УДК 621.396.946

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В МОБІЛЬНИХ МЕРЕЖАХ

Зубик С. О.
Інститут телекомунікаційних систем НТУУ «КПІ», Україна
E-mail: zubyk.sergey@gmail.com

Way to improve security of mobile networks

Examining types of attacks and way to protect mobile networks, increasing the efficiency of information security through using cryptography algorithms.

This paper gives general information about the standards of mobile communication, described attacks on mobile networks, discussed ways to protect mobile networks and both the GSM and UMTS, the program implemented block cipher KASUMI.

KASUMI – блочний шифр, що використовується в мережах стільникового зв'язку 3GPP, найбільш широке визнання отримав при використанні в мобільних мережах стандарту UMTS, але зараз активно впроваджується в стільниковій мережі GSM, де позначається A5/3. KASUMI був розроблений групою SAGE (Security Algorithms Group of Experts), яка є частиною Європейського Інституту по Стандартизації в області Телекомунікацій (ETSI). За основу був узятий існуючий алгоритм MISTY1 і оптимізований для використання в стільниковому зв'язку.KASUMI використовує 64-бітний розмір блоку і 128-бітний ключ у 8-раундовій схемі Фейстеля. У кожному раунді використовується 128-бітний раундовий ключ, що складається з восьми 16-бітових підключів, отриманих з вихідного ключа фіксованою процедурою генерації підключів.

Алгоритм KASUMIє алгоритмом Фейстеля з різними парними і непарними раундами. У непарних раундах, в порівнянні з парними раундами виконується додатково операція FL, яка також виконується і по завершенні останнього раунду. Кількість раундів дорівнює восьми. На рисунку 1 представлена послідовність операцій, виконуваних при шифруванні даних за алгоритмом KASUMI.

Таким чином, при виконанні операції FL32-бітне вхідне значення розбивається на два блоки по 16 біт, над якими виконуються операція додавання за модулем 2 і побітові логічні операції, причому в логічних операціях беруть участь певні фрагменти розширеного ключа шифрування для операції K_{L1} і K_{L2}.

Більш складною є операція FO. В даній операції 32-бітове вхідне значення також ділиться на два 16-бітових фрагменти, один з яких обробляється операцією додавання за модулем 2 з визначеним фрагментом

ключа для операції FO (K_{Ox}) і операцією FI, після чого значення даних в цих блоках додаються за модулем 2 і міняються містами.

На відміну від операцій FL і FO, операція FI обробляє 16-бітові блоки вхідних даних.

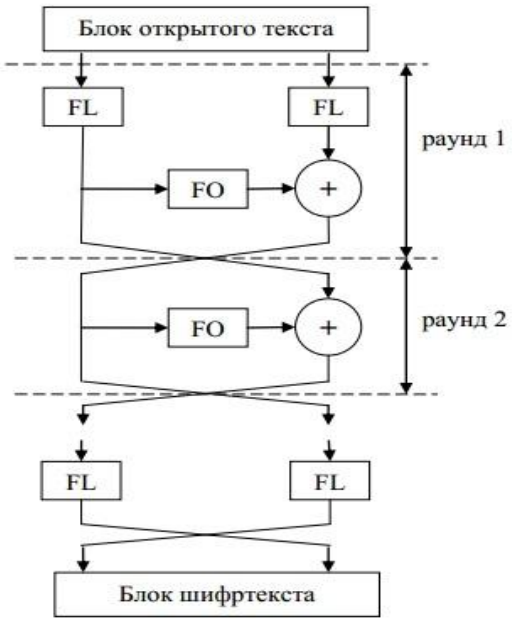

Рис. 1 Послідовність шифрування даних за алгоритмом KASUMI.

Це 3-раундова мережа Фейстеля, яка оброблює 7-бітний і 9-бітний блоки, над якими виконуються наступні операції:

- Табличні заміни S7 і S9 над 7 - і 9-бітовим блоком відповідно;

- Додавання блоків між собою за модулем 2, причому в першому і третьому раундах 7-бітний блок доповнюється нулями, і результатом додавання є 9-бітний блок, а в другому раунді при додаванні відкидаються два лівих біта 9-бітного блоку і результатом додавання є 7-бітний блок;

- Додавання за модулем 2 відповідних блоків з 7- і 9-бітовими фрагментами розширеного ключа шифрування K_{L1} і K_{L2}, що виконується у другому раунді;

Кожен раунд KASUMI отримує ключі із загального ключа K наступним чином:

- 128-бітний ключ K поділяється на 8 ключів: $K = K_1 || K_2 || K_3 || \dots || K_8$;

- Обчислюється другий масив $K_{j'} = K_j \oplus C_j$, де C_j визначається матрицею, яка наведена в таблиці 1.

Таблиця 1. Матриця значень C_j для розрахунку K_j,

C_1	0x0123
C_2	0x4567
C_3	0x89AB
C_4	0xCDEF
C_5	0xFEDC
C_6	0xBA98
C_7	0x7654
C_8	0x3210

- Ключі для кожного раунд обчислюються, як показано в таблиці 4.2

Таблиця 2. Розрахунок ключів для кожного раунду.

Ключ	1	2	3	4	5	6	7	8
$KL_{i,1}$	K1<<<1	K2<<<1	K3<<<1	K4<<<1	K5<<<1	K6<<<1	K7<<<1	K8<<<1
$KL_{i,2}$	K3'	K4'	K5'	K6'	K7'	K8'	K1'	K2'
$KO_{i,1}$	K2<<<5	K3<<<5	K4<<<5	K5<<<5	K6<<<5	K7<<<5	K8<<<5	K1<<<5
$KO_{i,2}$	K6<<<8	K7<<<8	K8<<<8	K1<<<8	K2<<<8	K3<<<8	K4<<<8	K5<<<8
$KO_{i,3}$	K7<<<13	K8<<<13	K1<<<13	K2<<<13	K3<<<13	K4<<<13	K5<<<13	K6<<<13
$KI_{i,1}$	K5'	K6'	K7'	K8'	K1'	K2'	K3'	K4'
$KI_{i,2}$	K4'	K5'	K6'	K7'	K8'	K1'	K2'	K3'
$KI_{i,3}$	K8'	K1'	K2'	K3'	K4'	K5'	K6'	K7'

Шифр KASUMI реалізується функцією безпеки f_8в стандартах UMTS та CDMA, причому він функціонує в режимі зворотного зв'язку, де функція f_8 використовується для генерування блоків ключового потоку, які побітово додаються до блоків відкритого тексту за модулем 2.

У 2009 році було опубліковано атаку на KASUMI «методом бумерангу», який зламує шифр швидше, ніж повний перебір. Складність атаки дорівнює 2^{76}, що порівняно з алгоритмомA5/1, для якого складність атаки складає 2^{40}, більше на 10-ки порядків. Отже шифр KASUMI є найбільш криптостійким і є оптимальним вибором для шифрування інформації в мобільних мережах.

Література

1. Ветров Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров. - СПб.: Издательство Политехника ун-та, 2011. - 174 с.
2. *Куприянов А.И., Сахаров А.В., Швецов В.А.* Основы защиты информации: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2006. – 256 с.
3. *Чекалин А.А., ЗаряевА.В.* Защита информации в системах мобильной связи: Учебное пособие для вузов. - М.: Горячая линия – Телеком, 2005. - 171с.
4. *Ярочкин В.И.* Безопасность информационных систем (Безопасность предпринимательства). – М.: Ось-89, 1996. – 318 с.