ВИКОРИСТАННЯ ПОТОКОВОГО ШИФРУВАННЯ В INTERNET-СИСТЕМАХ ТЕЛЕМОНІТОРИНГУ СТАНУ ЗДОРОВ'Я ЛЮДИНИ

БЕЛЗЕЦЬКИЙ Р., ВЛАСЮК Н.

Вінницький національний технічний університет (Вінниця, Україна)

Науковий керівник: Власюк А.І., к.т.н., доцент

Постійне "дистанційне" спостереження за станом здоров'я людини, з використання мережі Internet, дає змогу вирішити проблему своєчасної діагностики та контролю за станом здоров'я людини без відвідування спеціалізованих медичних закладів, що економить час та кошти [1,2]. Сьогодні, уже створені та функціонують Internet-системи телемоніторингу, які дозволяють не тільки отримати миттєвий зріз стану здоров'я людини, а й діагностувати на ранніх стадіях різноманітні захворювання людини.

Проте, поряд з перевагами, які надають засоби мережі Internet для передачі даних моніторингу стану здоров'я людини, постає проблема захисту діагностичної інформації від несанкціонованого доступу та пошкоджень. Адже будь-яке стороннє втручання може значно вплинути на результати обробки діагностичних даних та прийняття рішення про стан здоров'я пацієнта. В зв'язку з цим, актуальним напрямком наукових досліджень є побудова моделі політики безпеки (ПБ) для захисту потоків даних в Internet-системах телемоніторингу стану здоров'я людини [3,4].

Одним із методів захисту інформації в Internet-системах медичного телемоніторингу, є використання потокового кодування з використанням SSC2 шифру [3,4].

SSC2 - потоковий шифр, який складається з доданих за модулем 2 результатів двох "напівшифрів". Перший напівшифр формується з лінійного зсувного регістра зворотного зв'язку (LFSR) з нелінійним фільтром. Другий напівшифр формується генератором Фібоначчі (LFG) і мультиплексора, який вибирає значення з регістра Фібоначчі. Структурна схема потокового шифратора , з використанням шифру SSC2 приведена на рис.

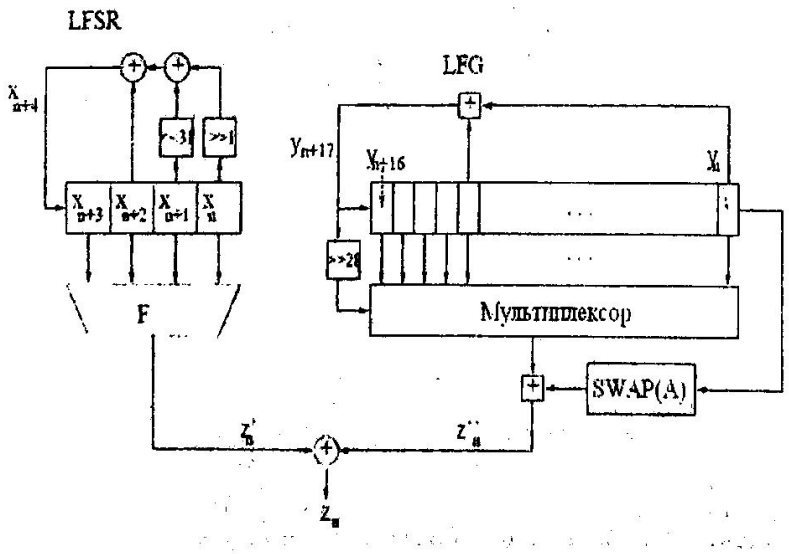

Рис. Структурна схема шифратора потокового шифру SSC2

LFSR складається з регістра, який запам'ятовує послідовність бітів, що називаються кроком, і функція, яка є лінійним модулем 2. Ця функція оновлює біт крок за кроком. LFG складається з регістра, який запам'ятовує послідовність цілих чисел за модулем N (ще раз викликаючи крок) і функції, яка є лінійним модулем N. Ця функція модифікує крок число за числом. У SSC2, модуль - N = 2 32, і цілі числа зберігаються як 32-бітні блоки, що називаються словами.

SCC2 використовує 32-розрядні операції. Потік отримується від 127-бітового LFSR, 17-слівного LFG і мультиплексора, який вибирає значення з регістра LFG. 127-розрядний регістр для LFSR зберігається в чотирьох 32-бітних словах (додатковий біт примушений до 1 у фільтруючій функції);

Після ініціалізації LFSR і LFG виконуються наступні кроки;

1. 32-біти LFSR модифікуються одночасно. *Не лінійний фільтр* (NLF) рахує 32-розрядний вихід N з чотирьох слів в LFSR.
2. Стан LFG модифікується. Верхні і нижні 16 бітів LFG переставлені, щоб сформувати 1 і.

3. Мультиплексор використовує чотири старші біти модифікованого слова, щоб вибрати одне з 16 значень в LFG, щоб вивести *m* i.

4. Виведення шифру – $z\ i = (l_i + m\ i \mod 2^{32})$ XOR Ti. Значення N_i *являється виведенням з напівшифру* LFSR, а $V_i = (l_i + m_i \mod 2^{32})$ – з напівшифру LFG.

Структура, приведена на рис. реалізується в Internet-системах телемоніторингу стану здоров'я людини програмно. Проведені експерименти дозволили оцінити результати роботи програми за допомогою спеціалізованого статистичного тесту NIST STS 1.6.

Література

1. Лисогор В.М., Власюк А.І., Яремко С.А. Вибір базової медичної технології для систем телемоніторингу // Вісник ВПІ. - 2005. - №1. - С. 69 - 75.
2. Центр медицинського телемоніторинга http://www.medcare.ru
3. Daniel Bleichenbacher1 and Willi Meier2. Analysis of SSC2 - Bell Laboratories, Rm. 2A-366, 700 Mountain Av Murray Hill, NJ07974-0636, USA.
4. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптологии. - М.: Горячая линия - Телеком, 2001.