УДК 681.322

Ю. В. Нагорняк, асп.;
Ю. В. Дементьєв, к. т. н., доц.

ВДОСКОНАЛЕННЯ БЛОЧНОГО АЛГОРИТМУ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ RC-5 ТА ОЦІНКА ЙОГО ЕФЕКТИВНОСТІ

Подано варіант класифікації криптографічних алгоритмів, детально розглянуто блочний алгоритм RC-5, визначено його основні недоліки та показано шляхи їх усунення у модифікованому алгоритмі, а також проаналізовано вимоги, що висуваються до криптографічних алгоритмів та запропоновано оригінальні критерії визначення їх якості.

Вступ

Інформація є одним з основних понять сучасного життя. Її створюють, зберігають, транспортують, продають і купують. Тому постає питання її захисту. В останні десятиліття відбувся бурхливий розвиток електронної техніки. Тому нині слово інформація часто асоціюється з її електронною формою, де інформація подається та передається у вигляді електромагнітних сигналів та параметрів. Часто виникає необхідність захистити саме таку інформацію від небажаного доступу. Перш за все це стосується секретної державної інформації, військової та комерційної інформації, інформації в банківських мережах, проте навіть пересічний громадянин часто бажає захистити електронну інформацію, якою він володіє. Так, в багатьох розвинутих країнах існують спеціальні відомства, які мають повноваження перехоплювати електронні повідомлення. Одним з можливих шляхів вирішення зазначеної проблеми є криптографічний захист інформації. Для цього можна було б використати відомий закордонний програмний криптографічний засіб, що вбудований в популярні офісні програми чи поштові клієнти. Проте, існує думка, що американські компанії, що бажають продавати за кордоном свою криптографічну продукцію, на вимогу АНБ переробляють використані криптографічні алгоритми таким чином, що:

— час від часу окремі біти ключа підмішуються в шифртекст;

— ключ має меншу довжину, ніж заявлено офіційно;

— в початок кожного шифрованого повідомлення вставляється фіксований заголовок — чи фрагмент відкритого тексту що полегшує криптоатаку зі знанням відкритого тексту;

Така ситуація створює необхідність розробки власних криптографічних засобів захисту інформації.

Класифікація криптографічних засобів захисту інформації

Всі криптографічні засоби захисту інформації можна поділити на програмні, програмно-апаратні та апаратні. Перевагами апаратних та програмно-апаратних засобів перед програмними є вища швидкість шифрування, простіша реалізація захисту від випромінювання електромагнітних хвиль, ширші межі використання. Кожний з таких засобів захисту інформації функціонує на основі певного криптографічного алгоритму. Існує два основних класи криптографічних алгоритмів: симетричні, які використовують той самий ключ в процесі як шифрування, так і розшифрування, і асиметричні, в яких використовується два різних, проте певним чином пов'язаних між собою ключі. Кожний з цих способів шифрування має свої переваги і недоліки та свою сферу застосування.

В залежності від характеру впливу на дані алгоритми поділяються на:

— переставні, де блоки інформації (байти, біти, більш великі одиниці) не змінюються, а лише змінюється порядок їх слідування, що робить інформацію недоступною для використання;

— підставні, де блоки інформації змінюються за законами криптоалгоритму. Переважна більшість сучасних алгоритмів належить саме до цієї групи;

У залежності від розміру блока інформації криптоалгоритми поділяються на:

— потокові шифри: відкритий текст M розбивається на байти або біти m_1, m_2.... m_n і криптографічне перетворення застосовується до кожного елемента m_i у відповідності до елемента ключового потоку k_i. Результат кодування не залежить від попереднього вхідного потоку. Така схема застосовується в системах передачі потоків інформації, тобто в тих випадках, коли передача інформації починається і закінчується в довільні моменти часу і може випадково переривatися;

— блокові шифри: відкритий текст M розбивається на послідовні блоки M_1, M_2... M_n і криптографічне перетворення застосовується до кожного блока. Схема застосовується для пакетної передачі інформації і кодування файлів [1].

Постановка проблеми

Була поставлена задача розробити алгоритм шифрування електронної інформації, який буде забезпечувати високу стійкість до лінійного та диференційного криптоаналізу з невеликою кількістю операцій перетворень та буде придатний до програмно-апаратної реалізації.

В якості прототипу взято симетричний алгоритм шифрування RC5. Це блочний шифр, розроблений Роном Рівестом для RSA laboratories. Шифрування полягає в почерговому перетворенні підблоків з використанням операцій циклічного зсуву, операцій додавання за модулем 2, які виконуються над двома підблоками, і операції додавання за модулем 2^b (де b — довжина підблока даних) які виконуються над підблоком і підключем. [2]

Спосіб здійснюється таким чином:

1. Задають число раундів r і довжину підблока b;
2. Формують ключ шифрування у вигляді сукупності підключів — $K_0, K_1, \ldots, K_{2r+2}$;
3. Розбивають блок даних на два b-бітових підблока — A і B;
4. Виконують перетворення:

$$A := (A + K_0) \bmod 2^b; \qquad B := (B + K_1) \bmod 2^b;$$

5. Проводять r раундів перетворень:

$$A := \left(\left(A \oplus B\right) << B\right) + K_{2i} \bmod 2^b; \quad B := \left(\left(B \oplus A\right) << A\right) + K_{2i+1} \bmod 2^b.$$

Результати досліджень

Було проведено аналіз алгоритму RC5, в ході якого виявлені такі недоліки:

— В даному алгоритмі, для малої кількості раундів шифрування, є можливість часткового розкриття зашифрованого тексту у разі використання ключа близького до справжнього. Це призводить до необхідності проведення багатьох раундів шифрування (зазвичай 12 і більше).

— В розглянутому алгоритмі варіанти операцій циклічного зсуву відрізняються величиною зсуву від 0 до $b - 1$ двійкових позицій, тобто на керовану операцію циклічного зсуву мають вплив лише $\log_2 b$ молодших бітів керувального блоку (кількість бітів необхідна для двійкового представлення числа b).

— Даний спосіб не має достатньої стійкості до диференційного і лінійного криптоаналізу, оскільки тут для будь-яких вхідних блоків даних використовуються ті самі підключі [3].

Для усунення виявлених недоліків прототипу впроваджено таке:

— Здійснюється модифікація таємного ключа для кожного наступного блока даних в залежності від поточного блока за допомогою операцій додавання за модулем 2 та операцій керованого циклічного зсуву, що виконуються над підключем і підблоком даних. Таке рішення дозволяє використовувати інший ключ для кожного нового блока даних.

— В якості першого блока даних використовується випадкове число, що разом з міжблоковою модифікацією таємного ключа підвищує криптостійкість у разі зіставлення зашифрованого тексту з відкритим.

— В процесі шифрування здійснюється керований циклічний зсув підблоків даних в залежності від просумованих за модулем 2 усіх підключів. Це дозволяє уникнути часткового розшифрування

інформації в разі використання ключа, що близький до справжнього, у випадку, якщо кількість раундів шифрування невелика.

— Під час виконання операцій керованого циклічного зсуву вліво, зсув здійснюється на значення просумованих за модулем 2 байтів керувального операнда. Таким чином, всі біти керувального блока мають вплив на операцію перетворення.

В створеному алгоритмі для досягнення необхідної криптостійкості достатньо проведення трьох раундів шифрування (в RC5 — 12). Таким чином для шифрування одного блока даних виконується 66 операцій перетворення над b-бітовими підблоками, порівняно з 74 в RC5.

Розроблений алгоритм реалізується таким чином:

1. Задають довжину підблока b та кількість раундів шифрування r.

Вхідні дані розбивають на n – 1 блоків, довжиною 2b біт.

Генерують випадковий блок даних, та вставляють його перед блоками вихідних даних.

Представляють початковий ключ шифрування як сукупність чотирьох b-бітових підключів K_1, K_2, K_3, K_4.

5. Проводять шифрування n блоків даних (випадковий блок та n – 1 блоків відкритого тексту).

Шифрування блока даних здійснюється в такій послідовності:

1. Вхідний блок даних розбивають на два b-бітових підблока — A і B.

2. Визначають ключ, що буде використовуватися для наступного блока даних за такими співвідношеннями:

$$K_1(t+1) := \left(K_1(t) \oplus A\right) << \Sigma B; \quad K_2(t+1) := \left(K_2(t) \oplus B\right) << \Sigma A;$$

$$K_3(t+1) := \left(K_3(t) \oplus A\right) << \Sigma B; \quad K_4(t+1) := \left(K_4(t) \oplus B\right) << \Sigma A;$$

де t — номер блока даних.

3. Перетворюють підблоки A і B за співвідношеннями

$$A := \left(\left(A + K_1\right) \bmod 2^b\right) << \sum\left(K_1 \oplus K_2 \oplus K_3 \oplus K_4\right);$$

$$B := \left(\left(B + K_2\right) \bmod 2^b\right) << \sum\left(K_1 \oplus K_2 \oplus K_3 \oplus K_4\right);$$

4. Проводять r раундів перетворень підблоків:

$$A := \left(\left(A << \sum B\right) + K_3\right) mod\, 2^b; \quad B := \left(\left(B << \sum A\right) + K_4\right) mod\, 2^b.$$

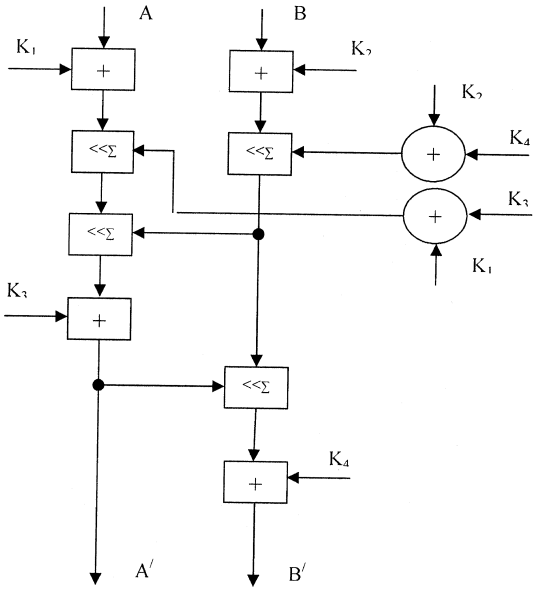

Рис. 1. Структурна схема одного раунду шифрування модифікованим алгоритмом

На рисунках 1 та 2 графічно зображено структуру одного раунду шифрування та міжблокової модифікації ключа шифрування.

Розробка будь-якого шифру передбачає оцінку його стійкості до різноманітних типів криптографічних атак. Здатність криптосистеми протистояти атакам криптоаналітика називається стійкістю. Кількісно стійкість виміряється як складність найкращого алгоритму, що приводить криптоаналітика до успіху, з прийнятною імовірністю. В залежності від цілей і можливостей криптоаналітика змінюється і стійкість. Розрізняють стійкість ключа (складність розкриття ключа найкращим відомим алгоритмом), стійкість безключового читання, імітостійкість (складність нав'язування помилкової інформації найкращим відомим алгоритмом). Аналогічно можна розрізняти стійкість власне криптоалгоритму, стійкість протоколу, стійкість алгоритму генерації і поширення ключів. Рівень стійкості залежить як від можливостей криптоаналітика, так і від користувача. Так, розрізняють криптоаналіз на основі лише шифрованого

тексту, коли криптоаналітик володіє тільки набором шифрограм і не знає відкритих текстів, і криптоаналіз на основі відкритого тексту, коли криптоаналітик знає відкриті та відповідні шифровані тексти.

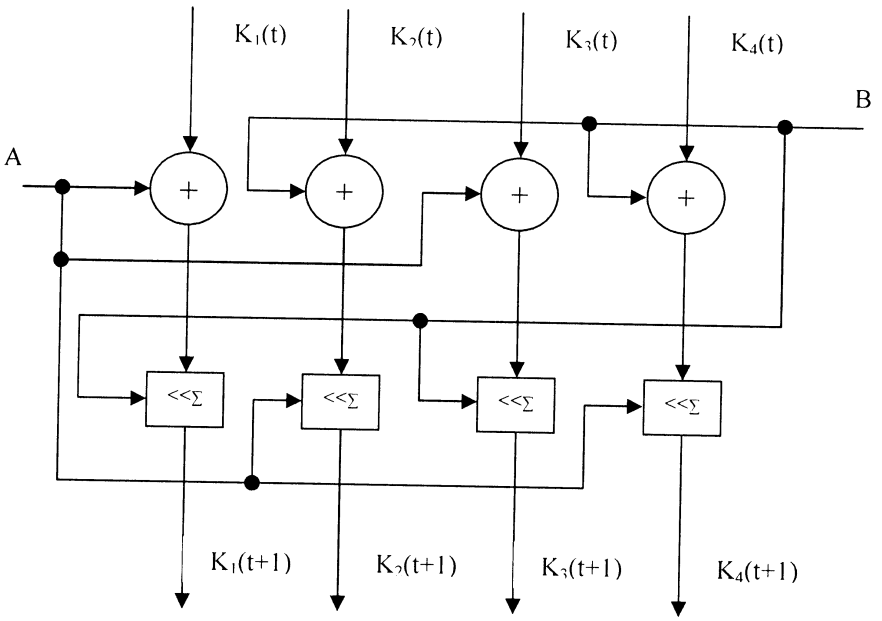

Рис. 2. Структурна схема міжблокової модифікації ключа шифрування

Рівень стійкості залежить як від можливостей криптоаналітика, так і від користувача. Так, розрізняють криптоаналіз на основі лише шифрованого тексту, коли криптоаналітик володіє тільки набором шифрограм і не знає відкритих текстів, і криптоаналіз на основі відкритого тексту, коли криптоаналітик знає відкриті та відповідні шифровані тексти.

Більшість блочних шифрів (DES, RC5, ГОСТ та ін.) є вразливими до криптоаналізу на основі формування випадкових апаратних помилок (ВАП), тому використовуючи їх, необхідно забезпечити захист апаратури від нав'язування збоїв. Це вид нападу на шифри у випадку, коли передбачуваний порушник має можливість здійснення на шифратор зовнішнього фізичного впливу, викликаючи таким чином одиничні помилки в процесі шифрування блока даних. Розгляд питання стійкості до цього типу атак особливо актуальний для шифраторів, що використовуються в інтелектуальних електронних картках. Тому виникає необхідність передбачити захист у самому алгоритмі [3, 4].

Критеріями якості блочних криптографічних алгоритмів можуть слугувати такі показники:

— ступінь впливу зміни ключа шифрування на зміну шифртексту;

— ступінь впливу зміни відкритого тексту на зміну шифртексту;

— випадковість послідовності символів шифрованого тексту.

Вказані показники, можна легко отримати провівши статистичний аналіз відкритого та зашифрованого текстів. Для якісних криптоалгоритмів навіть незначна модифікація ключа шифрування чи відкритого тексту має значно відображатися на результаті шифрування, а характеристики шифртексту мають бути близькими до випадкового набору. Індикатором випадковості шифртексту може слугувати ступінь його стиснення. Так, текст, шифрований якісним криптографічних алгоритмом, стиснути практично не вдається.

Крім того, такий підхід дає ще одну перевагу. Стиснення проведене перед шифруванням, дозволяє позбутися надлишковості, що властива будь-якому відкритому тексту та зменшити його довжину і, відповідно, скоротити час шифрування та ускладнити криптоаналіз [5].

Для проведення статистичного аналізу алгоритм RC-5 та модифікований алгоритм були реалізовані програмно в середовищі Delphi та використанні для шифрування довільного тесту. При цьому проводилася модифікація бітів ключа шифрування та відкритого тексту (від 1...256 біт) і фіксувалася

зміна елементів шифртексту. Стиснення шифрованих повідомлень перевірялася за допомогою відомого архіватора WinRar при архівації з однаковими параметрами. Результати дослідження показали, що модифікований алгоритм має в середньому на 5—10 % кращі статистичні показники, ніж його прототип RC-5. В створеному алгоритмі використовуються лише такі операції, які швидко виконуються на звичайних процесорах, тому він добре підходить як для програмної, так і для програмно-апаратної реалізації.

Висновки

В результаті проведених досліджень визначено основні недоліки симетричного блочного алгоритму RC-5 та розроблено методи їх усунення. Запропоновано оригінальні статистичні критерії оцінювання ефективності криптографічних алгоритмів, що легко визначаються на практиці. Для підвищення швидкості шифрування та стійкості до криптоаналізу пропонується шифрування проводити разом з стисненням. Здійснений порівняльний аналіз криптоалгоритму RC-5 та модифікованого алгоритму за вказаними критеріями показав переваги створеного алгоритму.

СПИСОК ЛІТЕРАТУРИ

1. Ярочкин В. И. Информационная безопасность: Учебник для вузов. — М.: Фонд «Мир» и изд-во «Академический проспект», 2003.

2. R. Rivest. The RC5 Encryption Algorithm, Fast Software Encryption, Second International Workshop Proceedings (Leuven, Belgium, December 14—16, 1994) Lecture Notes in Computer Sciens, v.1008, Springer-Verlag, 1995.

3. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. — NY: Springer-Verlag, 1993.

4. Matsui M. Linear Cryptanalysis Method for DES Cipher. — Advances in Cryptology-EUROCRYPT '93 Proceedings. — NY: Springer-Verlag, 1994.

5. Pippenger N. Entropy and Enumeration of Boolean function // IEEE Transactions and information theory. 1999. Vol. 45. — № 6. — P. 2096—2100.

Матеріали статті рекомендовані до опублікування оргкомітетом конференції «Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування» (2—5. 07.05)

Надійшла до редакції 11.07.05
Рекомендована до друку 21.07.05

Нагорняк Юрій Васильович — аспірант; ***Дементьєв Юрій Вікторович*** — доцент.

Кафедра проектування комп'ютерної та телекомунікаційної апаратури

Вінницький національний технічний університет