УДК 004.056.55: 004.421.5

І.О. РОЗЛОМІЙ
Черкаський національний університет імені Богдана Хмельницького

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ МОДИФІКАЦІЄЮ ШИФРУ ГАМУВАННЯ

Широке впровадження інформаційних систем обміну даними потребує забезпечення захисту конфіденційної інформації. Стаття присвячена розгляду проблеми забезпечення інформаційної безпеки електронних документів. Розглянуті особливості процесу шифрування та дешифрування інформації. Досліджено принципи використання псевдовипадкових послідовностей чисел в криптографії, зокрема в шифруванні методом гамування. Побудовано схему алгоритму криптографічних перетворень даним методом. Проведено аналіз основних властивостей та вимог шифру гамування, які впливають на криптографічну стійкість. Запропонований новий метод побудови криптографічних систем з використанням вдосконаленого шифру гамування на основі випадкових чисел. Показано схему модифікованого алгоритму шифрування методом накладання гами.

Ключові слова: шифрування, шифр гамування, псевдовипадкові числа, сума за модулем, криптографічна стійкість.

I.O. ROZLOMII
Cherkassy Bogdan Khmelnytsky National University

IMPROVING EFFICIENCY OF PROTECTION OF DIGITAL DOCUMENTS WITH MODIFICATION OF THE STREAM CIPHER

The aim of this work is to develop an effective method of increasing the level of information security of digital documents by modifying a stream cipher. The widespread of the information systems for data exchange deployed needs to protect of confidential information. In the article we explored some features of the encryption and decryption of information. Study of the principles of using pseudorandom sequence of numbers in cryptography was conducted, including a method with using the stream cipher. The schema of the cryptography algorithm of this method was developed. Main features and requirements of the stream cipher which affect the cryptographic strength of it were analyzed. The new method of building the cryptography systems with the use of improved stream cipher based on random numbers was suggested. Based on the conducted research, a schema of modified cipher algorithm with the application of gamma was built, and the main principles of its functioning were described.

Keywords: encryption, stream cipher, pseudorandom numbers, XOR, cryptography strength.

Вступ. У зв'язку з інтенсивним впровадженням, майже в усі сфери діяльності людини, автоматизованих систем обміну конфіденційною інформацією виникає необхідність її захисту. Все більша частина інформації, яка є інтелектуальною власністю, обробляється і зберігається в електронному вигляді. Одним з критеріїв функціонування сучасної держави є наявність захищеного, динамічно розвинутого інформаційного простору. Інформаційна безпека (ІБ) є одним із основних напрямків забезпечення надійності функціонування будь-якої організаційної структури. Захист інформації представляє собою комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Поняття ІБ включає здатність системи зберігати свою цілісність і працездатність за умов можливого негативного впливу і досягається шляхом проведення відповідного рівня політики безпеки.

Особливо актуальною ця проблема є по відношенню до систем електронного документообігу. Захист електронних документів (ЕД) є актуальним для різних задач: захист документообігу промислових підприємств, забезпечення конфіденційності інформації в медичних закладах, захист ЕД, що забезпечують функціонування платіжних мереж в банківській сфері [1]. Питання захисту ЕД не можуть бути повністю вирішеними лише стандартним набором засобів захисту інформації. Тому використання інформаційних технологій призвело до розвитку різноманітних методів захисту інформації, серед яких можна виділити кодування та криптографію.

Постановка проблеми. Зростаюча потреба в надійному захисті електронних документів ставить безпрецедентні завдання перед комп'ютерною індустрією. За умов сучасного розвитку інформаційних технологій забезпечення надійно захищеного електронного документообігу є актуальною задачею. В основній більшості, системи захисту електронних документів базуються на засобах криптографії [2]. Недавні успіхи криптографії демонструють різноманітні способи вирішення питання захисту ЕД. Слід зауважити те, що деякі алгоритми шифрування характеризуються низькою швидкодією, або не відповідають вимогам криптографічної стійкості. До криптографічних алгоритмів зараз пред'являють жорсткі технологічні вимоги не лише по забезпеченню криптостійкості, а також щодо швидкості та простоти реалізації. В зв'язку з підвищенням вимог до сучасних криптосистем вдосконалення існуючих та розробка алгоритмів шифрування є першочерговим завданням забезпечення безпеки інформаційних ресурсів.

Аналіз останніх досліджень та публікацій. Останнім часом спостерігається великий інтерес до функціонування систем захищеного документообігу. Питаннями захисту ЕД займалася значна кількість науковців, серед яких варто відмітити праці Михерського Р.М., Астахової Т.С., Панасенка С.П., Авдошина С.М. та інших фахівців галузі інформаційної безпеки.

Виділення невирішених раніше частин загальної проблеми. Проте, більшість із запропонованих алгоритмів забезпечення ІБ не можуть повністю вирішити проблему захисту ЕД. Сучасні криптографічні

системи характеризуються дисбалансом між криптографічною стійкістю та ефективністю захисту. Не достатньо уваги приділяється створенню надійних швидкодіючих механізмів захисту.

Формулювання цілей статті. Метою роботи є підвищення рівня ІБ електронних документів. Для досягнення мети досліджено основні принципи та механізми шифрування. Визначено роль псевдовипадкових послідовностей чисел (ПВЧ) в криптографічних алгоритмах, способи отримання ПВЧ. Запропоновано новий метод побудови криптографічних систем з використанням вдосконаленого шифру гамування на основі випадкових чисел.

Виклад основного матеріалу дослідження. Забезпечення інформаційної безпеки є одним з пріоритетних напрямків розвитку інформаційних технологій. Коло завдань, що вирішуються в цій сфері, постійно розширюється, як в кількісному, так і якісному відношенні. Одним із основних засобів, що використовуються для захисту інформації в комп'ютерних системах є криптографічні перетворення. Криптографічні методи, безумовно, найнадійніший спосіб захисту інформації, оскільки захищається безпосередньо сама інформація, а не доступ до неї. Сучасні криптосистеми поділяють на криптосистеми з відкритим ключем – симетричні та з закритим ключем – асиметричні [3]. Всі існуючі криптографічні методи базуються на таких перетвореннях, як підстановки, перестановки, блочні шифри та гамування. Розробка сучасних алгоритмів захисту інформації потребує постійного вдосконалення і відповідності поставленим вимогам.

Постійний розвиток методів криптографічного аналізу не дозволяє довгий час використовувати криптосистему без її вдосконалень, які ускладнюють роботу криптоаналітика. Криптографічні системи модифікуються різними способами: збільшенням довжини ключа, за рахунок багатократного шифрування та іншими.

Для забезпечення захисту електронних документів (ЕД) використовуються різні криптографічні методи, що дозволяють перетворювати інформацію таким чином, що її зміст можна прочитати лише володіючи ключем шифрування. Шифрування сприяє забезпеченню основних властивостей ЕД, таких як: конфіденційність, цілісність та достовірність. Шифрування – процес перетворення відкритих даних в закриті за визначеними криптографічними правилами [4]. Дане перетворення в математичній формі можна представити у вигляді залежностей, які описують алгоритм шифрування (1) та дешифрування (2) інформації.

$$Z = Fk_1(T), \tag{1}$$

$$T' = Rk_2(Z), \tag{2}$$

де T– відкритий текст документу, Z– зашифрований текст, F– функція шифрування, яка виконує криптографічні перетворення над відкритим текстом за допомогою ключа шифрування k_1, T'– розшифрований текст, R– функція розшифрування, що виконує обернені криптографічні перетворення над зашифрованим текстом, використовуючи ключ розшифрування k_2. Найважливішою характеристикою будь-якого шифру є його криптографічна стійкість, яка відображає наскільки успішно алгоритм вирішує завдання шифрування. Крипостійкість – головна характеристика алгоритму шифрування, що говорить про складність отримання зловмисником вихідного тексту ЕД не володіючи ключем розшифрування [5].

В загальному вигляді алгоритм шифрування-дешифрування електронних документів можна показати таким чином (рис. 1).

Рис. 1. Алгоритм шифрування-дешифрування ЕД

Останнім часом великої популярності набули методи шифрування на основі використання послідовностей випадкових чисел. Насамперед, це пов'язано з легкою реалізацією, модифікацією та високою швидкодією таких шифрів [6]. ПВЧ грають в криптографії визначну роль, вони використовуються для формування ключових параметрів криптографічних алгоритмів, а також послідовностей шифруючих підстановок в криптосистемах. Датчики ПВЧ застосовуються в криптографічних протоколах для формування ключів, при хешуванні паролів, а також в симетричних системах захисту конфіденційної інформації. Криптографія і випадковість взаємопов'язані поняття, оскільки засобами криптографічних перетворень відкритий текст перетворюється в зашифровану послідовність випадкових символів. Для реалізації систем шифрування використовують ПВЧ, тому стійкість шифру в основному залежить від алгоритму формування випадкової послідовності.

Ідея використання ПВЧ знайшла своє застосування в шифрі гамування, в якому алгоритм генерації гами грає вирішальну роль. Одним з ефективних методів забезпечення захисту ЕД є застосування шифру гамування. Формально гамування можна віднести до класу шифрів багатоалфавітної заміни, але завдяки зручності реалізації і формального опису, шифри гамування широко використовуються і зазвичай їх виділяють в окремий клас [7]. На (рис. 2) показано схематичне зображення алгоритму шифрування-

розшифрування текстового документу методом гамування.

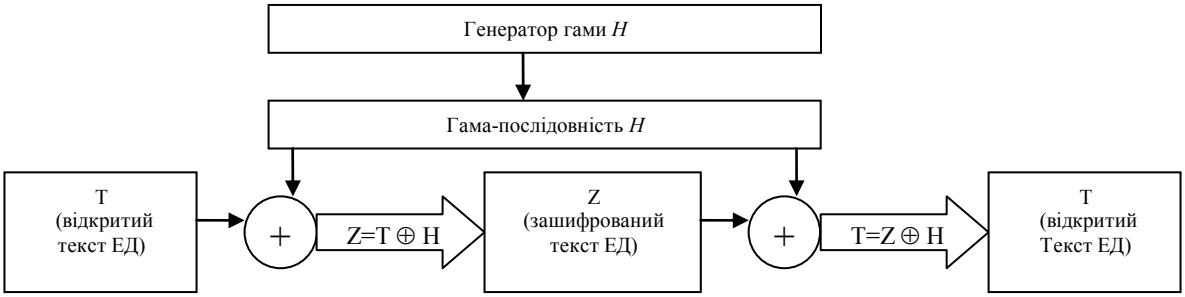

Рис. 2. Алгоритм шифрування-дешифрування тексту ЕД методом гамування

Суть даного методу полягає в накладанні на відкритий текст ЕД деякої псевдовипадкової послідовності – гами, що згенерована на основі ключа. Зазвичай, для генерації ПВЧ використовуються генератори ПВЧ (ГПВЧ), конгруентні датчики, датчики *M*-послідовностей, нелінійні датчики ПВЧ. Датчик ПВЧ генерує гаму, з визначеним періодом повтору, в залежності від вказаних параметрів і ключа, який може бути обраний будь-якого розміру. Лінійний конгруентний датчик генерує ПВЧ за модулем деякого натурального числа *m*, який задається формулою (3).

$$X_{k+1} = (aX_k + c) \bmod m, \tag{3}$$

де *a*, *c*, *m* – цілочисельні коефіцієнти, вибрані константи. Отримана послідовність залежить від обраного значення початкової величини X_0. Очевидно, що послідовність отримана за такою формулою матиме період, рівний *m*. При шифруванні великих об'ємів текстів періодичність призводить до зниження криптостійкості алгоритму.

Крім ГПВЧ, конгруентних датчиків, мають місце і інші, більш складні, варіанти отримання чисел для гами шифру. Відомий ряд ГПВЧ і з великими періодами, але кількість надійних генераторів досить невелика, що сприяє полегшенню відкриття зашифрованої інформації. Як альтернатива, замість псевдовипадкових, можна застосовувати квазівипадкові послідовності чисел. Такі послідовності не періодичні, що дозволяє використовувати їх для шифрування даних довільного розміру [8].

Принцип шифрування методом гамування досить простий – відкритий текст заміняється шифрованим текстом, шляхом накладання згенерованої гами на текст. Зазвичай, шифрувати доводиться документи різного розміру. Представимо відкритий текст ЕД довільного розміру у вигляді послідовності $\dot{O} = (t_1, t_2, ..., t_n)$, де $t_i \in [0,1]$ – операнди-розряди, символи відкритого тексту ЕД. Згенеровану, на основі секретного ключа *k,* гаму псевдовипадкових чисел представимо у вигляді послідовності $H = (h_1, h_2, ..., h_n)$, де $h_i \in [0,1]$ – символи гами. Шифрування методом гамування відкритого тексту, попередньо перетвореного в послідовність двійкових символів t_i, здійснюється шляхом додавання за модулем символів t_i з двійковими символами гами h_i.

$$Z = T \oplus H \tag{4}$$

Розшифрування тексту здійснюється аналогічним способом – накладанням гами *H* на зашифровану послідовність *Z*.

$$\dot{O} = Z \oplus H \tag{5}$$

Стійкість шифрування методом гамування залежить від довжини гами, а також ймовірності повтору її символів. Очевидно, найстійкішим гамування буде за таких умов: всі символи гами будуть повністю випадковими, з'являтимуться в рівній ймовірності і довжина гами має бути не меншою за довжину відкритого тексту. Фактично, якщо період гами перевищує довжину всього зашифрованого тексту і невідома жодна частина вихідного тексту, то шифр можна розкрити лише шляхом прямого перебору. Криптостійкість в такому разі визначається розміром ключа. Метод гамування є неефективним, якщо зловмиснику стає відомим фрагмент вихідного тексту і відповідна йому частина шифру. За допомогою операції XOR відкривається фрагмент ПВЧ, за допомогою якої відновлюється вся послідовність.

Зашифрований текст є достатньо складним для розшифрування, якщо гама не має бітових послідовностей, які повторюються. Гама шифру має змінюватися випадковим способом для кожного слова тексту окремо, щоб розшифрування стало складною проблемою для зловмисника.

Враховуючи умови забезпечення криптостійкості шифру гамування, даний алгоритм цілком можна використовувати для захисту ЕД. Метод гамування характеризується простотою виконання – додаванням символів за модулем два, що аналогічно логічній операції XOR [9]. Відповідно, в зворотному порядку, шляхом накладання гами на зашифрований текст, стане відомою інформація, яка була зашифрованою. Тому, при розробці криптографічних систем, необхідно передбачувати можливість розсекречування, перехоплення ключа шифрування. В традиційному шифруванні методом гамування біт за бітом символи відкритого тексту додаються за модулем два з символами гами-послідовності, як показано на (рис. 3).

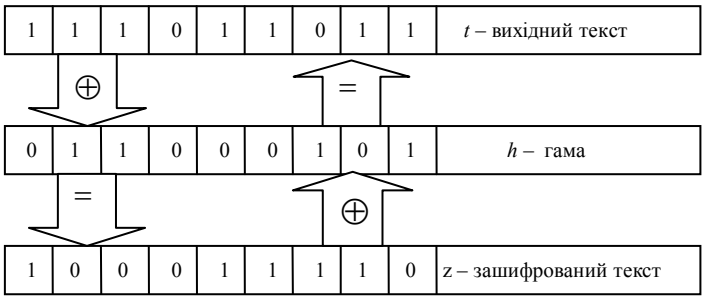

Рис. 3. Алгоритм прямого і зворотного накладання гами

З (рис. 3) видно, що шляхом додавання гами з символами зашифрованого тексту отримуємо початковий текст. Ускладнити завдання непередбаченого розшифрування даних можна шляхом модифікації шифру гамування. Суть вдосконаленого шифру гамування полягає в тому, що додавання символів відкритого тексту з випадковими числами відбувається не послідовно, як в традиційному шифруванні, а за певним принципом. Щоразу, коли в відкритому тексті, представленому у двійковій формі, зустрічається значення рівне нулю, в послідовності h відбувається зсув на один символ, тобто h_1 переміщується в кінець послідовності. Потім, додавання за модулем два вже відбувається починаючи з значення біта рівного нулю з символами нової гами h' до наступного біта із значенням нуль. Випадкова послідовність буде змінюватися стільки, скільки в послідовності вихідного тексту траплятиметься двійковий символ нуль, до тих пір, поки не буде зашифрований весь текст. Схематично, суть даного методу можна представити наступним чином (рис. 4).

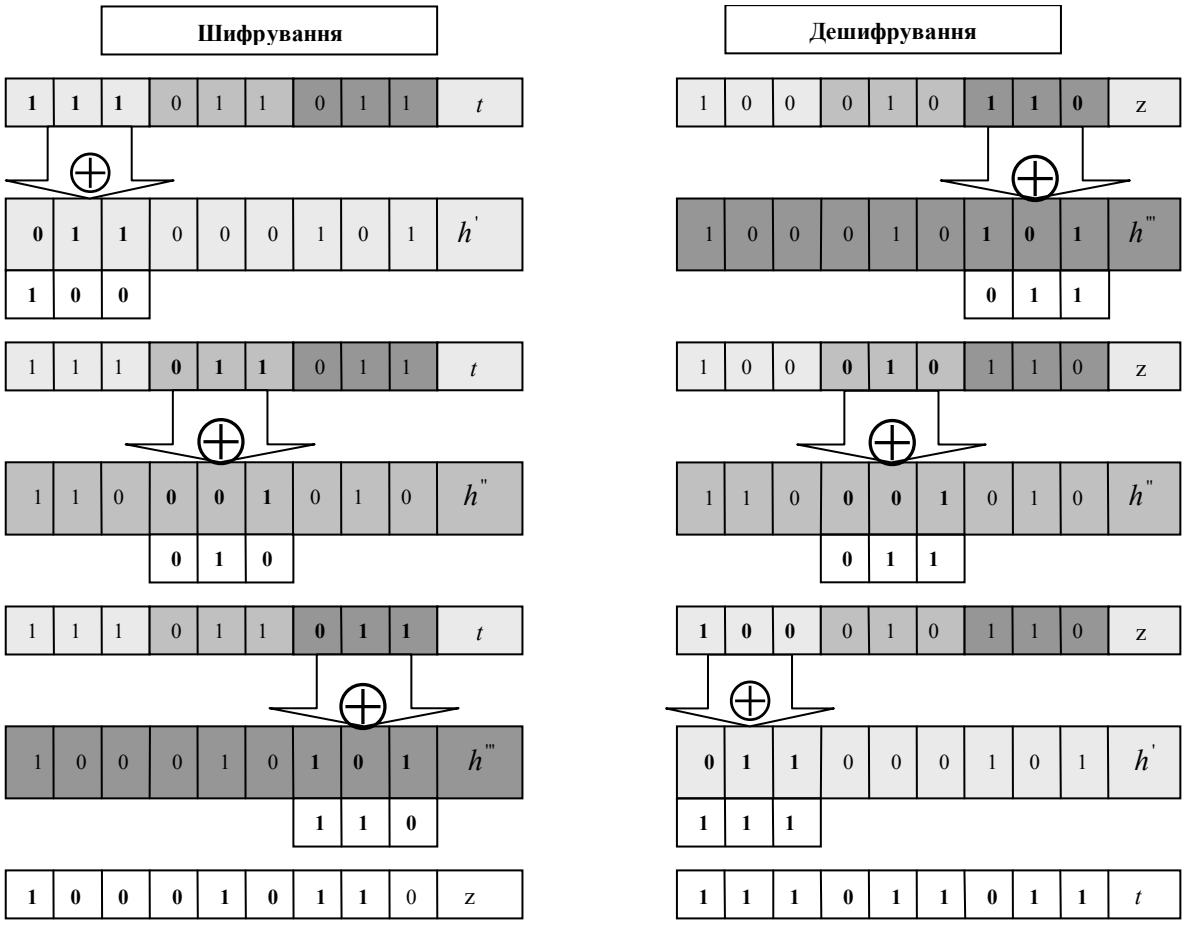

Рис. 4. Алгоритм шифрування-дешифрування модифікованим шифром гамування

З (рис. 4) видно, що четвертий біт тексту має значення рівне нулю – символи зміненої послідовності h' сумуються з символами відкритого тексту до наступного біта із значенням нуль. Знову відбувається зміщення символів шифруючої послідовності і, аналогічно, за допомогою операції суми за модулем два, символи гами додаються з символами відкритого тексту. В результаті отримуємо, зашифрований текст *Z*. Отриманий таким способом шифр-текст, відрізняється, від отриманого методом звичайного шифру гамування (рис. 3). З цього слідує, що зашифрована інформація стала складнішою для дешифрування, відповідно і більше захищеною.

Висновки

Активне використання технологій електронного обміну суттєво підвищило вразливість інформації, що циркулює в сучасних інформаційних системах. Криптографія залишається одним з найефективніших способів забезпечення ІБ. В статті запропонований новий метод побудови криптографічних систем з використанням вдосконаленого шифру гамування на основі випадкових чисел. Суть вдосконаленого методу полягає у зміні принципу накладання гами не послідовно, а з зміщенням символів шифруючої послідовності. Тобто, шифр, покращений за рахунок багатократного шифрування. Модифікований метод шифрування накладання гами здатний підвищити ефективність захисту ЕД. Описана концепція вдосконаленого методу шифрування може бути використана для розробки криптографічних систем захисту ЕД. Проте, не слід забувати один з фундаментальних принципів криптологічної практики, який говорить про те, що навіть складні шифри можуть бути чутливими до атак. Тому, не варто зупинятися на досягнутому, оскільки вимоги, щодо гарантування інформаційної безпеки, постійно зростають і вимагають швидкого їх вирішення.

Література

1. Штанько С. В. Криптографический протокол защиты информации в радиоканалах сетевых спутниковых систем с использованием асимметричных алгоритмов / С.В. Штанько, А.А. Корниенко // Защита информации. Информационно-управляющие системы. – 2006. – № 5. – С. 21–26.

2. Авдошин С.М. Криптографические методы защиты информационных систем / С.М. Авдошин, А.А. Савельева // Известия АИН им. А.М. Прохорова. Бизнес-информатика. – 2006. – Т. 17. – № 2 – С. 91–99.

3. Moore C. Targeting FPGA DSP slices for a large integer multiplier for integer based FHE / C. Moore, N. Hanley, J. McAllister, M. O'Neill, E. O'Sullivan // Financial Cryptography and Data Security. – Springer Berlin Heidelberg. – 2013. – P. 226–237.

4. Орлова С.И. Методика оценки эффективности поточных шифров / С.И. Орлова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2004. – № 9. – С. 141–152.

5. Бедратюк Л.П. Використання системи комп'ютерної алгебри MAPLE в класичних криптосистемах / Л.П. Бедратюк, Г.І. Бедратюк // Вісник Хмельницького національного університету. Технічні науки. – 2015. – № 6 (231). – С. 148–153.

6. Калмыков И.А. Разработка псевдослучайной функции повышенной эффективности / И.А. Калмыков, О.И. Дагаева // Известия ЮФУ. Технические науки. – 2011. – № 12(125). – С. 160–169.

7. Михерский Р.М. Шифр на основе случайных чисел с неравномерным распределением / Р.М. Михерский // Програмні системи захисту інформації ISSN 1727-4907. Проблеми програмування. – 2011. –№ 4. – С. 90–95.

8. Рейзлин В.И. Новый метод шифрования с использованием последовательностей квазислучайных чисел / В.И. Рейзлин // Фундаментальные исследования. Технические науки. – 2014. – №12. – С. 505–508.

9. Козлов А.А. Сложение по модулю 2n в блочном шифровании / А.А. Козлов, А.М. Карондеев, Силков А.А. // Вопросы кибербезопасности. – 2015. – № 3(11). – С. 34–42.

Рецензія/Peer review : 6.3.2016 р. Надрукована/Printed :19.4.2016 р.
Рецензент : .т.н., професор Рудницький В. М.