.

Метою посібника є виклад матеріалу, використання якого передбачається на етапі розробки концепції системи КЗІ електронного документообігу організації.

Посібник призначений для студентів старших курсів вищих навчальних закладів і аспірантів, знайомих з елементарною теорією чисел (включаючи теорію символу Якобі), а також фахівців, що займаються впровадженням засобів КЗІ.

Автори щиро вдячні докторові технічних наук, професорові Кузнєцову Георгію Віталійовичу, докторові технічних наук, професорові Скрипникові Леоніду Васильовичу і докторові технічних наук, професорові Шелесту Михайлу Євгеновичу за доброзичливе і уважне ставлення до запропонованої книги, а також за зауваження і рекомендації, що сприяли значному покращенню матеріалу.

Ми вдячні НВФ «КРИПТОН» і ТОВ «ТРИТЕЛ» за надану можливість використання в книзі матеріалів за виробами цих фірм.

Ми виражаємо також особливу подяку всім авторам, роботи яких були використані при підготовці даного посібника і допомогли розширити тематику, порушену в книзі.

ГЛАВА 1 ОСНОВНІ ПОНЯТТЯ І ЗАДАЧІ КРИПТОЛОГІЇ

1.1 Предмет криптології, криптографія і криптоаналіз

Історія криптографії – ровесниця історії писемності, з її широким розповсюдженням криптографія сформувалася як мистецтво тайнопису. Згадки про перші шифри зустрічаються вже на початку нашої ери. Так, римський імператор Гай Юлій Цезар використовував в своєму листуванні шифр, що одержав згодом його ім'я.

Постійними замовниками криптографічних систем в усі часи були дипломати і військові. Саме збільшення об'ємів інформації, що передається, і скорочення строків на її обробку у відповідних відомствах сприяло швидкому розвитку шифрувальної техніки і її впровадженню замість ручних шифрсистем.

В розвитку шифрувальної техніки можна прослідкувати декілька етапів.

З початку і до середини XX століття – використання механічних і електромеханічних шифрмашин: вироби М-94, М-138-Т4 (США), С-36 (Швеція), «Енігма» (Німеччина, рис.1.1).

Вже на цьому етапі використовувалися оригінальні і достатньо стійкі, за мірками того часу, криптоалгоритми.

Наприклад, шифратор «Енігма» реалізує оригінальний метод комутації електричних сигналів за допомогою декількох дисків, що рухаються за певним законом (рис. 1.1). Кожний диск має рівну кількість вхідних і вихідних контактів, з’єднаних попарно.

Електричний струм послідовно проходить через контактну групу натиснутої клавіші, стале з'єднання дисків, повертається через рефлектор, знов через диски і запалює індикаторну лампу, що відповідає зашифрованій букві.

В 50 - 80-х роках XX століття – застосування електронної шифртехніки, побудованої на дискретних радіоелементах і мікросхемах малого ступеня інтеграції.

Починаючи з 80-х років минулого століття – впровадження шифрувальної техніки на основі мікрокомп'ютерів і мікроконтролерів, створення спеціалізованих мікросхем, що реалізовують криптографічні функції (зокрема, стандарти шифрування DES, RSA).

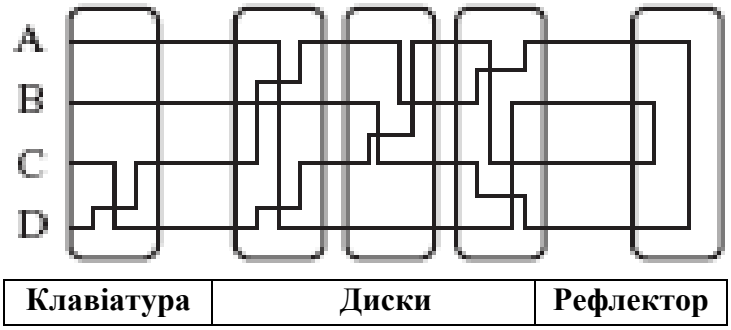

Рисунок 1.1 - Модель комутації сигналів в шифрмашині «Енігма»
(символ А переходить в С, символ В – в D і навпаки)

Нові технічні можливості в 70-80 роках XX століття надали більший простір математикам для створення все більш складних для проведення криптоаналізу криптоалгоритмів. У тому числі, широке впровадження згаданих алгоритмів DES і RSA в значній мірі було зумовлено повсюдним розповсюдженням комп'ютерної техніки і впровадженням обчислювальних мереж.

З іншого боку, створення потужних комп'ютерів, технологій мережевих обчислень збільшувало ризик розкриття криптографічних систем, які ще недавно вважалися стійкими. Відзначимо, що перша в світі електронно-релейна обчислювальна машина була створена англійцями в роки другої світової війни для дешифрування німецької шифрмашини «Енігма».

Широке використання комп'ютерних мереж, зокрема, глобальної мережі Інтернет, розвиток електронних банківських технологій, збільшення об'ємів передачі інформації з обмеженим доступом державного, військового, комерційного і приватного характеру зумовили розвиток нових напрямів в криптографії, включаючи системи відкритого розподілу ключів і системи електронного цифрового підпису. На сьогодні важко знайти інформаційну (ІС) або інформаційно-телекомунікаційну систему (ІТС), в якій не застосовувалися б механізми криптографічного захисту інформації.

Сучасна шифрувальна техніка характеризується малими габаритами і вагою, високою швидкістю шифрування, надійним захистом інформації з обмеженим доступом (рис. 1.2 - 1.6).

Питання до розділу 11

1. Що розуміється під архітектурою системи електронного цифрового підпису (ЕЦП)?
2. Які характеристики архітектури системи ЕЦП є основними?
3. Які основні послуги відносять до сервісу реєстрації системи ЕЦП?
4. Які основні процедури відносять до сервісу сертифікації?
5. Яке призначення сервісу ведення баз даних і для чого використовуються протоколи LDAP і OCSP?
6. Які функції виконує сервіс блокування і відміни?
7. Які завдання служби управління ключами?
8. У чому відмінність між ієрархічною і мережевою моделями довіри?
9. Які вимоги до масштабовної архітектури системи ЕЦП?
10. Що таке політика центру сертифікації?
11. Яким чином визначається статус ЕЦП в Законі України «Про електронний цифровий підпис»?
12. Яким чином організовується система ЕЦП відповідно до законодавства України?
13. Для чого призначений центр сертифікації ключів другого рівня?
14. У чому полягає акредитація центру сертифікації ключів?
15. У чому полягає сертифікація і допуск до експлуатації засобів КЗІ?

ЛІТЕРАТУРА

1. Тилборг ван Х. К. А. Основы криптологии / Тилборг ван Х. К. А. – М. : Мир, 2006. - 471 с.
2. Основы криптографии / [Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.]. – М. : «Гелиос АРВ», 2001. –480 с.
3. Бабаш А. В. Криптография (аспекты защиты) / А. В.Бабаш, Шанкин Г. П. – М. : СОЛОН-Р, 2002. – 512 с.
4. Ленков С. В. Методы и средства защиты информации / Ленков С. В., Перегудов Д. А., Хорошко В. А. – К. : АРИЙ, 2008, Том I – 464с., Том II – 344 с.
5. Харин Ю. С. Математические основы криптологии / Харин Ю. С. Берник В. К. Матвеев Г.В. – Минск, БГУ, 1999. – 319 с.
6. Защита информации в системах телекоммуникации: Учебное пособие для вузов / [Банкет В. Л. и др.]. – Од., УГАС им. А.С. Попова, 1997. – 96 с.
7. Иванов М.А. Криптографические методы защиты в компьютерных системах и сетях / Иванов М.А. – М. : КУДИЦ-ОБРАЗ, 2001. – 368 с.
8. Фомичев В.М. Дискретная математика и криптология / Фомичев В.М. – М. : ДИАЛОГ-МИФИ, 2003. – 400с.
9. Гулак Г. Різні підходи до визначення випадкових послідовностей: / Г. Гулак. Л. Ковальчук // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2001. – №3 – С. 127-133.
10. Кнут Д. Искусство программирования для ЭВМ. Том 2. Получисленные алгоритмы / Кнут Д. – М. : МИР, 1977. – 235 с.
11. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – М. : Изд-во ТРИУМФ, 2002. – 816 с.
12. Венбо Мао. Современная криптография. Теория и практика / Венбо Мао ; [пер. с англ.]. – М. : Изд. дом «Вильямс», 2005. – 786 с.
13. Винокуров А. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89 и алгоритма Rijndael, выбранного в качестве

нового стандарта шифрования США, «Системы безопасности» / А.Винокуров. Применко Э. – М. : Изд. «Гротэк», 2001, №№1,2.

14. А.Винокуров. Алгоритм шифрования ГОСТ 28147-89, его использование и реализация для компьютеров платформы Intel x86. Работа на правах рукописи, доступна на веб-сайте http://www.enlight.ru/crypto.

15. Основные принципы проектирования, оценка стойкости и перспективы использования в Украине алгоритма шифрования AES / [Гулак Г., Горбенко И., Олейников Р. и др.] // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні» – Київ. – 2003. – №7 – С. 14-25.

16. Коблиц Н. Курс теории чисел и криптографии / Коблиц Н. – М. : Научное издательство ТВП, 2001. – 106с.

17. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии / Черемушкин А. В.– М. : МЦНМО, 2002.

18. Мухачев В. А. Методы практической криптографии / В. А. Мухачев, В. А. Хорошко. – К. : ООО «ПолиграфКонсалтинг», 2005. –215с.

19. Бессалов А. В. Криптосистемы на эллиптических кривых / А. В. Бессалов, А. Б. Телиженко. – К. : ІВЦ Видавництво «Політехніка», 2004. – 224 с.

20. Введение в криптографию/ [Ященко В. В. и др.]; под общ. ред. В. В. Ященко. – М.: МЦНМО, «ЧеРо», 1998. – 272 с.

21. ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

22. ГОСТ Р ИСО/МЭК 9594-8-98 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации.

23. ГОСТ Р ИСО/МЭК 9594-9-95 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 9. Дублирование.

24. Горбатов В.С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская. – М. : Горячая линия – Телеком. 2004. С.171-224.

25. Бернет С. Криптография. Официальное руководство RSA Security / С. Бернет, С. Пейн. – М. : Бином-Пресс, 2002. С.279-292.

26. Щербаков А. Прикладная криптография. Использование и синтез криптографических интерфейсов / А. Щербаков, А. Домашев. – М.: «Русская редакция», 2003. С.28-136.

27. Вербицький О. Вступ до криптології / Вербицький О. – Львів : Видавництво науково-технічної літератури, 1998. – 247 с.

28. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах: Навч. Посібник. Ч.1. Криптографічний захист інформації / І. Д. Горбенко. Т. О. Гріненко. – Харків: ХНУРЕ, 2004. – 368 с.

29. Аналіз властивостей алгоритмів блокового симетричного шифрування (за результатами міжнародного проекту NESSIE): Радіотехніка. Всеукраїнський міжвідомчий науково-технічний збірник, вип. 141 / [Горбенко І.Д., Гулак Г.М., Олійников Р.В. та інш.]. – Харків: ХНУРЕ, 2005. – С. 7-24.

30. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

31. ГОСТ 34.310-95 Криптографическая защита информации. Процедура выработки и проверки цифровой подписи на базе асиметричного криптографического алгоритма

32. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования.

33. Блочный симметричный алгоритм SHACAL-2 / Г. Гулак. И. Горбенко. М. Михайленко. Ю. Гитис // Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – 2003. – №7 – С. 86-100.

34. Гулак Г. Н. Национальная технология ЕЦП: «время собирать камни» / Г. Н. Гулак, Л. В. Скрыпник // Збірка наукових праць Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, спеціальний випуск «Моделювання та інформаційні технології» – 2005 – С. 23-28.

35. Конхейм А. Г. Основы криптографии / Конхейм А. Г. – М. : Радио и связь, 1987. – 412 с.

36. Математичні основи криптографії / [Кузнецов Г. В., Фомічов В. В., Сушко С. О., Фомічова Л. Я.]. – Дніпропетровськ : НГУ, 2004. – 389 с.

37. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації. Затверджено наказом ДСТСЗІ СБ України від 30.11.99 №53, зареєстровано в Міністерстві юстиції України 15.12.99 за № 868/4161, із змінами, згідно з наказом ДСТСЗІ СБ України від 30.04.04 № 31.

38. Шеннон К.Э. Теория связи в секретных системах / К.Э. Шеннон // Работы по теории связи и кибернетике. – М.: ИЛ, 1963. – С. 333-402.

39. NIST Special Publications 800-22. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, 2000.

40. RIJNDAEL description. Submission to NIST by Joan Daemen, Vincent Rijmen. http://www.csrc.nist.gov/encryption/aes/round1/docs.htm.

41. Mecanismes cryptographiques Version 1.10. Crypto DCSSI @sgdn.pm.gouv.fr, 2006.

42. Feldman P. A practical scheme for non-interactive verifiable secret sharing // Proc. 28th Annu. Symp. on Found. of Comput. Sci. 1987. P. 427-437.

43. ФоменковГ.В. http://www.citforum.ru/cryptography/fortezza/.shtm.

Навчальне видання

Гулак Геннадій Миколайович
Мухачов Владислав Андрійович
Хорошко Володимир Олексійович
Яремчук Юрій Євгенович

ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Підручник

Редактор В. О. Дружиніна

Оригінал-макет підготовлено Ю. Є. Яремчуком

Підписано до друку 14.10.2011 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк. 13,01
Наклад 500 (1-й запуск 1-150) прим. Зам. № 2011-157

Вінницький національний технічний університет,
навчально-методичний відділ ВНТУ.
21021, м. Вінниця, Хмельницьке шосе, 95.
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-85-32.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті
в комп'ютерному інформаційно-видавничому центрі.
21021, м. Вінниця, Хмельницьке шосе, 95.
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-87-38.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.