УДК 004.77
Я. Сидорик, Г. Шимчук
(Тернопільський національний технічний університет імені Івана Пулюя)

ОГЛЯД АЛГОРИТМУ КОНФІДЕНЦІЙНОСТІ ДАНИХ

З розвитком та поширенням телекомунікаційних технологій постає задача забезпечення конфіденційності інформації. Одним із завдань, яке необхідно вирішувати є верифікація існуючих систем захисту. На зміну другому поколінню безпровідних технологій зв'язку приходять стандарти третього покоління, зокрема UMTS. Universal Mobile Telecommunications Аналіз захищеності інформації в UMTS мережах дає змогу вказати на вразливі місця в системі безпеки, а також сформулювати можливі рекомендації для підвищення ступеня захисту.

Алгоритм конфіденційності f8 – потоковий шифр, який використовується для шифруванні і дешифрування блоків даних з секретним ключем (СК). Розмір блоку може бути в межах від 1 до 20000 біт. Алгоритм використовує KASUMI в режимі OFB як генератор потокового ключа. OFB – режим зворотного зв'язку, який перетворює блочний шифр в синхронний потік.

Алгоритм f8 використовує два 64-бітні регістри: статичний регістр А і лічильник BLKCNT. Ініціалізація А здійснюється з використанням 64-бітної змінної ініціалізації IV:

$$IV = COUNT \,||\, BEARER \,||\, DIRECTION \,||\, 0 \ldots 0\,, \qquad (1)$$

де COUNT – 32-бітна стрічка;
BEARER – 5 бітна стрічка;
DIRECTION – 1-бітна стрічка.

IV отримується шляхом з'єднання 32 біт COUNT, 5 біт BEARER, 1 біта DIRECTION і 26 нульових бітів. Змінна COUNT ініціалізується під час встановлення з'єднання. Змінна BEARER ідентифікує об'єкт, з яким встановлено з'єднання. Змінна DIRECTION вказує напрямок передачі, «0» – для вихідного з'єднання, «1» – для вхідного з'єднання. Початкове значення лічильника BLKCNT встановлюється в 0. Схема генератора потокового ключа показана на рис. 1.

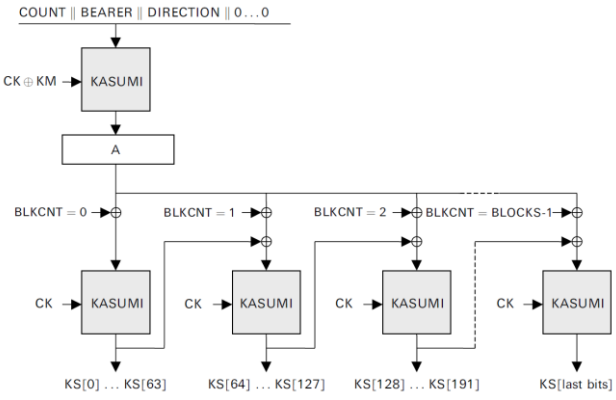

Рис. 1. Генератор потокового ключа

1. 3GPP TS 35.201: «3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification» [Електронний ресурс]. – Режим доступу: http://www.3gpp.org/DynaReport/35201.htm – Назва з екрану.

2. V. Niemi. UMTS Security / V. Niemi, K. Nyberg. – Finland, Helsinki: John Wiley & Sons, 2005. – 273 с.