УДК 681.511.3
Череватий М., Лендель Р. — ст. гр. КСМм-51
Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ МЕТОДУ ДВОХСТОРОННЬОЇ АТАКИ

Науковий керівник: к.е.н., доц. Тимошенко Л.М.

Алгоритм шифрування вважається стійким, якщо атака методом грубої сили проти нього є не ефективною, а більш швидких методів розкриття алгоритму не існує.

Будь-які методи, що здатні розкрити алгоритм шифрування, базуються на аналізі недоліків алгоритму або його реалізації. Розглянемо метод двохсторонньої атаки (meet-in-the-middle).

Найпростіший приклад такої атаки — це розкриття будь-якого алгоритму шифрування, що представляє подвійне шифрування даних за допомогою будь-якого «одинарного» алгоритму. Розглянемо алгоритм Double DES, що представляє собою подвійне шифрування звичайним DES (рисунок 1):

$$\mathbf{C = DES_{k2/2}(DES_{k1/2}(M))},$$

де $\mathbf{k_{1/2}}$ і $\mathbf{k_{2/2}}$ – половини подвійного ключа алгоритму Double DES, кожна з яких є звичайний 56-бітний ключ DES.

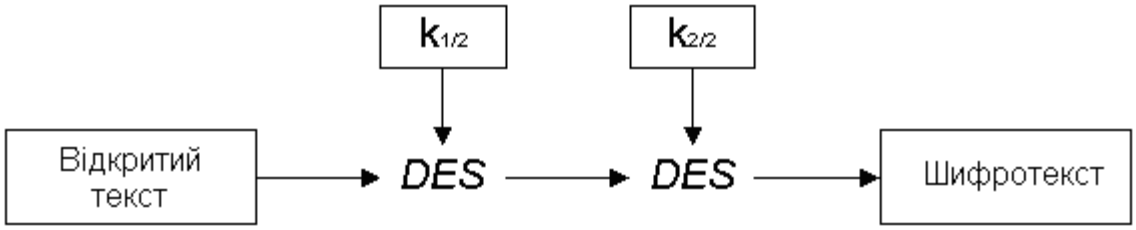

Рисунок1. Алгоритм Double DES.

Double DES вирішує основну проблему алгоритму DES (56-бітний ключ шифрування є занадто малим) – 112-бітний ключ Double DES значно важче атакувати методом повного перебору. Проте, розкриття Double DES успішно виконується атакою на основі відомих відкритих текстів. Припустимо, що у криптоаналітика є відкритий текст **M1** і результат його шифрування – **C1**. Він може здійснити наступну послідовність дій:

1. Виконується операція шифрування $\mathbf{DES_{kx}(M1)}$ у всій множині ключів ($\mathbf{kx}$ = $0…2^{56}$-1) із записом результатів у таблицю.
2. Здійснюється операція дешифрування $\mathbf{DES^{-1}_{ky}(C1)}$ також у всій множині ключів; результати дешифрування порівнюються із записами в таблиці, що формується на етапі 1.
3. Якщо будь-який результат, що отриманий на етапі 2, співпав з одним із результатів етапу 1, то можна припустити, що потрібний ключ знайдено, тобто відповідають результату $\mathbf{kx = k_{1/2}}$, а $\mathbf{ky = k_{2/2}}$, що співпав.

На відміну від Double DES, атака малоефективна проти алгоритмів шифрування даних, що використовують більше 256-бітні довжини ключів. Проте метод «двохсторонньої атаки» застосовується в контексті інших атак, а також для оцінки стійкості криптографічних алгоритмів проти модифікованих алгоритмів.