УДК 004.021

# ПОРІВНЯННЯ ПРОГРАМНОЇ І АПАРАТНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ ШИФРУВАННЯ AES

***І.В. ШАПОВАЛ***[1*]

[1]*студент, НТУУ «КПІ», Київ, Україна*
[*]*email: _shapoval_ivan@ukr.net*

Advanced Encryption Standard (AES), на даний момент найбільш розповсюджений алгоритм шифрування. Шифрування/дешифрування проходить за певну кількість раундів число яких залежить від довжини ключа: 128/192/256 біт, відповідно 10/12/14 раундів. Всі раунди ідентичні окрім останнього. Також від довжини ключа залежить і криптостійкість алгоритму. Одним із основних параметрів алгоритму шифрування є його швидкість роботи, оскільки це значно впливає на швидкодію програм, які використовують даний алгоритм. Тому метою даної роботи буде дослідження швидкодії програмної і апартної реалізації алгоритму, і в подальшому створення конкуренто спроможної, в плані швидкості роботи, її апаратної реалізації.

Шифрування складається з таких функції: ExpandKey – функція для визначення раундового ключа; SubBytes – функція для підстановки байтів (використовуючи таблицю підстановок); ShiftRows – функція, що забезпечує циклічний зсув на визначену величину; MixColumns – функція, що змішує данні в кожному стовбці з State; AddRoundKey – складення раундового ключа зі State.

Також для алгоритму використовуються такі змінні: State (форма) – матриця байтів 4x4; RoundKey (раундовий ключ) – унітарний ключ який використовується в кожному раунді шифрування (обраховується на базі основного ключа для кожного раунду); State – матриця станів або проміжний результат шифрування; S-Box – таблиця підстановок використовується для заміни байтів в процедурі ExpandKey.

Алгоритм програми представлений у вигляді блок-схеми на рис. 1.

Розшифровка проходить аналогічним шляхом тільки в зворотному порядку.

Для порівняння апаратної і програмної реалізацій даного алгоритму було вибрано мову програмування C++ скомпільовану на Microsoft Visual C++ 2005 SP1 і запущено на Intel Core 2 процесорі 1.83 ГГц, на Windows Vista 32-біта x86, також були використані процедури мови асемблера для цілочисленої арифметики. Результати представлені в табл. 1.

Цикли на байт є одиницею вимірювання, яка показує кількість тактів мікропроцесора за які він буде обробляти один байт. Він широко використовується в якості часткового показника реальної продуктивності для криптографічних функцій.

Таблиця 1 – Швидкість алгоритму шифрування

| Алгоритм | МБ/с | Цикл на байт |
|---|---|---|
| AES (128- біт) | 96 | 12,6 |
| AES (192- біт) | 113 | 15.4 |
| AES (256- біт ) | 139 | 18.2 |

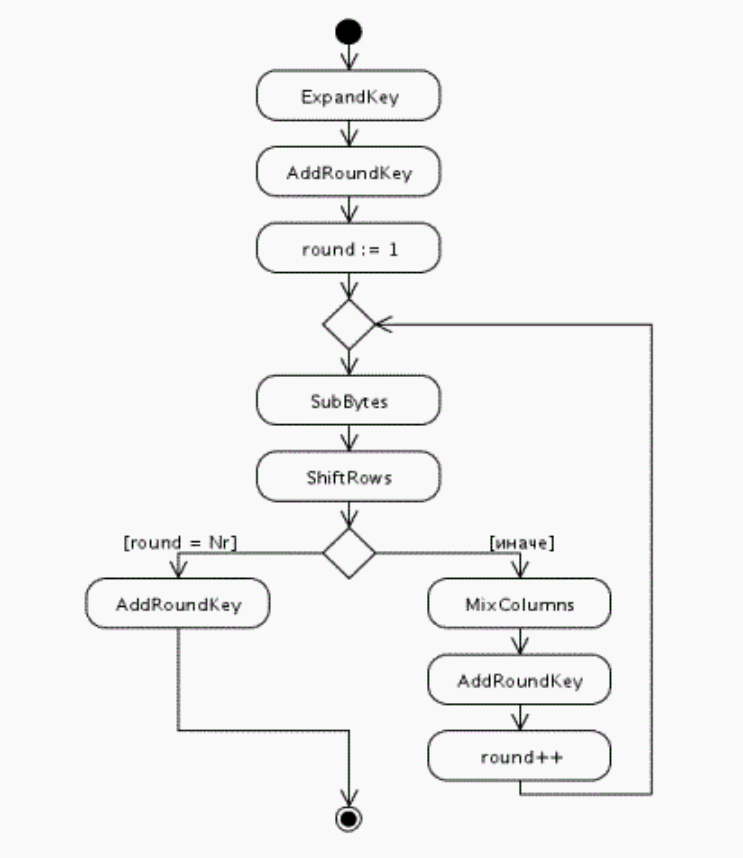


Рис. 1 – Блок-схема алгоритму AES

Для порівняння в табл. 2 представлено швидкодію алгоритму AES (128-біт) на процесорах іншої архітектури (amd64).

Таблиця. 2 – Швидкодія алгоритму на процесорах архітектури amd64

| Процесор | Цикл на байт |
|---|---|
| AMD Athlon 64 (15,75,2) | 13,125 |
| Intel Pentium D (f64) | 15,4 |
| AMD Opteron 240 (f58) | 13,45 |

Для апаратної реалізації було вибрано FPGA Spartan-II XC2S30-6 і для ключа розміром 128 було досягнуто показник швидкості 166 МБ/с. Очевидно, це майже в двічі більше, ніж відповідна програмна реалізація. Слід зауважити, що швидкодія алгоритму AES на процесорах x86, починаючи з Intel Core i7-980X Extreme Edition, буде мати кращі показники, оскільки вони підтримують систему команд для даного алгоритму.