практика тестування самих програм і пакетів антивірусного захисту за певними балами і рейтингами та за певною сукупністю часткових показників функціонування тільки антивірусів. Це вірно, але цього не достатньо. Необхідно ще обов'язково оцінювати стан антивірусної безпеки самої комп'ютерної системи при використанні цих антивірусів. Безсумнівно, що це має велике практичне значення.

2. Для формування політики безпеки комп'ютерних систем доцільно визначати складову політику не антивірусного захисту, а антивірусної безпеки. Поняття "захист" від вірусів передбачає пасивні оборонні дії. Поняття "безпека" передбачає, навпаки, активні оборонні контрдії проти певних загроз. Тому при такій постановці задачі для формування складових політики безпеки комп'ютерних систем найбільш доцільно визначати "політику надання послуг антивірусної безпеки".

3. Запропоновані основи побудови системи антивірусної безпеки в корпоративних комп'ютерних мережах Інтранет, методи та приклади експертної кількісної оцінки стану антивірусної безпеки комп'ютерних систем різних конфігурацій можуть бути корисними для їх адміністраторів безпеки, користувачів, власників при організації антивірусного захисту, а також для аспірантів, магістрів, студентів вищих навчальних закладів і науково–дослідних установ при проведенні досліджень по цій тематиці.

*Література: **1**. Шорошев В. В., Домарев В. В. Журнал "Бизнес и безопасность" № 1, 2 1998 г. Рекомендации по обеспечению безопасности конфиденциальной информации согласно "Критериев оценки надежных компьютерных систем TCSEC" (Trusted Computer Systems Evaluation Criteria)", США, "Оранжевая книга". **2**. Шорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно европейским "Критериям оценки безопасности информационных технологий ITSEC" (Information Technology Security Evaluation Criteria). Журнал "Бизнес и безопасность" № 3, 1998 г. **3**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 5 1998 г. Международные стандарты безопасности компьютерных систем: эволюция развития, проблемы, рекомендации. **4**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 6 1998 г. Рекомендации по основам информационной безопасности согласно Канадских критериев CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), 1993 г. **5**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 1 1999г. Рекомендации по основам информационной безопасности согласно Единых критериев CCITSE (Common Criteria for Information Technology Security Evaluation), 1996 – 1997 г. г. **6**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 2 1999 г. Класифікація комп'ютерних вірусів і основи захисту від них. **7**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 3, 4, 5 1999 г. Основи захисту інформації ПЕОМ від загроз НСД. **8**. Шорошев В. В., Ильницкий А. Е., Маматкулов В. Т., Кривошеєв Е. А. Журнал "Бизнес и безопасность" № 6. 1999 г. Антивирусная защита вашей ПЭВМ. **9**. Ільніцький А. Ю., Шорошев В. В., Близнюк І. Л. Основи захисту інформації від несанкціонованого доступу. Звіт НДР, К. 2000. **10**. Зегжда Д. П.. Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с. **11**. Симонович С. Windows 98: учебный курс – СПб: Питер Ком, 1998. – 512 с.: ил.*

УДК 681.3.06

БЛОКОВИЙ СИМЕТРИЧНИЙ ШИФР НА ОСНОВІ МОДУЛЬНОЇ АРИФМЕТИКИ

Віталій Сокирук, Володимир Лужецький
Вінницький національний технічний університет

Анотація: **Пропонується блоковий симетричний шифр на основі модульної арифметики. Блоки даних та секретні ключі розглядаються як цілі числа, над якими виконуються арифметичні операції множення, ділення, додавання та віднімання за модулем 2^n.**
Summary: **Block cipher based on modular arithmetic is offered. Data blocks and secret keys examine as big integer numbers on which the multiplication, division, addition and subtraction modulo 2^n is executed.**
Ключові слова: **Захист інформації, криптографія, блокові симетричні шифри.**

І Вступ

Блокові симетричні шифри (БСШ) широко застосовуються для захисту інформації в сучасному інформаційному суспільстві. Вони є невід'ємним атрибутом багатьох систем захисту інформації і вирішують широкий спектр сучасних криптографічних задач. БСШ володіють високою швидкістю і забезпечують високий рівень криптостійкості, що робить їх використання безальтернативним для задач

шифрування великих об'ємів даних [1].

Більшість відомих БСШ побудовані на принципах, які були закладені розробниками алгоритму DES ще на початку 50-х років, а саме: використання великої кількості різноманітних логічних операцій над частинами блоку даних та над окремими розрядами з метою перемішування і розсіювання розрядів відкритого тексту на основі секретного ключа [2]. В таких БСШ блок даних розглядається як набір бітів з певною статистикою, і результатом роботи процедури зашифрування є змінення цієї статистики і приведення її до рівномірного закону розподілення.

Такі алгоритми ефективно реалізуються в апаратному вигляді, але мають малоефективні програмні реалізації, оскільки передбачають виконання великої кількості операцій над частинами блоку даних та над окремими розрядами, що не притаманно універсальним обчислювальним пристроям. Сучасні процесори здатні ефективно виконувати арифметичні і логічні операції над 32- та 64-розрядними числами, крім того існує постійна тенденція до збільшення розрядності обчислювальних пристроїв та появи спеціалізованих інструкцій для швидкого виконання арифметичних операцій над великими числами.

Блоковий шифр, що пропонується, побудований на основі модульної арифметики і розглядає блоки даних як великі цілі числа. Основними операціями в алгоритмах зашифрування та розшифрування є множення, ділення, додавання та віднімання за модулем.

II Операції множення та ділення за модулем

Нехай $Z_m = \{0,\ 1,\ 2,\ ...,\ m-1\}$ – множина цілих додатних чисел. Операція множення за модулем m чисел $A, B \in Z_m$ описується таким виразом:

$$A \cdot B \equiv C(\mathrm{mod}\, m). \tag{1}$$

Особливість операції множення за модулем полягає в тому, що результат завжди менший за модуль, тобто $C \in Z_m$. Якщо відомі добуток чисел A і B за модулем m і один з множників, наприклад, число B, то для знаходження іншого множника A необхідно виконати операцію ділення за модулем m:

$$A = \left(\frac{C}{B}\right)_{\mathrm{mod}\, m} = \left(C \cdot \frac{1}{B}\right)_{\mathrm{mod}\, m} = \left(C \cdot \left(\frac{1}{B}\right)_{\mathrm{mod}\, m}\right)_{\mathrm{mod}\, m} \tag{2}$$

При обчисленні результату ділення чисел C та B спочатку обчислюють число $B^{-1} = \left(\frac{1}{B}\right)_{\mathrm{mod}\, m}$, яке називають оберненим до числа B за модулем m. Для його обчислення використовується розширений алгоритм Евкліда [3]. Число B^{-1} існує, а рівняння (2) має єдиний розв'язок, коли виконується таке співвідношення:

$$НСД(B, m) = 1 \tag{3}$$

III Процедура зашифрування

Для того, щоб блоковий симетричний шифр був стійким до криптоаналізу, він має містити процедури перемішування та розсіювання розрядів відкритого тексту [3]. Тобто кожен розряд шифротексту має залежати від кожного розряду відкритого тексту і характер цієї залежності не повинен відслідковуватись алгоритмічними або статистичними методами. Внутрішня будова алгоритму вважається відомою криптоаналітику, і єдиним носієм секретної інформації є ключ, який використовується для зашифрування та розшифрування інформації.

Для перемішування і розсіювання розрядів відкритого тексту широко застосовуються таблиці підстановок та різноманітні логічні операції. Як правило, в блокових симетричних шифрах використовується велика кількість подібних операцій, які повторюються декілька раз в циклі, при чому в цих операціях приймають участь окремі розряди або групи розрядів відкритого тексту або проміжного результату. Цим досягається залежність вихідних розрядів блока шифротексту від усіх розрядів відкритого тексту і зміни статистичних характеристик повідомлення. Блок відкритого тексту в такому випадку розглядається як набір розрядів.

Пропонується розглядати блоки даних і ключі як цілі числа з множини Z_m. Як базові використовуються операції за модулем m, а для перемішування та розсіювання розрядів відкритого тексту використовується операція множення за модулем, яка володіє корисними властивостями:

– кожен розряд результату множення залежить від значень всіх попередніх розрядів обох операндів;

– розрядність блоку даних залишається незмінною;

– якщо відомий один з операндів (секретний ключ), то можна відновити невідомий операнд (блок відкритого тексту), якщо виконується умова (3).

Реалізація БСШ на основі арифметики за модулем m, де m – довільне число, є складною. Крім того, за використання одних тільки арифметичних операцій неможливо побудувати криптографічно стійкий шифр, оскільки закладені математичні залежності можуть бути легко викриті, якщо криптоаналітик може отримати деякі специфічні пари відкритих та зашифрованих текстів. Підвищити криптостійкість можна шляхом введення додаткових логічних нелінійних операцій, наприклад, додавання за модулем 2. Використання логічних операцій у випадку довільного модуля неприпустимо, оскільки для представлення чисел у двійковому вигляді необхідно, щоб модуль m дорівнював 2^n, де n – додатнє ціле число.

Використання в якості модуля числа 2^n дозволяє значно спростити реалізацію та прискорити виконання арифметичних операцій за модулем із збереженням усіх корисних властивостей і припускає використання логічних операцій.

Нехай M – блок відкритого тексту, C – блок шифротексту і K – секретний ключ, при чому $M, C, K \in Z_{2^n}$. Запишемо процедуру зашифрування у випадку використання однієї операції множення за модулем:

$$C = \left(M \times K\right)_{\mathrm{mod}\, 2^n} \tag{4}$$

Криптостійкість такого алгоритму базується на тому факті, що якщо M та K великі складені цілі числа, то відновити їх за відомим значенням C дуже складно і при великих значеннях M практично неможливо. Такий алгоритм може використовуватись в тих випадках, коли вимоги щодо криптостійкості незначні, режим записної книжки не є необхідним, а вірогідність отримання зловмисником пар відкритих та зашифрованих текстів незначна. Якщо відомі одна або декілька пар шифротекстів і відповідних до них відкритих текстів, знаходження секретного ключа стає задачею тривіальною, оскільки в цьому випадку можна обчислити ключ розділивши число C на число M за модулем 2^n. Головна перевага запропонованого підходу – швидкість, з якою виконується шифрування.

Для того, щоб ускладнити криптоаналіз, необхідно ввести в алгоритм операцію, яка б вносила нелінійність і перешкоджала використанню відомих пар шифротекстів. Такою операцією може бути, наприклад, дзеркальна перестановка розрядів результату множення чисел M та K з подальшим множення на додатковий секретний підключ. Ця операція є складною для програмної реалізації, але забезпечує рівномірне перемішування та розсіювання розрядів блоку відкритого тексту M. В такому випадку зміна значення будь-якого розряду числа M призведе до перемішування всіх розрядів числа C. Однак реалізація шифру у випадку використання подібної операції значно ускладнюється, оскільки перемішування розрядів може виконуватись лише над двійковими числами. Тому з метою створення швидкої і одночасно простої реалізації шифру доцільніше використовувати логічну операцію додавання за модулем 2 і додатковий секретний підключ K_2.

$$C = \left(M \times K_1\right)_{\mathrm{mod}\, 2^n} \oplus K_2 \tag{5}$$

При умові, що секретні підключі K_1 та K_2 невідомі, наявність випадкових шифротекстів та відповідних їм відкритих текстів не надає переваг криптоаналітику. Критичним є лише випадок, коли $M = 0$, і тоді:

$$K_2 = C \oplus 0 \tag{6}$$

З виразу (6) можна легко обчислити секретний підключ K_2. У випадку, коли криптоаналітик може сам обирати значення M і отримувати відповідні значення C, також існує можливість часткового або повного розкриття секретних ключів шляхом перебирання специфічних значень M на вході алгоритму. Наприклад, змінюючи старші розряди числа M, коли всі інші розряди дорівнюють нулю.

Вирішити цю проблему можна шляхом додавання ще двох секретних підключів K_3 та K_4 наступним чином:

$$C = \left(\left(\left(\left(M \times K_1\right)_{\mathrm{mod}\, 2^n} \oplus K_2\right) \times K_3\right)_{\mathrm{mod}\, 2^n} + K_4\right)_{\mathrm{mod}\, 2^n} \tag{7}$$

Підключі K_3 та K_4 служать для підвищення стійкості шифру до криптографічних атак на основі вибраних шифротекстів. Процедура зашифрування, представлена виразом (7) є стійкою до криптографічних атак, які мали місце у випадку використання виразів (4) та (5). Так, якщо прийняти, що $M = 0$, отримаємо таке значення C:

$$C = \left(\left(\left(K_2 \oplus 0\right) \times K_3\right)_{\mathrm{mod}\, 2^n} + K_4\right)_{\mathrm{mod}\, 2^n} \tag{8}$$

Цей вираз не дає корисної інформації криптоаналітику, оскільки неможливо однозначно визначити будь-який розряд одного з 3-х невідомих ключів.

Таким чином, маємо вираз для зашифрування, в якому використовуються арифметичні операції множення та додавання за модулем m і операція додавання за модулем 2. Процедура зашифрування використовує секретний ключ, представлений підключами $K_1 - K_4$. Кожен підключ використовується один раз, тобто приймає участь тільки в одній операції. Розмір блоку даних n обирається довільно і може змінюватись в процесі зашифрування. У випадку, коли число n є кратним до розрядності обчислювального пристрою, досягається найбільша швидкодія, оскільки в цьому випадку арифметичні операції над великими числами можна представити як набір операцій над числами меншої розрядності, якими може ефективно оперувати обчислювальний пристрій.

Замість операції додавання за модулем 2 можуть бути використані інші логічні операції для перемішування розрядів. Найбільш ефективною є дзеркальна перестановка значень розрядів одного з проміжних результатів, однак її реалізація ефективна лише на апаратному рівні.

Зауважимо, що алгоритми обчислення арифметичних операцій незмінні, тому реалізації процедури зашифрування для різних розмірів блока даних також однакові.

IV Процедура розшифрування

Для відновлення блоку відкритого тексту M, зашифрованого за допомогою виразу (7), необхідно виконати зворотні арифметичні дії, тобто знайти число M:

$$M = \left(\left(\left(\left(C - K_4\right)_{\mathrm{mod}\, 2^n} / K_3\right)_{\mathrm{mod}\, 2^n} \oplus K_2\right) / K_1\right)_{\mathrm{mod}\, 2^n} \tag{9}$$

Операція розшифрування складається з двох операцій ділення і операції віднімання за модулем 2^n, та операції додавання за модулем 2.

Необхідною і достатньою умовою однозначного відтворення блоку відкритого тексту M є вибір таких підключів K_4 і K_3, які є взаємно простими з числом 2^n, тобто задовольняють умові (3). Оскільки число 2^n має єдиний дільник – число 2, взаємно простим з ним буде будь-яке непарне ціле число. Це і є достатньою і необхідною умовою існування єдиного розв'язку рівняння (9).

Використовуючи властивості арифметичної операції ділення за модулем (2) складні операції ділення у виразі (9) можна замінити більш швидкими і простими операціями множення. Це значно спрощує реалізацію шифру і дозволяє використовувати однаковий набір простих арифметичних операцій як в процедурі зашифрування, так і в процедурі розшифрування.

Користуючись виразом (2), операцію розшифрування (9) можна представити як:

$$M = \left(\left(\left(\left(\left(C - K_4\right)_{\mathrm{modn}} \times \left(\frac{1}{K_3}\right)_{\mathrm{mod2n}}\right)_{\mathrm{mod2n}} \oplus K_2\right) \times \left(\frac{1}{K_1}\right)_{\mathrm{mod2n}}\right)_{\mathrm{mod2n}}\right). \tag{10}$$

Обчислення чисел $\left(\frac{1}{K_3}\right)_{\mathrm{mod}\, 2^n}$ і $\left(\frac{1}{K_1}\right)_{\mathrm{mod}\, 2n}$ здійснюється за узагальненим алгоритмом Евкліда, реалізація якого для великих чисел складна. Тому пропонується попередньо, на етапі формування ключів, обчислити значення виразів $K_1^* = \left(\frac{1}{K_1}\right)_{\mathrm{mod}\, 2^n}$ та $K_3^* = \left(\frac{1}{K_3}\right)_{\mathrm{mod}\, 2^n}$. Для спрощення апаратної реалізації операцію віднімання за модулем можна замінити на операцію додавання шляхом попереднього обчислення виразу $K_4^* = \left(-K_4\right)_{\mathrm{mod}\, 2^n}$.

Тоді вираз (10) можна записати як:

$$M = \left(\left(\left(\left(C + K_4^*\right)_{\mathrm{mod}\,2^n} \times K_3^*\right)_{\mathrm{mod}\,2^n} \oplus K_2\right) \times K_1^*\right)_{\mathrm{mod}\,2^n}. \quad (11)$$

Як бачимо, операцію розшифрування можна представити у вигляді виразу, подібного до того, що використовується для зашифрування. Таким чином, процедури зашифрування і розшифрування використовують однаковий ключ K_2, і три різних ключа K_1, K_3 та K_4 для зашифрування і K_1^*, K_3^* та K_4^* для розшифрування.

Значення числа n (розрядність блоку даних) обирається довільно із міркувань швидкодії та криптостійкості, а також може змінюватись в процесі шифрування. Із збільшенням n автоматично збільшується кількість елементарних операцій, необхідних для опрацювання блока даних.

V Висновки

Запропоновано алгоритм блокового симетричного шифрування на основі арифметичних операцій за модулем 2^n. Всі операції в алгоритмі виконуються над блоками даних, які представляються як цілі числа з множини Z_{2^n}. Операції зашифрування та розшифрування використовують секретний ключ, що складається з чотирьох секретних підключів. Секретні підключі K_1, K_2, K_3 та K_4 використовуються для зашифрування, а для розшифрування необхідно попередньо обчислити підключі K_1^*, K_3^*та K_4^*. Ключ K_2 не змінюється при розшифруванні.

Запропонований БСШ володіє високою швидкістю за рахунок використання простих арифметичних операцій, які швидко виконуються на сучасних ЕОМ. Також алгоритм просто реалізується в апаратному вигляді, оскільки містить обмежений набір простих операцій. Швидкість процедур зашифрування та розшифрування приблизно однакова і залежить окрім тактової частоти від розрядності обчислювального пристрою. Для підвищення швидкості виконання операції множення великих чисел можна скористатись додатковими інструкціями процесора, кількість яких постійно збільшується.

Література: ***1.*** *А. В. Потий, О. И. Олешко. Новые требования и принципы разработки современных алгоритмов блочного шифрования (по результатам анализа алгоритмов-кандидатов в AES)// Открытые информационные и компьютерные технологии. 2000. Вып. 12. С. 30 - 45.* ***2.*** *Вильям Столлингс. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Издательский дом "Вильямс", 2001. – 452 с.* ***3.*** *Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448с.* ***4.*** *Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin. The RC4 Block Cipher, version 1.1 – 04. 1998*

УДК 681.3.067:681.3.016

МЕТОДИКА СОЗДАНИЯ ГЕНЕРАТОРОВ ПЕРИОДИЧЕСКИХ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Тарас Левченко
Национальный банк Украины

Аннотация. **Исследована возможность использования решений однородных линейных уравнений с формальными производными как генераторов периодических битовых последовательностей. Предложена методика синтеза таких генераторов. Даны рекомендации по применению методики.**
Summary. **There is investigated possibility to exploring the linear boolean equations as a periodic bits sequences generators. There is proposed methodology for such generator synthesis. There are given recommendations on application of a methodology.**
Ключевые слова: **формальная производная, разностное уравнение, псевдослучайные последовательности.**

Безопасное функционирование информационных систем в банковской сфере Украины, помимо прочих факторов [1], связано с надежной высокоскоростной генерацией битовых последовательностей, используемых для криптозащиты [2]. Существует несколько способов генерации статистически удовлетворительных битовых последовательностей [3] с некоторым, обычно весьма большим, периодом. В