АНАЛІЗ ЛЕГКОВАГОВИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ ДАНИХ МІЖ КІНЦЕВИМИ ПРИСТРОЯМИ З ОБМЕЖЕНИМИ РЕСУРСАМИ В СИСТЕМІ ІНТЕРНЕТ РЕЧЕЙ

Євдокименко М.О., Єременко О.С.
Харьковский национальный университет радиоэлектроники
61166, Харків, пр.Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20,
e-mail: marina.ievdokymenko@nure.ua

This article focuses on the issue of ensuring security transmission of data between end devices and servers of IoT-system, namely, the investigation of cryptographic functions for data encryption. In this paper, a comparative analysis of lightweight cryptographic algorithms (RSA, ECC, AES, XTEA), designed for devices with limited resources such as memory, CPU energy consumption and execution time. As a result of the analysis, there arises the need to develop a secure algorithm that combines the best characteristics of lightweight symmetric and asymmetric algorithms with the minimization of execution time with the corresponding energy needs and ensuring confidentiality, integrity and authenticity.

Інтенсивний розвиток ринку інфокомунікаційних систем поступово призводить до появи нових технологій і різноманітних концепцій. Так, одним з перспективних впроваджуваних напрямків є розвиток сегмента «Інтернету речей» (IoT, Internet of Things). Основний принцип цієї концепції полягає в тісній взаємодії звичайних для повсякденного життя речей і швидкісними обчислювальними мережами. Система IoT являє собою комплекс технологій, що застосовуються для збору інформації з системи розподілених датчиків та дистанційного керування автоматичними пристроями, підключеними до мережі Інтернет, а також для зберігання, обробки і візуалізації цих даних на локальних або віддалених серверах. Область застосування «Інтернет речей» може бути «Smart Home», «Smart Grid», мережа автоматичних метеостанцій, телеметрія станів складних пристроїв, управління трафіком, диспетчеризація перевезень та інші.

Слід зазначити, що ефективність, надійність і безпека роботи системи IoT залежить від усвідомленого та грамотного проектування архітектури системи, розподілу функцій між локальним і серверним рівнем, обліку питань безпеки та відмовостійкості системи в цілому. Тому основна увага при впровадженні таких систем спрямована на усунення ряду недоліків, пов'язаних із різноманіттям протоколів і відсутністю загальноприйнятих стандартів, необхідністю зниження енергоспоживання підключених пристроїв і забезпечення захисту даних при використанні системи IoT. Дана робота буде сфокусована на питанні забезпечення захисту передачі даних між кінцевими пристроями

і серверами системи IoT, а саме на дослідженні криптографічних функцій для шифрування даних.

Аналіз легковагових криптографічних алгоритмів для безпечної передачі даних в системі Інтернет Речей

Безпечне розгортання інфраструктури Інтернет речей обов'язково передбачає захист в розрізі трьох областей безпеки (рис.1):

- *безпека пристроїв,* яка полягає в забезпеченні захисту пристрою IoT під час розгортання в умовах експлуатації;
- *захист з'єднання,* що відповідає за забезпечення конфіденційності даних і їх захисту від несанкціонованої зміни при передачі між пристроєм IoT і сервером IoT;
- *безпека в хмарі,* що забезпечує захист даних при їх передачі та зберіганні в хмарі.

Також, для безпечної експлуатації пристроїв необхідна насамперед перевірка їх автентичності. Для цього передбачено генерацію унікального ключа, який далі використовується для обміну даними з працюючим пристроєм. Створений ключ і ідентифікатор обраного користувачем пристрою разом утворюють токен, який використовується для обміну даними між пристроєм і службою серверу IoT.

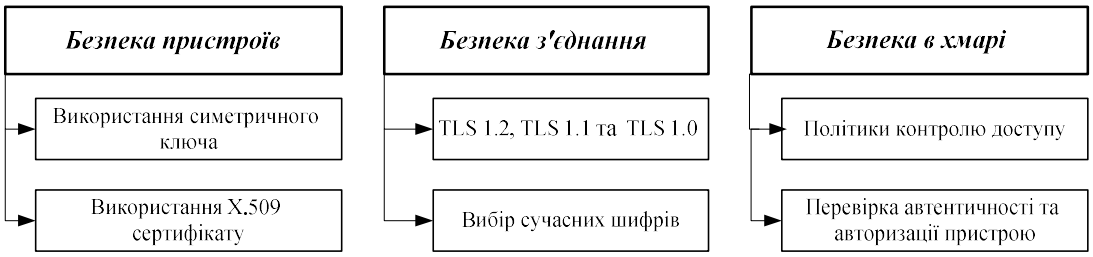

Рисунок 1. – Методи забезпечення захисту інфраструктури Інтернет речей

Захист з'єднання між пристроєм і сервером IoT забезпечується за допомогою різних версій протоколу TLS. На цей час рекомендується використовувати TLS 1.2, оскільки ця версія протоколу забезпечує максимальний рівень безпеки. Захист на рівні хмари забезпечується різними методами, починаючи від шифрування даних і закінчуючи їх обробкою в хмарі.

Слід зазначити, що існуючі системи Інтернет речей, як і інші інфокомунікаційні мережі вразливі до багатьох атак, таких як відмова в обслуговуванні, підслуховування, віруси, веб-атаки и т.д. Причому, використовувати існуючі методи захисту даних не завжди можливо, це обумовлено вперш за все обмеженістю ресурсів кінцевих пристроїв. Одним з можливих рішень в області безпеки – це використання алгоритмів легковагової та малоресурсної криптографії при передачі повідомлень між пристроями, які мають не достатньо пам'яті, потужності та інших ресурсів. На сьогодні відомі такі симетричні легковагові алгоритми, як AES, Hight, PRESENT, TEA,XTEA, RC5 та асиметричні – ECC і RSA.

В даній роботі проведено порівняльний аналіз легковагових криптографічних алгоритмів (RSA, ECC, AES, XTEA), призначених для пристроїв з такими обмеженими ресурсами як пам'ять, споживання енергії та час виконання (табл.1).

Таблиця 1. - Аналіз легковагових криптографічних алгоритмів

Алгоритм	Час виконання, мс		Використання пам'яті, байт		Споживання енергії CPU, мДж	
	Шифрування	Дешифрування	ROM	RAM	Шифрування	Дешифрування
RSA	1,375	13,75	7346	643	23,03	40,17
ECC	1,084	1,08	9804	564	1,86	1,85
AES	0,576	0,676	5490	699	0,96	1,12
XTEA	0,624	0,624	3012	278	1,04	1,04

Висновки

В результаті проведеного аналізу отримали, що асиметричні алгоритми характеризуються найкращою продуктивністю, що в майбутньому можна використовувати для створення гібридної схеми обміну ключами, симетричні алгоритми, в свою чергу, виграють за показниками часу для шифрування даних. Як висновок, треба зазначити, що симетричні алгоритми забезпечують конфіденційність, цілісність, мають невеликий розмір ключа, і є менш складними, але вони не пропонують автентичність і характеризуються складною задачею розподілу ключів. З іншого боку, асиметричні алгоритми забезпечують конфіденційність, цілісність і автентичність відбитку, але мають занадто великий розмір ключа, що робить їх більш складними і не підходять для обмежених ресурсів системи IoT. Таким чином, стає необхідність розробки безпечного гібридного алгоритму, який поєднає в собі найкращі характеристики легковагових симетричних і асиметричних алгоритмів з мінімізацією часу виконання з відповідними енергетичними потребами та забезпеченням конфіденційності, цілісності та автентичність відбитку.