УДК 004.056.55

СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ BLUETOOTH ЗВ'ЯЗКУ СИМЕТРИЧНИМ АЛГОРИТМОМ БЛОКОВОГО ШИФРУВАННЯ

Корсун Д. М.
Науковий керівник – к.т.н., ст. викладач кафедри автоматизації та проектування обчислювальної техніки Рожнова Т. Г.
Харківський національний університет радіоелектроніки
(61166, Харків, проси. Науки,14, каф. АПОТ, тел. (057) 702-13-26)

This work is devoted to the study of data protection in the Bluetooth channel in modern IoT devices. Bluetooth 4.0 and above have addressed security issues by implementing the Security Manager, responsible for authentication, security, confidentiality, and privacy protocols. The Security Manager uses AES, a 128-bit symmetric block cipher, as the encryption key algorithm in the latest Bluetooth versions. The goal is to describe the block encryption method for transmitting data packets between devices using Bluetooth.

Версія Bluetooth 4.0 та вище вирішила багато проблем безпеки попередніх поколінь Bluetooth. Поточні версії Bluetooth використовують стек BLE. Четвертий рівень стека, відомий як Security Manager, який займається тим, що стосується аутентифікації, безпеки та конфіденційності. Найбільш поширеним алгоритмом шифрування, що використовується в останній версії Bluetooth (4.0 і вище): Advanced Encryption Standard (AES) – симетричний блоковий шифр довжиною 128 біт.

Добре відомими реалізаціями алгоритму блочного шифрування є Стандарт шифрування даних (DES), TripleDES та Стандарт розширеного шифрування (AES) [1]. Це криптостійкий алгоритм, що пропонує Агентство національної безпеки США для шифрування цінної інформації з використанням ключа розміром 128 бітів. Особливістю блокових криптоалогритмів є обробка блоку кількох байт за одну ітерацію блок вхідної інформації фіксованої довжини, як правило 8 або 16 байт в результуючий блок того ж обсягу за одну ітерацію, розбиваючи текст повідомлення на окремі блоки і перетворючи ці блоки за допомогою ключа.

Мета роботи – розглянути актуальний спосіб криптографічного захисту каналу Bluetooth в сучасних IoT пристроях. *Задача* – описати блоковий спосіб шифрування для передачі пакетів даних, що передаються між пристроями за допомогою технології Bluetooth.

Схему роботи алгоритму, що зображена на рисунку 1, можна описати такими функціями: Y = EnCrypt (X, Key), X = DeCrypt (Y, Key). Де, ключ (Key) представляє блок двійкової інформації фіксованого розміру, але необов'язково рівний вихідний блоку (X) і зашифрованому блоку даних (Y) які мають фіксовану розрядність, рівну між собою.

Прочитати зашифрований блок можна перебравши всі можливі ключі. За теорією ймовірності ключ буде знайдено з ймовірністю 1/2 після перебору половини всіх ключів, а на пошук ключа довжини N потрібно в середньому 2N-1 перевірок.

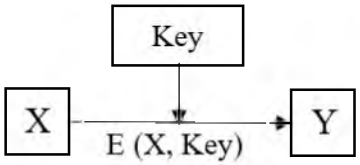

Рисунок 1 – Модель блочного шифру в найпростішому режимі

Так як функція, що шифрує – проста змінна, це викликає серйозну проблему: статистичні властивості відкритих даних частково зберігаються, тому що кожному однаковому блоку даних однозначно відповідає зашифрований блок даних. При великій кількості даних (відео, звук) це може дати деякі відомості для криптоаналізу про зміст даних [2]. Для вирішення цієї проблеми використовується циклічне кодування, щоб змінити структуру даних перед їх шифруванням, тим самим ускладнюючи процес криптоаналізу. Циклічний код є підкласом лінійних блокових кодів, у яких циклічний зсув бітів кодового слова призводить до іншого кодового слова. Відповідно до *властивості лінійності*, лінійна комбінація двох кодових слів повинна генерувати інше третє кодове слово.

Припустимо, у нас є два кодові слова C_i та C_j . Отже, при додаванні $C_i+C_j=C_p$, де C_p також має бути кодовим словом. Відповідно до *властивості циклічного зсуву*, зсув праворуч або ліворуч бітів кодового слова, також, повинен генерувати інше третє кодове слово.

Впровадження диспетчера безпеки в Bluetooth 4.0 і вище дозволило вирішити багато проблем безпеки попередніх поколінь Bluetooth. Використання Advanced Encryption Standard (AES) як 128-бітного симетричного блочного шифру для алгоритму ключа шифрування в останніх версіях Bluetooth забезпечує безпечну передачу пакетів даних між пристроями. Однак статистичні властивості звичайних даних можуть бути частково збережені, що робить їх вразливими для криптоаналізу. Для вирішення цієї проблеми використовується циклічне кодування.

Список використаних джерел:

1. Що таке блок-шифр? - визначення з техопедії. Icy Science. URL: https://uk.theastrologypage.com/block-cipher (дата звернення: 12.01.2023).

2. Потокова модифікація алгоритму rsa для шифрування зображень з чітко виділеними контурами / Ю. Рашкевич та ін. м. Львів. С. 171–178.