УДК 004.056.55

А. О. Душко

АЛГОРИТМ ПОТОКОВОГО ШИФРУВАННЯ ДАНИХ МЕТОДОМ ПСЕВДОНЕДЕТЕРМІНОВАНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Вінницький національний технічний університет

Анотація

Проаналізовано застосування генераторів псевдовипадкової послідовності в алгоритмах шифрування. Запропоновано новий спосіб генерування гами у засобі захищеного обміну даними, що побудований на основі псевдонедетермінованих криптографічних перетвореннях.

Ключові слова: псевдонедетермінований, криптографічні перетворення, шифрування даних, алгоритм.

Abstract

The application of pseudo-random sequence generators in encryption algorithms is analyzed. A new method of gamma generation in secure data exchange means based on pseudo - indeterminate cryptographic transformations is proposed.

Keywords: pseudonondeterministic, cryptographic transformations, data ciphering, algorithm.

Вступ

Сучасні алгоритми потокового шифрування даних, які використовують для їх захисту у засобах обміну інформацією, мають відносно просту реалізацію та стійкий захист. Але вони, попри всі переваги, зустрічаються з проблемами, що пов’язані з криптографічними атаками. Алгоритми потокового шифрування даних, які використовуються у засобах обміну даними, є детермінованими, а тому, потребують удосконалення для підвищення складності реалізації криптоаналізу шифру для зловмисника [1, 2]. Ідеї, закладені у генераторах псевдовипадкової послідовності, що лежать в основах таких алгоритмів, можуть бути використані для реалізації концепції псевдонедетермінованого потокового шифрування [2, 3]. Тому актуально розробити такий алгоритм потокового шифрування, який врахує концепцію псевдонетермінованого криптографічного перетворення.

Метою даного дослідження є підвищення складності криптоаналізу методу шифрування за допомогою використання псевдонедетермінованих криптографічних перетворень.

Для досягнення мети необхідно розв’язати такі задачі:

- проаналізувати сучасні методи потового шифрування;
- проаналізувати концепцію псевдонедетермінованих криптографічних перетворень;
- розробити алгоритм накладання гами;
- розробити алгоритм генерування гами;
- проаналізувати доцільність застосування удосконаленого методу потокового шифрування даних у засобі захищеного обміну даними на основі псевдонедетермінованих криптографічних перетворень.

Аналіз методів потокового шифрування даних

Серед систем, що виконують функцію криптоперетворення інформації, особливе місце посідають потокові шифри, в яких дані подаються та обробляються у вигляді нескінченного потоку або послідовності, яка гіпотетично може бути нескінченною.

Потоковий шифр повинен забезпечувати необхідний рівень швидкодії, функціонувати на різних платформах та, найголовніше, забезпечувати високий рівень криптографічної стійкості. Серед сучасних алгоритмів шифрування слід виділити наступні: Trivium, Sosemanuk, Rabbit, Геффе [4-7].

Trivium – апаратно орієнтований паралельний потоковий шифр, що має можливість програмної реалізації. Головна ідея Trivium – це компактність в середовищі з обмеженими вхідними параметрами,

енергоефективність на платформах з малими джерелами енергії, а також швидкодія в застосунках, що потребують високошвидкісного шифрування даних. Компактна реалізація даного шифру передбачає бітово-орієнтований підхід, що також обумовлює використання нелінійного внутрішнього стану, для того, щоб не витрачати нелінійність на виході генератора [4].

Rabbit – високошвидкісний програмно орієнтований потоковий шифр. Початково Rabbit було розроблено, надаючи пріоритет швидкодії над стійкістю [5], тому з точки зору мети даного дослідження він потребує удосконалення.

Sosemanuk – відносно новий синхронний програмно-орієнтований потоковий шифр зі змінною довжиною ключа [6]. Розробники Sosemanuk в ході реалізації даного алгоритму передбачили можливість різних атак на шифр, а тому забезпечили його захист та зробили стійким до цих атак. Хоча через декілька років все ж з'явилися нові атаки до яких шифр може бути нестійким [6].

Структура генератора Геффе використовує три РЗЛЗЗ [7]. Це генератор, що використовує нелінійне перетворення з об'єднанням декількох РЗЛЗЗ. РЗЛЗЗ 2 та 3 слугують входами мультиплексора, а РЗЛЗЗ 1 керує виходом мультиплексора. Довжини кожного з регістрів це попарно прості числа. За рахунок нелінійності даного генератора та об'єднання декількох регістрів, такий генератор може підвищити криптографічну стійкість системи в якій використовується.

Проаналізовані шифри можуть бути удосконалені на основі концепції псевдонедетермінованої криптографії. Методи криптографічних перетворень виглядають для зловмисника як такі, що виконуються за допомогою недетермінованого автомата [2, 8]. Недетермінованим є автомат, правила переходу якого представлено відображенням, яке не обов'язково передбачає функціональну залежність у правилі переходу автомата з одно стану до іншого [2, 3, 8, 9].

Нехай ε – порожнє повідомлення, тоді недетермінований автомат описується у вигляді п'ятірки $\{S, A, \delta', s_0, D\}$, де δ' – відображення $S \times (A \cup \{\varepsilon\}) \to S$, де S – множина станів автомата; A – вхідний алфавіт; s_0 – виокремлений стан автомата, що називається початковим ($s_0 \in S$); D – підмножина в S, що називається множиною завершальних станів [2, 3, 9]. Відповідно поняття псевдонедетермінованого криптографічного перетворення, аналогічно до поняття псевдовипадкових чисел, передбачає, що дане перетворення для стороннього спостерігача (зловмисника) має такий вигляд, наче воно виконується недетермінованим автоматом [1-3, 8]. Однак для спостерігача, який знає правило, що відіграє роль своєрідного ключа, виконане перетворення виглядає, як таке, що виконується детермінованим автоматом. З наведених вище визначень випливає, що дана задача розв'язується шляхом заміни відображення δ, яке є однозначним, тобто δ – функція, на відображення δ', яке не обов'язково є однозначним [2, 8].

Для впровадження концепції псевдонедетермінованих криптографічних перетворень обрано алгоритм потокового шифрування відповідно до схеми Геффе, оскільки він початкового передбачає внесення деякої невизначеності для зловмисника щодо способу генерування гами, що є природним для даної концепції.

Алгоритм потокового шифрування даних

Розробка алгоритму псевдонедетермінованого потокового шифрування (рис.1) передбачає декомпозицію задачі на такі складові [10]:

- генерування гами;
- накладання гами;
- забезпечення псевдонедетермінованості процедур генерування та накладання гами.

Остання процедура може бути виокремленою або інтегрованою в тіло інших процедур [10]. В межах даного дослідження обрано шлях інтеграції в тіло інших процедур, оскільки керування параметрами даних процедур відбувається незалежно одна від одної.

Процес захисту даних відбувається шляхом генерування гами (G) та накладання її на відкрите повідомлення (P). Генератор гами побудований подібно до генератора Геффе, у якому використовується три регістри зсуву. Для початку роботи самого алгоритму йому потрібно отримати вхідні дані: ключ та відкрите повідомлення, яке потрібно захистити.

Сам процес шифрування повідомлення буде здійснено шляхом накладання на нього згенерованої гами, відповідно до концепції псевдонедетермінованих криптографічних перетворень [1, 2].

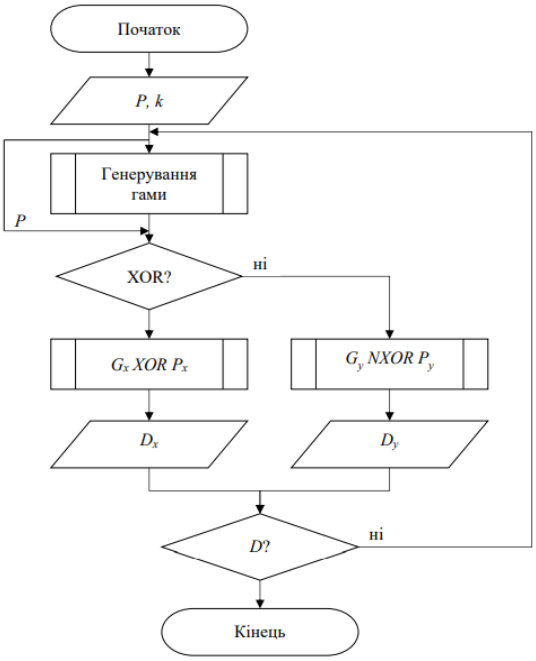

Рисунок 1 – Алгоритм потокового шифрування

Ключ k розділяється на 4 частини по 32 біта, які заповнюють початкові стани усіх регістрів генератора гами. Повідомлення також розділяється на дві частини, відповідно до того, яка операція між P та G має бути виконана. Обрані частини гами та повідомлення надходять до відповідних блоків XOR чи NXOR, де і виконується накладання відповідних бітів за заданою операцією [3]. На виході буде отримано частини зашифрованого повідомлення D_x та Dy, які поєднуються в одну послідовність. Якщо повідомлення було зашифроване не повністю, то генерується наступні біти гами і накладаються на повідомлення доти, доки не буде сформовано одну зашифровану послідовність D.

Найважливішою складовою алгоритму потокового шифрування є процедура генерування гами. Під час виконання цієї процедури ключ розділяється на 4 рівні частини. Четверта частина йде до генератора ітерацій s. А перші три частини заповнюють початкові стани регістрів для генерації гами-послідовності. Далі відбувається процес генерування двох бітів гами-послідовності (рис. 2).

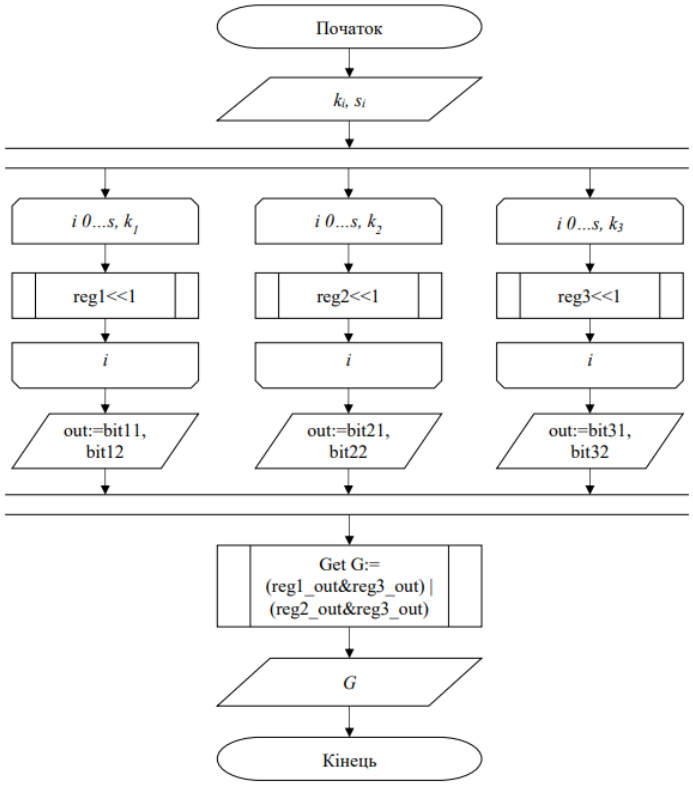

Рисунок 2 – Алгоритм генерування двох бітів гами-послідовності

Два біти, що сформувалися внаслідок роботи генератора ітерацій s, визначають яка буде кількість перебору станів для кожного регістра. Після того, як згенерувалися останні стани регістрів, на блок

формування гами потрапляють лише два біти. Даний блок містить біти спочатку від третього регістру, далі до нього потрапляють біти від першого та другого регістрів. Далі визначається, які саме біти підуть далі у гаму: вихідні біти з третього регістру визначають, які біти з першого чи з другого регістру підуть далі. Після отриманих бітів від відповідного регістру формується так звана гама, яка містить в собі біт гами та біт, що визначає тип операції накладання G на P.

Таким чином буде отримано псевдовипадкову послідовність – гаму, яка є найважливішою складовою для подальшого перетворення повідомлення.

Висновки

Розроблений алгоритм шифрування даних дозволить досягти підвищеної захищеності даних при їх передачі між користувачами. Процедура генерування гами, яка є основою всього алгоритму, побудована таким чином, щоб щоразу по-різному генерувати біти послідовності гами відповідно до концепції псевдонедетермінованих криптографічних перетворень. А за рахунок визначення певної операції накладання буде створено невизначеність для зловмисника у виконуваному перетворенні, що ускладнить процес криптоаналізу запропонованого алгоритму. Реалізація даного алгоритму шифрування у засобі обміну даними, дозволить легко та безпечно користувачам обмінюватися інформацією, а її цілісність та достовірність не буде порушена.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лужецький В. А., Баришев Ю. В. Концепція псевдонедетермінованого хешування. *Системи управління, навігації та зв'язку*. Київ, 2010, №3. С. 94-98.
2. V. Luzhetskyi, Y. Baryshev, V. Derech. Pseudononderterministic Approach of Control Systems Cryptographic Protection. Information Technology in Selected Areas of Management 2017. Krakow: AGH University of Science and Technology Press. 2018. P. 25-38.
3. Душко А. О., Баришев Ю. В. Засіб захищеного обміну даними на основі псевдонедетермінованих криптографічних перетворень. *XLIX науково-технічної конференції підрозділів ВНТУ*: матеріали доповідей (18-29 травня 2020). Вінниця, 2020. 3 с. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/9327/7593 (accessed 23.11.2020)
4. Good T., Chelton W., Benaissa M. Review of stream cipher candidates from a low resource hardware perspective. UK: Department of Electrical & Electronic Engineering University of Sheffield, 2006. 24 p. URL: https://www.ecrypt.eu.org/stream/papersdir/2006/016.pdf (accessed 25.11.2020)
5. Boesgaard M., Vesterager M., Christensen T., Zenner E. The Stream Cipher Rabbit. Denmark. 30 p. URL: https://www.ecrypt.eu.org/stream/p3ciphers/rabbit/rabbit_p3.pdf (accessed 25.11.2020)
6. Ahmadi H., Eghlidos T., Khazaei S.. Improved Guess and Determine Attack on Sosemanuk. Iran: Tehran, 2005. 8 p. URL: https://www.ecrypt.eu.org/stream/papersdir/085.pdf (accessed 25.11.2020)
7. Глинчук Л. Я. Криптологія: навчально-методичний посібник. Луцьк: ВежаДрук, 2014. 164 с.
8. Luzhetsky V., Baryshev Y. The Generalized Construction of pseudononderterministic hashing. *Computing*, Ternopil, 2012. Vol. 11. Issue 3. P. 302-308.
9. Андерсон Дж. А. Дискретная математика и комбинаторика : Пер. с англ. Москва, Издательский дом «Вильямс», 2004. 960 с.
10. Баришев Ю. Структури операційних пристроїв для реалізації псевдонедетермінованих криптографічних перетворень. *Інформаційні технології та комп'ютерне моделювання*: матеріали Міжнародної науково-практичної конференції, 23-28 травня 2016 року. Івано-Франківськ, 2016. С. 109-110.

Душко Аліна Олександрівна – студент, факультет інформаційних технологій та компютерної інженерії, Вінницький національний технічний університет, Вінниця, email: dushko483@gmail.com.

Науковий керівник - ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, email: yuriy.baryshev@vntu.edu.ua.

Dushko Alina – student, Faculty of Information Technology and Computer Engineering, Vinnytsa National Technical University, Vinnytsia, email: dushko483@gmail.com.

Baryshev Yurii – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, email: yuriy.baryshev@vntu.edu.ua.