УДК 004.056.55

СПОСІБ ШИФРУВАННЯ І ДЕШИФРУВАННЯ ДАНИХ

В.В. Авраменко, *канд. техн. наук, доцент;*
М.І. Заболотний*,
Сумський державний університет, м. Суми;
**ТОВ "Ефективні рішення-Київ"*

Розроблений алгоритм шифрування інформації за допомогою функцій на множині дійсних чисел. Зазначені функції мають випадкову складову, яка не відома ані відправнику, ані одержувачу повідомлення. Розшифрування повідомлення виконується за допомогою функцій непропорційності.

Ключові слова*: криптосистема, аналіз, шифрування, розшифрування, функція, ключ, непропорційність, шифротекст, обчислення, повідомлення.*

Разработан алгоритм шифрования информации с помощью функций на множестве действительных чисел. Указанные функции имеют случайную составляющую, которая не известна ни отправителю, ни получателю сообщения. Расшифрование сообщения осуществляется при помощи функций непропорциональности.

Ключевые слова: *криптосистема, анализ, шифрование, расшифровывание, функция, ключ, непропорциональность, шифротекст, расчет, уведомление.*

ВСТУП

Переважно всі криптосистеми використовують множину простих чисел [1]. Потужність множини простих чисел менша відносно множини цілих чисел, а тим більше - дійсних чисел. Це примушує збільшувати довжину ключів з метою підвищення криптостійкості систем, що породжує проблеми генерації ключів та швидкості роботи алгоритму шифрування та дешифрування. Тому актуальним є завдання розроблення криптосистем, які використовують дійсні числа.

ПОСТАНОВКА ЗАВДАННЯ

Розробити симетричну криптосистему, яка використовує як поле для ключів множину дійсних чисел. Також необхідно, щоб шифрування не мало статистичних закономірностей, тобто шифрування одного і того самого повідомлення за допомогою одних і тих самих ключів кожного разу давало різний шифротекст.

РЕЗУЛЬТАТИ

Пропонується симметрична система [2], в якій як ключ використовується набір функцій на множині дійсних чисел $f_i(\tau(t)) \in R \quad i = \overline{1 \ldots m}$.

Кожний символ повідомлення подається в бінарному коді, таким чином, що бінарний код місить більше, ніж одну одиницю.

i-му бінарному розряду ставиться у відповідність еталонна функція $f_i(\tau(t)) \in R \quad i = \overline{1 \ldots m}$, де m більше, ніж кількість бінарних розрядів. Функція шифрування повідомлення має вигляд

$$f_0(t) = \sum_{i=1}^{m} a_i k_i f_i(\tau(t)), \qquad (1)$$

де $t \in R$ (як t може виступати місцеположення символу в повідомленні), a_i - значення i-го бінарного розряду (0 або 1); k_i - масштабний множник, значення якого генерується випадковим чином і невідомо ні відправнику, ні одержувачу повідомлення; $\tau(t) \in R$ служить для генерації аргументів еталонних функцій з метою підвищення криптостійкості.

$f_i(\tau(t))$ мають задовольняти такі обмеження:

1. Функція повинна належати до області дійсних чисел.
2. Вона повинна мати похідні до порядку m включно.
3. Функція і її похідна будь-якого порядку (у тому числі і m) не повинні бути константою.
4. Функція не повинна містити відрізків, на яких при декількох контрольних обчисленнях вона практично дорівнює константі (наприклад, функція $x^{-\alpha}$ при великих значеннях x).

У результаті вищезазначених операцій отримуємо шифрування $f_0(t)$.

При числовій реалізації алгоритму передаються функції $f_0(t)$ в дискретній формі. Тобто у вигляді масиву. Довжина масиву не повинна бути сталою. Змінюватися довжина масиву буде за заздалегідь обумовленим користувачами правилом.

Як приклад такої схеми можна визначити такий алгоритм: довжина масиву визначається як $60 + (\sum_{i=1}^{m} a_i \cdot i) \bmod 30$.

Надійність же самої системи передачі інформації можна підвищити за допомогою біноміальної системи обчислень [3].

На відміну від бінарних чисел біноміальні числа використовують для своєї побудови доволі складні обмеження. Вони вводять додаткову надлишкову інформацію, яку можна використовувати для виявлення, а в деяких випадках і виправлення помилок. Показником наявності помилок є порушення вказаних обмежень.

Розшифрування повідомлення

Розшифрування виконується за допомогою функцій непропорційності [4], які мають вигляд

$$F_{0i} = @d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0^{\cdot}(t)}{f_i^{\cdot}(\tau(t))}, \qquad (2)$$

де $@d^{(1)}_{f_i(\tau(t))} f_0(t)$ - позначення непропорційності за похідною першого порядку функції $f_0(t)$ за $f_i(\tau(t))$; $f_0(t)$ - функція, що становить зашифроване повідомлення; $f_i(\tau(t))$ - еталонна функція; $f_0'(t)$, $f_i'(\tau(t))$ - похідні від функцій $f_0(t)$, $f_i(\tau(t))$.

Після отримання зашифрованого повідомлення завдання зводиться до знаходження бінарного коду, який зашифрований у повідомленні $f_0(t)$. Для цього за допомогою функцій непропорційності (2) визначається, які саме еталонні функцій складають зашифрований блок повідомлення. Оскільки кожна з еталонних функцій відповідає певному розряду двоїстого числа, то це дозволяє визначити бінарний код зашифрованого символу.

Для знаходження еталонних функцій, які увійшли в суму $f_0(t)$, використовуємо такий алгоритм.

Послідовно перебираються всі можливі з m - розрядних бінарних кодів повідомлень, а отже, і відповідні їм набори еталонних функцій. Для кожного елемента вибірки обчислюється функція непропорційності значення шифротексту за еталонними функціями. Якщо ця функція непропорційності дорівнює нулю, а це буде тільки в тому випадку, якщо набір еталонних функцій з припущення відповідає початковому повідомленню, то повідомлення розшифровано.

Коли в бінарному коді одна одиниця, то функція непропорційності має вигляд

$$F_{0i} = @\, d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0^{'}(t)}{f_i^{'}(\tau(t))}.$$

У випадку, якщо кількість одиниць дорівнює дві, - функція непропорційності має вигляд

$$F_{0iji} = @\, d^{(1)}_{F_{ji}(t)} F_0(t) = \frac{F_{0i}(t)}{F_{ji}(t)} - \frac{F_{0i}'(t)}{F_{ji}'(t)},$$

$$F_{ji} = @\, d^{(1)}_{f_i(\tau(t))} f_j(\tau(t)) = \frac{f_j(\tau(t))}{f_i(\tau(t))} - \frac{f_j^{'}(\tau(t))}{f_i^{'}(\tau(t))}.$$

Аналогічно формується вигляд функції непропорційності при більшій кількості одиниць у бінарному коді.

Похідна від функції при числовій реалізації може обчислюватися за формулою Ньютона-Стірлінга:

$$f^{'} = (\Delta^1 f + \frac{\Delta^2 f}{2} - \frac{\Delta^3 f}{6} + \frac{\Delta^4 f}{12} - \frac{\Delta^5 f}{20} + \frac{\Delta^6 f}{30}) \cdot \frac{1}{h},$$

де h – крок;

$$\Delta^1 f = f_i - f_{i-1};$$

$$\Delta^2 f = \Delta^1 f_i - \Delta^1 f_{i-1} \text{ і т. д.}$$

Як приклад розглядається алгоритм визначення вигляду функції непропорційності та розпізнавання еталонних функцій, що увійшли в $f_0(t)$ у випадку коли $\sum_{i=1}^{m} a_i = 3$, тобто кількість одиниць у бінарному коді дорівнює три. Кількість одиниць у бінарному коді дорівнює кількості еталонних функцій, що увійшли в суму $f_0(t)$. А i - це номер першої одиниці у бінарному коді, j - номер другої одиниці, q - третьої.

Етап перший. Знаходиться непропорційність функції $f_0(t)$ за однією із будь-якою функцією $f_i(t)$, яка позначається через $F_{0i}(t)$:

$$F_{0i} = @d^{(1)}_{f_i(\tau(t))} f_0(t) = \frac{f_0(t)}{f_i(\tau(t))} - \frac{f_0^{'}(t)}{f_i^{'}(\tau(t))}.$$

Замість $f_0(t)$ в (2) підставляється його вираз в (1).

Отримаємо

$$F_{0i}(t) = \sum_{i \neq j} k_j \left(\frac{f_j(\tau(t))}{f_i(\tau(t))} - \frac{f_j'(\tau(t))}{f_i'(\tau(t))}\right) = \sum_{i \neq j} k_j F_{ji}(t), \quad (3)$$

де

$$F_{ji}(t) = @d^{(1)}_{f_i(\tau(t))} f_j(\tau(t)). \quad (4)$$

Етап другий. Знаходиться непропорційність $F_{0iji}(t)$ за похідною першого порядку функції $F_{0i}(t)$ за однією із будь-яких функцій $F_{ji}(t)$:

$$F_{0iji}(t) = @d^{(1)}_{F_{ji}(t)} F_{0i}(t) = \frac{F_{0i}(t)}{F_{ji}(t)} - \frac{F_{0i}'(t)}{F_{ji}'(t)}. \quad (5)$$

З огляду на формулу (3)

$$F_{0iji}(t) = \sum_{q \neq j} k_q F_{qiji}(t), \quad (6)$$

де

$$F_{qiji}(t) = @d^{(1)}_{F_{ji}(t)} F_{qi}(t). \quad (7)$$

Етап третій. Знаходиться непропорційність $F_{0ijiqiji}(t)$ за похідною першого порядку функції $F_{0iji}(t)$ за однією із будь-яких функцій $F_{qiji}(t)$ з (7):

$$F_{0ijiqiji}(t) = @d^{(1)}_{F_{qiji}(t)} F_{0iji}(t). \quad (8)$$

Якщо функція непропорційності (8) дорівнює нулю, то вважається, що зашифроване повідомлення при розшифруванні дорівнює поточному елементу з вибірки можливих повідомлень.

За аналогічною схемою розшифровуються інші можливі повідомлення, коли $\sum_{i=1}^{m} a_i \neq 3$. Кількість етапів обчислення дорівнює $\sum_{i=1}^{m} a_i$.

Як було сказано вище, індекси при обчисленні функцій непропорційності залежать від положення одиниці в бінарному коді. Наприклад, бінарний код можливого повідомлення з вибірки має вигляд 11100000. Відповідний набір індексів має вигляд $ijqklmnp$.

Тоді $i = 1, j = 2, q = 3, k = 4, l = 5, m = 6, n = 7, p = 8$.

Функції непропорційності дозволяють розпізнати [5], які еталонні функції входять у суму (1) незалежно від невідомих значень k_i, і таким чином розшифрувати повідомлення.

ВИСНОВКИ

Завдяки запропонованому способу шифрування збільшується кількість можливих ключів, тим самим зростає стійкість системи при атаці методом підбору. Через більшу кількість можливих варіацій ключів спрощується їх вибір. Таким чином, завдяки використанню разом з еталонними функціями випадкових коефіцієнтів, досягається те, що одне й те саме повідомлення, з однаковими ключами, кожного разу дає різне шифрування, що робить виявлення статистичних властивостей більш складним.

SUMMARY

THE METHOD OF THE DATA ENCRYPTING AND DECODING

V.V. Avramenko, M.I. Zabolotnyi*

Sumy State University, Sumy

**Kyiv*

The algorithm of the information encrypting by means of functions on set of real numbers was developed. The specified functions have a random component which is not known neither to the sender, nor the addressee of the message. De-encryption of messages is carried out by means of disproportional functions.

Key words:*data encrypting, decoding, de-encryption,disproportional function.*

СПИСОК ЛІТЕРАТУРИ

1. Смарт Н. Криптография / Н. Смарт. - Москва: Техносфера, 2006. – 528 с.
2. Авраменко В.В., Заболотний М. І. Патент України "Спосіб шифрування даних" №42957 від 27.07.09, МПК (2009) H04L 9/00.
3. Борисенко А.А. Биномиальный счет / А.А. Борисенко. – Сумы: Университетская книга, 2004. - 167с.
4. Характеристики непропорциональности числовых функций и их применение / В.В. Авраменко. - Деп. В ГНТБ Украины 19.01.98, N59 – Ук 98.
5. Авраменко В.В. Распознавание фрагментов заданных эталонов в анализируемом сигнале с помощью функций непропорциональности / В.В. Авраменко, А.П. Карпенко // Вісник СумДУ. - 2002. - №1(34). – С.96-101.

Надійшла до редакції 4 вересня 2009 р.