УДК 681.3.06

НОВІТНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Ю.Мінгальова
Науковий керівник: д.п.н. Спірін О.М.

Кафедра прикладної математики та інформатики
Житомирський державний університет ім. І.Франка
e-mail: Mingalyova.Yuliya@yandex.ru

У статті розглянуто сучасні симетричні та асиметричні методи криптографічного захисту інформації, квантову криптографію та особливості криптосистем на основі еліптичних кривих.

Ключові слова: *захист інформації, криптографія, методи криптографічного захисту інформації, симетричне шифрування, асиметричне шифрування.*

Розвиток нових інформаційних технологій і впровадження комп‘ютерних систем в усі сфери людської діяльності стали причиною різкого зросту інтересу широкого кола користувачів до проблеми інформаційного захисту. Захист інформації – це сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умови впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації [4]. Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одними із головних задач є: забезпечення конфіденційності, цілісність та автентичність даних, що передаються [2, с.5]. Криптографія – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми) і автентичності (цілісності і справжності автора) інформації [5]. На сьогодні криптографія, як галузь знань, та криптографічний захист інформації, як окрема галузь діяльності, стосується: питань шифрувальної справи, новітніх технологій електронної торгівлі, систем автоматизованого управління, звітування та контролю тощо. Формування високопродуктивних методів шифрування(розшифрування) з високою криптографічною стійкістю є важливою складовою у вирішенні питання інформаційної безпеки. Методи криптографічного захисту інформації – це системи шифрування інформації, алгоритми захисту від нав‘язування фальшивої інформації (MAC-коди та алгоритми електронного цифрового підпису) та криптографічні протоколи розподілу ключів, автентифікації та підтвердження факту прийому(передачі) інформації [12]. Криптографічна

стійкість методів криптографічного захисту інформації – це властивість криптографічних алгоритмів і криптографічних протоколів, що характеризує їх здатність протистояти методам дешифрування (процес несанкціонованого відновлення оригіналу тексту повідомлення) [8].

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. На сьогодні відомо більше десятка перевірених методів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу (наука "зламування" криптографічних перетворень).

Виділяють такі загальні вимоги для криптографічних методів захисту інформації [6]:

зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа (набір параметрів для шифрування повідомлення);

число операцій, необхідних для визначення використаного ключа шифрування по фрагменту повідомлення і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів;

число операцій, необхідних для розшифрування інформації шляхом перебору можливих ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп‘ютерів (із врахуванням можливості використання мережних обчислень);

знання алгоритму шифрування не повинно впливати на надійність захисту;

незначна зміна ключа повинна призводити до значної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

алгоритм має допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

Основні методи криптографічного захисту інформації можуть бути класифіковані різним чином, але найчастіше їх розподіляють в залежності від способу використання та за типом ключа [2, с.7]:

безключеві – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки);

перетворення з таємним ключем – використовується ключовий параметр – секретний ключ (симетричне шифрування, цифровий підпис, хеш-функції, ідентифікація);

перетворення з відкритим ключем – використовують в своїх обчисленнях два ключі – відкритий (публічний) та закритий(приватний) (асиметричне шифрування, цифровий підпис).

Цілісність інформації та автентичність сторін досягається використанням хеш-функції та технології цифрового підпису. Конфіденційність інформації забезпечується симетричним та асиметричним методами шифрування.

Методи симетричного шифрування(розшифрування) – це метод, за яким ключі шифрування і розшифрування є або однаковими, або легко

обчислюються один з одного, забезпечуючи спільний ключ, який є таємним [1]. Зазначений метод шифрування має велику кількість представників. Сучасними найбільш поширеними алгоритмами симетричного шифрування є такі системи [14, 16].

Система Lucifer – алгоритм блочного симетричного шифрування даних, розроблений в рамках дослідної програми з комп‘ютерної криптографії фірми IBM на початку 1970-х років.

Data Encryption Standard (DES) — це симетричний алгоритм шифрування даних, який прийнятий урядом США із 1976р. до кінця 1990-х рр., з часом набув міжнародного застосування.

International Data Encryption Algorithm (IDEA) – симетричний блочний алгоритм шифрування даних, запатентований швейцарською фірмою Ascom.

Advanced Encryption Standard (AES, Rijndael) — симетричний алгоритм блочного шифрування, прийнятий в якості американского стандарту шифрування урядом США. Станом на 2006 рік AES являється одним із найбільш поширених алгоритмів симетричного шифрування.

Blowfish — криптографічний алгоритм, який реалізує блочне симетричне шифрування. Розроблений на основі мережі Фейстеля Брюсом Шнайєром в 1993р.

ГОСТ 28147-89 - блокова шифросхема, яка при використанні методу шифрування з гамуванням, може виконувати функції потокового шифроалгоритма.

Методи асиметричного шифрування(розшифрування) – криптографічні алгоритми, в яких використовують пару ключів для кожного учасника протоколу – відкритий для шифрування і таємний для розшифрування, який не може бути обчислений з відкритого ключа за визначений час [11]. Сучасними методами даного шифрування є такі криптосистеми [15].

Схема McEliece - криптосистема з відкритими ключами на основі теорії алгебраїчного кодування. Перша схема, що використовує рандомізацію в процесі шифрування. Алгоритм McEliece заснований на складності декодування повних лінійних кодів.

Алгоритм Діффі-Хеллмана – криптографічний метод, який використовує функцію дискретного піднесення до степеня.

Схема ElGamal — криптосистема з відкритим ключем, заснована на труднощі обчислення дискретних логарифмів в скінченному полі, яка є удосконаленням системи Діффі-Хеллмана.

RSA — криптографічна система з відкритим ключем. Безпека алгоритму RSA побудована на принципі складності факторизації.

В останні роки значний інтерес викликає квантова криптографія, вагоме місце в якій займає квантовий розподіл ключів [7]. Квантова криптографія — метод захисту комунікацій, заснований на принципах квантової фізики [13]. На відміну від традиційної криптографії, яка використовує математичні методи, щоб забезпечити секретність інформації, квантова криптографія зосереджена на фізиці, розглядаючи випадки, коли інформація переноситься за допомогою

об'єктів квантової механіки. Процес відправки та прийому інформації завжди виконується фізичними засобами, наприклад, за допомогою електронів в електричному струмі, або фотонів у лініях волоконно-оптичного зв'язку. Технологія квантової криптографії грунтується на принциповій невизначеності поведінки квантової системи — неможливо одночасно отримати координати і імпульс частинки, неможливо виміряти один параметр фотона, не спотворивши інший.

Еліптична криптографія — розділ криптографії, який вивчає асиметричні криптосистеми, засновані на еліптичних кривих над скінченними полями [9]. Основна перевага еліптичної криптографії полягає в тому, що на сьогоднішній день невідомо субекспоненціальні алгоритми для вирішення задачі дискретного логарифмування в групах точок еліптичних кривих [10]. Використання еліптичних кривих для створення криптосистем було незалежно запропоновано Нілом Коблицом і Віктором Міллером в 1985 р.

У результаті аналізу джерел з розглянутої проблеми виділені та розглянуті сучасні найбільш поширені методи криптографічного захисту інформації від несанкціонованого доступу. В новітніх інформаційних системах для шифрування повідомлень, які передаються, використовуються симетричні алгоритми шифрування, зважаючи на велику обчислювальну здатність асиметричних алгоритмів, їх застосовують для генерації та поширення сеансових ключів (використовується під час сеансу обміну повідомленнями) [3]. Усунути основні недоліки, властиві як симетричним, так і асиметричним методам криптографічного захисту інформації, дозволяє їх комбіноване використання. Як відомо, у сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, а завданням «повільних» асиметричних алгоритмів стає шифрування ключа сеансу. В цьому випадку зберігаються переваги високої секретності (асиметричні) та швидкості роботи (симетричні) [11, 14]. Варто зазначити, що українським стандартом, який описує алгоритми формування та перевірки електронного цифрового підпису є прийнятий і введений в дію наказом державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 ґ 31 ДСТУ 4145-2002 (повна назва: "ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка").

Література:

1. Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с.
2. Бевз О.М. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню : монографія \ О.М. Бевз, Р.Н. Квєтний – Вінниця:ВНТУ, 2010. – 96 с.
3. Задірака В.К. Олексик О. Комп'ютерна криптологія / В. К. Задірака, О. Олексик. – Київ, 2002. – 505 с.
4. Захист інформації в телефонних лініях та радіо діапазоні [Електронний ресурс]. — Режим доступу: http://wiki.univ.uzhgorod.ua/index.php/Захист_інформації_в_телефонних_лініях_та_радіо_діапазоні
5. Криптографія [Електронний ресурс]. —Режим доступу: http://uk.wikipedia.org/wiki/Криптографія
6. Швець О.Ю., Лазаренко В.В. Аналіз методів і засобів захисту інформації та сучасних вимог до них / О.Ю. Швець, В.В. Лазаренко [Електронний ресурс]. — Режим доступу: http://www.rusnauka.com/25_DN_2008/Informatica/28842.doc.htm
7. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Учебное пособие, 2-е изд., испр. и доп. – М.. Гелиос АРВ, 2002. – 480 с., ил.
8. Бабаш А.В., Шангин Г.П. Криптография. Под редакцией В.П. Шестюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин. – М.:СОЛОН-ПРЕСС, 2007. – 512 с. – (Серия книг «Аспекты защиты»).
9. Болотов А.А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на Эллиптических кривых / А. А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – 280 с.
10. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.
11. Вельшенбах М. Криптография на Си и С++ в действии / М. Вельшенбах. Учебное пособие. – М.:Издательство Триумф, 2004 – 464 с.
12. Кузьминов В.И. Криптографические методы защиты информации / В.И. Кузьминов . – Новосибирск: Высшая школа, 1998.
13. Н. Смарт Криптография / Н. Смарт. – Москва: Техносфера, 2005. – 528 с.
14. Панасенко С.П. Алгоритмы шифрования / С.П. Панасенко. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.: ил.

15. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации / Б.Я. Рябко, А.Н. Фионов : Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2005. – 229 с.: ил.
16. Фергюсон, Нильс, Шнайер, Брюс. Практическая криптография / Фергюсон, Нильс, Шнайер, Брюс : Пер. с англ. – М.: Издательский дом "Вильямс", 005. – 424 с.:ил. – Парал. тит. англ.

MODERN CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

Yu.Mingalyova

Department of Applied Mathematics and Computer Science
Ivan Franko Zhytomyr State University
e-mail: Mingalyova.Yuliya@yandex.ru

The article deals with modern symmetric and asymmetric cryptographic methods of information security, quantum cryptography and features of the cryptosystems based on elliptic curves.

Keywords: *information security, cryptography, methods of cryptographic protection of information, symmetric encryption, asymmetric encryption.*