УДК 681.3

І. Дронюк, М. Назаркевич
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

РОЗРОБЛЕННЯ МЕТОДУ ШИФРУВАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ ЗА ДОПОМОГОЮ АТЕВ-ФУНКЦІЙ

© Дронюк І., Назаркевич М., 2008

Запропонований метод шифрування інформації, що ґрунтується на застосуванні теорії Ateb-функцій. В основу шифрування покладено поліалфавітні шифри. Приклади вихідного та зашифрованого тексту представлено на рисунках. Цей метод захисту електронних документів можна використати при пересиланні документів у мережі Інтернет.

Offered method for enciphering information, that is based on the Ateb-functions theory applicationf. Alphabetical codes are fixed in basis of enciphering to the flap. The examples of code the source and the cipher document are represented on pictures. This method of the electronic documents defence is possible to use for sending documents in a network.

1. Вступ

Математичними методами забезпечення конфіденційності, тобто неможливості прочитання інформації стороннім і автентичності, тобто цілісності і справжності авторства інформації, займається криптографія [1]. Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Відомо понад десять перевірених алгоритмів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму роблять шифрований текст недоступним для криптоаналізу.

До нашого часу криптографія займалася винятково забезпеченням конфіденційності повідомлень (тобто шифруванням) — перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотне відновлення на боці одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав, без секретного знання (а саме ключа, необхідного для дешифрування повідомлення). В останні десятиліття сфера застосування криптографії розширилася і передбачає не лише таємну передачу повідомлень, але й методи перевірки цілісності повідомлень, ідентифікування відправника/одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження та технології безпечного спілкування тощо.

Шифр вважається надійним в обчислювальному сенсі [1], якщо його розкриття хоча в принципі можливе, але навіть на найшвидшому комп'ютері вимагатиме нереального часу (роки, століття), після завершенння якого будь-яка таємниця стане неактуальною. Популярною криптосистемою, надійною саме в такому сенсі, є Data Encryption Standard (DES) – стандарт блочного шифрування даних, прийнятий у Сполучених Штатах Америки.

Незважаючи на те, що стандарт DES було визнано застарілим, він (та особливо його все ще дійсний варіант triple-DES) залишається досить популярним; він викристовується в багатьох випадках: від шифрування в банкоматах до забезпечення приватності електронного листування. Було також розроблено багато інших шифрів різної якості. Багато з них було зламано.

Потокові шифри [1], на відміну від блочних, створюють ключ довільної довжини, що накладається на відкритий текст побітово або політерно, у дечому подібно до одноразової дошки. В потокових шифрах потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем та у деяких алгоритмах ще і потоком відкритого тексту. RC4 є прикладом добре відомого та поширеного потокового шифру.

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, незважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.

В основному симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні. На практиці це означає, що якісні асиметричні алгоритми в сотні або в тисячі разів повільніші за якісні симетричні алгоритми. Недоліком симетричних алгоритмів є необхідність мати таємний ключ з обох боків передачі інформації. Оскільки ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації під час розповсюдження.

При застосуванні із асиметричними алгоритмами шифрування для передачі ключей майже завжди використовуються генератори криптографічно стійких псевдовипадкових чисел для генерування симетричних ключей сеансу. Однак, брак достатнього рівня випадковості в цих генераторах або в їх початкових векторах в минулому часто призводив до втрати конфіденційності при передачі даних. Дуже ретельний підхід до впровадження криптосистеми та генерація випадкових чисел із використанням високоякісних джерел випадкових чисел є дуже важливим для збереження конфіденційності даних, що передаються.

Головне досягнення асиметричного шифрування в тому, що воно дає змогу людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями.

2. Алгоритм шифрування електронної інформації на основі гіперболічних Ateb-функцій

Відомими методами шифрування є поліалфавітні шифри [1], тобто шифри заміни, в яких позиція букви у відкритому тексті впливає на те, за яким саме правилом ця буква буде змінена. Одним з відомих є шифр Віженера, за яким відкритий текст та криптотекст записуються в одному і тому алфавіті. Для букв *x* та *y* алфавіту означимо зашифровану букву сумою (N_x + N_y) як результат циклічного зсуву букви *x* вправо у алфавіті на кількість позицій, що дорівнює номеру букви *y* в алфавіті. Тут N_x позначає номер букви у алфавіті. При використанні шифру Віженера одинаковим буквам у відкритому тексті можуть відповідати різні букви у криптотексті. Ця обставина ускладнює частотний криптоаналіз.

У даній статті нами представлений метод шифрування інформації, що базується на застосуванні теорії Ateb-функцій [2], який можна вважати певною модифікацією поліалфавітних шифрів. Але на відміну від цих шифрів у розробленому методі відмовляємось від застосування циклічності зсуву, оскільки пропонується використовувати не алфавіт, а всю таблицю стандартних кодувань ASCII символів.

Суть цього методу полягає у заміні вихідної текстової інформації у файлі на зашифровану методом зміщення за нелінійним законом, що грунтується на протабульованих значеннях гіперболічних *Ateb*-функцій. А саме, нехай *X* – символ алфавіту, що підлягає шифруванню. Вважаємо, що *X* може набувати значень латинських та кириличних символів, цифр та розділових знаків. Зашифроване значення $П_x$ шукаємо за формулою

$$\pi_x = x + a(n,m), \qquad (1)$$

де π_x – *ASCII*-код зашифрованого символа $П_x$, *x* – ASCII-код символа алфавіту X, *a(n,m)* – протабульоване значення гіперболічної Ateb-функції у цілочисловому вигляді, що залежить від параметрів *n, m.*

Шифрування реалізуємо так. Знаходимо у файлі частину, що містить текст вихідного документа. Обчислюємо кількість символів вихідного тексту. Формуємо масив даних такої ж розмірності протабульованої гіперболічної Ateb-функції у цілочисельному вигляді з певними заданими

параметрами *n, m* (див. табл. 1) та переводимо його у шістнадцятковий формат (при отриманні надто великих значень числа можуть бути зменшені за модулем 16). Використання гіперболічної Ateb-функції зумовлене суттєвою нелінійністю та неповторюваністю її значень, що створює можливість встановити однозначну відповідність між шифрованим та нешифрованим текстом (рис. 1, 2). Додаємо ці значення до кодів символів алфавіту, що містять початковий текст, за формулою (1). Отримаємо зашифрований текст з символами $\pi_{x,}$ які відповідають зашифрованому значенню. При цьому розмір та структура вихідного файла не змінюється.

П О С Т А Н О В А
ВЕРХОВНОЇ РАДИ УКРАЇНИ

Про проект Закону України про внесення змін
до деяких законодавчих актів України
щодо вдосконалення регулювання відносин
у сфері забезпечення безпеки дорожнього руху

Верховна Рада України **п о с т а н о в л я є**:

1. Проект Закону України про внесення змін до деяких законодавчих актів України щодо вдосконалення регулювання відносин у сфері забезпечення безпеки дорожнього руху (реєстр. N 1061-5), поданий Президентом України, прийняти за основу в редакції, підготовленій Комітетом Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності станом на 17 червня 2008 року.
2. Доручити Комітету Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності:
доопрацювати зазначений законопроект з урахуванням зауважень та пропозицій, висловлених народними депутатами України під час його обговорення у першому читанні, у тому числі щодо вилучення із тексту законопроекту положень, що стосуються внесення змін до законів України "Про рекламу" (270/96-ВР) та "Про автомобільні дороги" (2862-15) щодо розміщення рекламоносіїв на дорогах, а також внесення змін до Закону України "Про обов'язкове страхування цивільно-правової відповідальності власників наземних транспортних засобів" (1961-15) стосовно обов'язкового укладення договорів обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів строком на один рік та щодо заборони реєстрації, перереєстрації, технічного огляду транспортних засобів у разі відсутності поліса обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів;
внести доопрацьований законопроект на розгляд Верховної Ради України в другому читанні 19 вересня 2008 року.

Голова Верховної Ради України А.ЯЦЕНЮК
м. Київ, 17 вересня 2008 року
N 512-VI

Рис. 1. Документ, який підлягає шифруванню

Даний метод здійснює шифрування інформації шляхом заміни алфавіту кириличної, латинської абетки та інших символів у документі. Нами пропонується ще метод заміни не алфавіту, а всіх символів поточного тексту в документі на суму поточного символу та значення Ateb-функції.

3. Результати роботи методу шифрування на основі гіперболічних Ateb-функцій

Приклад зашифрованого тексту представлено на рис. 2. Шифрування проводилося за допомогою $sha(n,m,\omega)$ при значеннях $n=\frac{1}{7}$, $m=\frac{1}{3}$, $\omega\in[0,\infty]$, крок обчислень вибраний 0.1 [3].

При необхідності дешифрування з допомогою розробленої програми вибираємо частину файлу, що містить зашифрований текст, віднімаємо від зашифрованих значень значення елементів масиву протабульованої *Ateb*-функції і отримуємо розшифрований текст, який вставляється у PS-файл на відповідне місце замість шифрованої інформації.

Роботу методу проілюстровано на наступному прикладі. На рис. 1 показано вихідний документ, а на рис. 2 – документ після застосування шифрування. Так за допомогою теорії *Ateb*-функцій можна зашифрувати весь документ чи його частину, а потім відтворити всю інформацію без втрат. Різні параметри m і n, а також вибір типу *Ateb*-функції та вибір кроку обчислень, початкових значень ω дають можливість підібрати унікальні значення шифрування. Знаючи ці параметри, а також формули табулювання *Ateb*-функцій, можна відтворити інформацію.

Рис. 2. Зашифрований документ методом гіперболічної Ateb-функції $sha(n,m,\omega)$ *m=1/3 n=1/7*

Приклад ключа для шифрування на основі гіперболічних Ateb-функцій

номер букви N_x	1	2	3	4	5	6	7	8	9	10
символ букви X	а	б	в	г	д	е	ж	з	и	й
код букви x	602	603	604	605	606	607	608	609	610	611
значення Ateb-функції для *m* 1/3 *n* 1/5 $a(n,m)$	108	120	133	147	162	176	193	211	229	247
шифрований код для *m* 1/3 *n* 1/5 $\pi_{x,}$	710	723	737	752	768	783	801	820	839	858
значення Ateb-функції для *m* 1/3 *n* 1/7 $a(n,m)$	110	122	136	151	167	180	197	214	231	249
шифрований код для *m* 1/3 *n* 1/7 $\pi_{x,}$	712	725	740	756	773	787	805	823	841	860

номер букви N_x	11	12	13	14	15	16	17	18	19
символ букви X	к	л	м	н	о	п	р	с	т
код букви x	612	613	614	615	616	617	618	619	620
значення Ateb-функції для *m* 1/3 *n* 1/5 $a(n,m)$	265	284	303	323	342	362	382	403	423
шифрований код для *m* 1/3 *n* 1/7 $\pi_{x,}$	877	897	917	938	958	979	1000	1022	1043
значення Ateb-функції для *m* 1/3 *n* 1/7 $a(n,m)$	266	284	302	320	338	357	375	394	413
шифрований код для *m* 1/3 *n* 1/7 $\pi_{x,}$	878	897	916	935	954	974	993	1013	1033

номер букви N_x	20	21	22	23	24	25	26	27	28	29	30	31
символ букви X	у	ф	х	ц	ч	ш	щ	ю	я	ь	є	і
код букви x	621	622	623	624	625	626	627	628	629	630	631	632
значення Ateb-функції для *m* 1/3 *n* 1/5 $a(n,m)$	444	465	486	508	529	551	573	595	618	640	663	686
шифрований код для *m* 1/3 *n* 1/7 $\pi_{x,}$	1065	1087	1109	1132	1154	1177	1200	1223	1247	1270	1294	1318
значення Ateb-функції для *m* 1/3 *n* 1/7 $a(n,m)$	432	451	471	490	510	530	549	569	589	610	630	650
шифрований код для *m* 1/3 *n* 1/7 $\pi_{x,}$	1053	1073	1094	1114	1135	1156	1176	1197	1218	1240	1261	1282

4. Висновки

Запропоновано для захисту електронних документів метод шифрування, що є певною модифікацією поліалфавітних шифрів та базується на протабульваних значеннях *Ateb*-функцій. Додатковою перевагою методу є невеликий розмір утвореного файлу (порядку десятків кілобайт) з шифрованою інформацією.

Метод захисту електронних документів з допомогою шифрування можна використати при пересиланні документів у мережі Інтернет.

1. Вербицький О.В. Введення в криптологію. – Львів: Наук.-техн. літ., 1998. – 248 с. 2. Грицик В.В., Назаркевич М.А. Алгоритм табулювання Ateb-функцій // Системні технології. Регіональний міжвузівський збірник наукових праць. – 2006. – Вип. № 6(47). – С.77–83. 3. Дронюк І.М., Назаркевич М.А. До розв'язування одного класу звичайних нелінійних диференціальних рівнянь // Фізико-технічне моделювання та інформаційні технології: Науковий збірник. – 2007. – № 6. – С.136–140.