Перевірка на стійкість блоково-динамічного шифрування

С.М. БІЛАН, І.М. ШВАРЦ

Київський університет економіки і технологій транспорту

Розглянуто можливість перевірки блоково-динамічного алгоритму на стійкість до атак відомими методами криптографічного аналізу, такими як імовірнісний, диференційний та лінійний методи криптоаналізу. Отримані результати засвідчили, що запропонований блоково-динамічний алгоритм є абсолютно стійким до всіх відомих методів криптоаналізу.

Рассмотрена возможность проверки блоково-динамического алгоритма на стойкость к атакам известными методами криптографического анализа, такими как вероятностный, дифференциальный и линейный методы криптоанализа. Полученные результаты засвидетельствовали, что предложенный блоково-динамический алгоритм абсолютно устойчив ко всем известным методам криптоанализа.

A possibility of testing the stability characteristic of the block-dynamic algorithm with the help of famous methods of cryptanalysis has been considered. The results have proved, that the block-dynamic algorithm is absolutely stable against all known methods of cryptanalysis.

Використання обчислювальної техніки і телекомунікаційних систем у рамках територіально розподіленої мережі, перехід на цій основі до безпаперової технології, збільшення обсягів оброблюваної інформації, розширення кола користувачів і багато інших факторів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем, до їхньої високої уразливості [1]

У даній статті ставиться задача перевірки на криптостійкість та надійність при передачі інформації по комп'ютерним мережам з використанням модифікованого криптографічного алгоритму шифрування Blowfish [2,3] з відповідними розробленими криптографічними протоколами [4].

Для проведення імовірносного аналізу приймемо, що відомо відкрите повідомлення та шифрований текст, що йому відповідає, а також алгоритм блоково-динамічного шифрування. Необхідно знайти ключ, за допомогою якого відкрите повідомлення із застосуванням алгоритму блоково-динамічного шифрування перетворюється в шифрований текст .

Імовірнісний метод криптоаналізу полягає в циклічній перевірці ключа *k*, отриманого на основі генератора випадкових чисел до тих пір, поки він не задовольнить рівність T(x,k)=y, де x – відкрите повідомлення; y – шифрований текст; T – шифр.

В якості функцій випадкової величини розглянемо стандартну для більшості мов програмування високого рівня функцію Random та ітеративну функцію виду $X_{i+1}=\{11X_i+\pi\}$.

При цьому випадковий ключ генерується за співвідношеннями при використанні функції Random

$$k = \sum_{i=1}^{m} \mathrm{Chr}(\mathrm{Random}(256))_i , \qquad (1)$$

при використанні функції $X_{i+1}=\{11X_i+\pi\}$

$$k = \sum_{i=1}^{m} \mathrm{Chr}(\mathrm{Trunc}(\mathrm{d_i} \cdot 256))_i \qquad (2)$$

$$d_{i+1} = Frac(11 d_i + \pi) , \qquad (3)$$

де m – довжина ключа в символах ANSI/ASCII;

Random(a) – функція випадкової величини 0≤Random<a;

d – випадкова величина 0≤d<1;

Trunc – функція цілої частини числа;

Frac – функція дробової частини числа;

Chr(a) – функція, яка повертає символ з кодом a в таблиці ANSI/ASCII;

Оскільки цей метод імовірнісний, то час "відкриття" одного й того самого ключа при різних початкових значеннях Random може суттєво відрізнятися. Тому час "відкриття" будемо оцінювати за середнім значенням. Середній час "відкриття" для імовірнісного методу криптоаналізу визначається за формулою:

$$t_{cp} = \frac{1}{n} \sum_{i=1}^{n} t_i , \qquad (4)$$

де n – кількість дублювань "відкриття" ключа; i – поточне значення дублювання "відкриття" ключа; t_i – час "відкриття" i-го дублювання "відкриття" ключа; $t_{ср}$ – середній час "відкриття" ключа.

Для зручності час переведемо із секунд в роки за формулою:

$$t_{ðîê³â} = \frac{t_ñ}{365{,}25 \cdot 24 \cdot 60 \cdot 60} , \qquad (5)$$

де t_c - час "відкриття" ключа в секундах; $t_{років}$ - час "відкриття" ключа в роках.

Для пошуку P-блоку, за допомогою якого відкрите повідомлення із застосуванням блоково-динамічного алгоритму шифрування перетворюється в шифрований текст, припустимо, що існує відкрите повідомлення та шифрований текст, що йому відповідає, а також частина алгоритму блоково-динамічного шифрування за винятком функції розгортання ключа в P-блок. Імовірнісний метод "відкриття" P-блоку блоково-динамічного шифру полягає в циклічній перевірці ключа P-блоку, отриманого на основі генератора випадкових чисел до тих пір, поки він не задовольнить рівність T(x,P)=y, де x – відкрите повідомлення; y – шифрований текст; T – шифр.

Для блоково-динамічного шифру Р-блок являє собою масив 32-бітних чисел.

Розглянемо такі функції випадкової величини, як стандартна функція Random та ітеративна функція виду $X_{i+1}=\{11X_i+\pi\}$.

Випадковий Р-блок генерується за співвідношеннями для функції Random

$$P_i = \text{Random}(2^{4\times 8})_i\,, \qquad (6)$$

для функції $X_{i+1}=\{11X_i+\pi\}$

$$P_i = \text{Trunc}(d_j \cdot 2^{4\times 8})_i\,; \qquad (7)$$

$$d_{j+1} = Frac(11d_j + \pi)\,, \qquad (8)$$

де i – поточний індекс елементу Р-блоку (i=0…n-1); n – кількість елементів Р-блоку (для блоково-динамічного шифру n=18); Random(a) – функція випадкової величини 0≤Random<a; d – випадкова величина 0≤d<1; Trunc – функція цілої частини числа; Frac – функція дробової частини числа; $2^{4\times 8}$ – кількість можливих варіантів 32-бітного числа.

В результаті проведеного імовірносного криптоаналізу блоково-динамічне шифрування доцільніше реалізувати за допомогою функції $X_{i+1}=\{11X_i+\pi\}$, оскільки до цієї функції вказаний шифр менш стійкий порівняно із стандартною функцією Random.

Лінійний криптоаналіз полягає в складенні та розв'язанні системи рівнянь виду

$$T(x,k)=y, \qquad (9)$$

де x – відкрите повідомлення; y – шифрований текст; T – шифр; k – ключ.

У випадку блоково-динамічного шифру ключ k розгортається перед початком шифрування у Р-блок та S-блоки. При чому Р-блок містить N 32-бітних елементів

$$\begin{cases} T(x_1,P_0,S_{0,0})=y_1; \\ T(x_2,P_0,S_{0,1})=y_2; \\ \quad\ldots \\ T(x_{256},P_0,S_{0,255})=y_{256}; \\ T(x_{257},P_1,S_{0,0})=y_{257}; \\ T(x_{258},P_1,S_{0,1})=y_{258}; \\ \quad\ldots \\ T(x_{512},P_1,S_{0,255})=y_{512}; \\ \quad\ldots \\ T(x_{kx},P_N,S_{3,255})=y_{kx}. \end{cases}$$

В результаті проведеного лінійного криптоаналізу встановлено, що відкриття повного 16-прохідного блоково-динамічного шифрування вимагає порядку 144 Кбайт відкритого тексту та 2,87 Гбайт оперативної пам'яті. Визначено, що максимальна кількість проходів, при якій доцільно застосовувати лінійний криптоаналіз блоково-динамічного шифрування дорівнює $n_{max}=9$ (рис. 1).

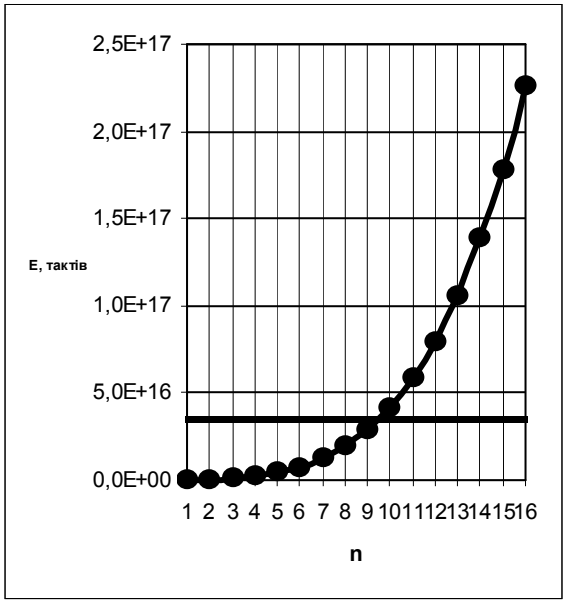

Рис. 1. Графічне визначення максимальної кількості проходів

Для проведення диференційного аналізу приймемо, що відомо відкрите повідомлення та шифрований текст, що йому відповідає, а також алгоритм блоково-динамічного шифрування. Необхідно знайти Р-блок, S-блоки, ключ, необхідну кількість відритих текстів і трудомісткість розкриття блоково-динамічного шифру, наявність слабких ключів та імовірність їх появи. Згідно джерела [5] для взлому блоково-динамічного шифру методом диференціального аналізу необхідно 2^{24} пар відкритого тексту. Для 4-раундового блоково-динамічного шифру трудомісткість складає 2^{32}, при 6-ти раундах - трудомісткість 2^{67}, при 7-ми раундах трудомісткість 2^{131}. На основі даних джерела проведений регресійний аналіз залежності трудомісткості E від кількості раундів r при використанні диференціального криптоаналізу блоково-динамічного шифрування (табл. 1.).

Таблиця 1. **Трудомісткість розкриття блоково-динамічного шифру з числом раундів 4-16 методом диференціального криптоаналізу**

Кількість раундів, r	4	5	6	7	8	9	10
Трудомісткість, E	2^{32}	2^{51}	2^{67}	2^{131}	2^{190}	2^{297}	2^{466}
Кількість раундів, r	11	12	13	14	15	16	
Трудомісткість, E	2^{731}	2^{1147}	2^{1799}	2^{2822}	2^{4426}	2^{6941}	

В результаті проведеного диференціального аналізу визначено що кількість відкритих текстів, необхідних для диференціального криптоаналізу блоково-динамічного шифру, в кількості $2^9...2^{129}$, залежить від кількості раундів. Визначено, що його доцільно проводити з кількістю раундів, яка менша або дорівнює 5 (рис. 2).

Проведений порівняльний аналіз показників криптостійкості блоково-динамічного алгоритму з відомими блочними алгоритмами для таких методів криптоаналізу, як повного перебору (табл. 2), імовірнісного (табл. 3), лінійного (табл. 4), та диференціального (табл. 5), встановлено, що найбільшу криптостійкість має блоково-динамічний шифр, а найнижчу - відповідно шифр DES.

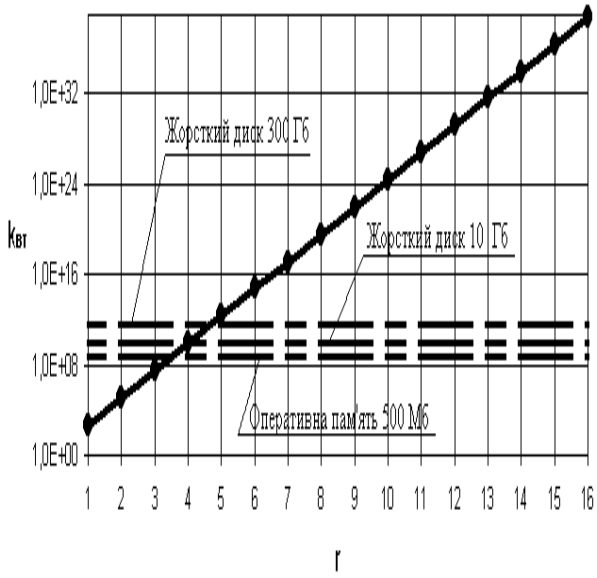

Рис. 2. Графік залежності кількості відкритих текстів $k_{ВТ}$, необхідних для взлому блоково- від кількості раундів r

Таблиця 2. **Трудомісткість E відкриття ключа методом повного перебору**

Назва шифру	Максимальна довжина ключа m, біт	Максимальна середня трудомісткість E відкриття ключа
Blowfish	448	3,6342E+134
IDEA	128	1,70141E+38
ГОСТ	256	5,7896E+76
DES	56	3,60288E+16
Twofish	256	5,7896E+76
Блоково-динамічний	448k	2,6415E+269

Таблиця 3. **Трудомісткість E відкриття ключа для імовірнісного методу**

Назва шифру	Максимальна довжина ключа m, біт	Максимальна середня трудомісткість E відкриття ключа
Blowfish	448	3,6342E+134
IDEA	128	1,70141E+38
ГОСТ	256	5,7896E+76
DES	56	3,60288E+16
Twofish	256	5,7896E+76
Блоково-динамічний	448k	2,6415E+269

За допомогою проведеного аналізу розробленого методу блоково – динамічного шифрування на криптостійкість встановлено, що серед розглянутих методів криптоаналізу для взлому ключа максимальної довжини m=448 біт блоково-динамічного шифру найбільш результативним є метод лінійного криптоаналізу, трудомісткість якого складає $E=4{,}5\cdot10^{47}$ при кількості відкритих текстів $1{,}65\cdot10^{7}$, а найменш результативним (тобто криптостійкість до якого найбільша) є метод диференціального криптоаналізу, трудомісткість якого складає $E=2^{6942}=10^{2090}$ при кількості відкритих текстів $2^{25}=3{,}36\cdot10^{7}$.

Таблиця 4. **Трудомісткість E відкриття ключа для лінійного методу**

Назва шифру	Максимальна довжина ключа m, біт	Максимальна середня трудомісткість E відкриття ключа
Blowfish	448	2,25E+47
IDEA	128	3,4E+38
ГОСТ	256	1,18E+16
DES	56	6,48E+15
Twofish	256	3,48E+28
Блоково-динамічний	448k	4,5E+47

Таблиця 5. **Трудомісткість E відкриття ключа для диференціального методу**

Назва шифру	Максимальна довжина ключа m, біт	Максимальна середня трудомісткість E відкриття ключа
Blowfish	448	2,25E+47
IDEA	128	3,4E+38
ГОСТ	256	1,18E+16
DES	56	6,48E+15
Twofish	256	3,48E+28
Блоково-динамічний	448k	4,5E+47

ЛІТЕРАТУРА

1. Жельніков В. Криптографія від папірусу до комп'ютера. М., ABF, 1996 р., 413 с.
2. С.М. Білан, І.М. Шварц. Вдосконалення алгоритму Blowfish з метою підвищення крипостійкості та швидкодії під час передачі інформації по каналам зв'язку // Реєстрація, зберігання та обробка даних. – 2005. - №1, т.7. - С. 97-102.
3. Деклараційний патент на винахід №8897, кл. 7H04L 9/04. Спосіб блочного шифрування даних // Білан С.М., Шварц І.М. – опубл. 15.08.05 – Бюл. № 8.
4. С.М. Білан, І.М. Шварц. Криптографічні протоколи блокового-динамічного шифрування // „Математичне моделювання " . – 2005. - № 1 (13) – С. 71-73.
5. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е издание. – М.: Дело, 2003. – 524 с.

пост. 18.11.05