

УДК 004.056.55

Чухно І.С.¹, Варов А.П.¹, Кладько К.С.¹, Козіна Г.Л.²

¹ студ. гр. РТ-818 НУ «Запорізька політехніка»

² канд. фіз-матем. наук, доц. НУ «Запорізька політехніка»

ОСОБЛИВОСТІ ДЕРЖАВНОГО СТАНДАРТУ ШИФРУВАННЯ УЗБЕКІСТАНУ

З появою в 2001 році Американського стандарту шифрування FIPS 197 (на базі алгоритму Rijndael [1]) поширились принципи його побудови при створенні нових національних стандартів шифрування.

Зокрема Український стандарт шифрування ДСТУ 7624:2014 [2], введений в дію в 2015 році, використовує ту ж саму архітектуру (SP-сітка) і базові операції, що і алгоритм Rijndael. В алгоритмі Rijndael в якості базових операцій запропоновано додавання за модулем 2 (додавання раундового ключа до вхідного масиву даних), заміна байтів за допомогою таблиці заміन, зсув бітових рядків, лінійне перетворення (множення на задану квадратну матрицю). В Українському стандарті, крім цього, запропоновано операція додавання за модулем 2^{64} .

Китайський стандарт шифрування для захисту бездротових мереж SM4 [3] використовує іншу архітектуру шифру (сітка Фейстеля), однак операції додавання за модулем 2, заміна байтів за допомогою таблиці заміन, зсув бітових рядків також є базовими в цьому стандарті.

На відміну від розглянутих стандартів Державний стандарт шифрування Узбекистану O'z_DSt_1105-2009 [4] має досить оригінальні особливості.

Математичною особливістю алгоритму є введення алгебри діаматриць модульної арифметики. Основною операцією алгебри діаматриць, що використовується в процедурах зашифрування та розшифрування, є операція обертання діаматриці в матрицю за заданим модулем.

В алгоритмі шифрування O'z_DSt_1105-2009 використовуються два секретні ключі: ключ шифрування та функціональний ключ, на базі яких формуються етапні ключі.

Алгоритм шифрування O'z_DSt_1105-2009 складається з 8 етапів.

На кожному етапі криптографічні перетворення здійснюються за допомогою чотирьох базових операцій: Qo'shBosqichKalit, Aralash, Sur, BaytAlmash.

Операція Qo'shBosqichKalit збігається з операцією додавання раундового (етапного) ключа до вхідного двовимірної масиву даних (додавання за модулем 2).

Для виконання операції Aralash двовимірний вхідний масив розбивається на діаматричні частини. Перетворення виконується з використанням сеансово-етапних ключів.

В операції Sur стовпці двовимірної вхідного масиву зсуваються циклічно вниз, а рядки відповідно циклічно вправо.

Операція BaytAlmash збігається з операцією заміна байт.

При реалізації алгоритму шифрування O'z_DSt_1105-2009 найбільш складною є робота з діаматрицями спеціальної структури.

Діаматриця спеціальної структури порядку 4x4 формується на основі десяти елементів на байтовому рівні.

В таблиці 1 наведена діаматриця, сформована на основі елементів d0, d1, d2, d3, d4, d5, d6, d7, d8, d9. Всі діагональні елементи матриці ідентичні.

Таблиця 1 – Діаматриця спеціальної структури

d7	d0	d1	d2
d8	d7	d8	d8
d9	d3	d7	d9
d4	d5	d6	d7

Діагональний елемент діаматриці спеціальної структури порядку 4x4 знаходиться як добуток діагонального елемента на три співмножники, кожен з яких являє собою суму елементів стовпця з елементом, розташованим на одному рядку з діагональним по сусідству справа.

Перевірка умов оборотності діаматриці є основною вимогою до параметрів алгоритму шифрування.

Таким чином, процес реалізації алгоритму шифрування O'z_DSt_1105-2009 Узбекистану потребує особливого підходу і значних часових ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Note on naming [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/228731433_Note_on_naming
2. Єфіменко А. А. Порівняльний аналіз алгоритму симетричного блокового перетворення «Калина» (ДСТУ 7624:2014) з іншими міжнародними стандартами шифрування даних [Електронний ресурс] // Єфіменко А. А., Байлюк Є. М., Покотило О. А. – Режим доступу: https://www.zvir.zt.ua/images/stories/ZbirnikNP/19_12_18/17.pdf
3. GM/T 0002-2012 SM4 Block Cipher Algorithm [Електронний ресурс] – Режим доступу: <http://www.codeofchina.com/standard/GMT0002-2012.html>
4. O'z_DSt_1105-2009 – Государственный стандарт шифрования Узбекистана [Електронний ресурс] – Режим доступу: [https://tace.uz/docs/O'z_DSt_1105-2009_\(ru\).pdf](https://tace.uz/docs/O'z_DSt_1105-2009_(ru).pdf)