Міністерство освіти і науки, молоді та спорту України
Вінницький національний технічний університет
Харківський національний економічний університет
Об'єднаний інститут проблем інформатики НАН Білорусі
Азербайджанська державна нафтова академія
Бєлгородський державний університет, Росія
Гірничо-металургійна академія AGH, Польща
Новий університет Лісабона, Португалія
Університет ЛІОН 2 ім. Люм'єра, Франція
Інститут інженерів з електротехніки та електроніки (IEEE), Українська секція

Тези доповідей Тертьої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації»

м. Вінниця, Україна
20-22 квітня 2011 року

Тезисы докладов Третьей Международной научно-практической конференции «Методы и средства кодирования, защиты и сжатия информации»

г. Винница, Украина
20-22 апреля 2011 года

ВНТУ 2011

УДК 004+681.3+621.3
М54

Відповідальний редактор В. А. Лужецький

Матеріали статей опубліковані в авторській редакції

Методи та засоби кодування, захисту й ущільнення
М54 інформації. Тези доповідей Третьої Міжнародної науково-практичної конференції. м. Вінниця, 20-22 квітня 2011 року. – Вінниця: ВНТУ, 2011. – 231 с.
ISBN 978-966-641-406-2

Збірка містить матеріали доповідей третьої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за п'ятьма основними напрямками: методи та засоби кодування інформації; методи та засоби криптографічного захисту інформації; інформаційна безпека комп'ютерних систем; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

УДК 004+681.3+621.3

ISBN 978-966-641-406-2

УДК 004.056.055

БЛОКОВІ ШИРФРИ НА ОСНОВІ ПСЕВДОНЕДЕТЕРМІНОВАНИХ ПОСЛІДОВНОСТЕЙ КРИПТОПРИМІТИВІВ

А. В. Остапенко, аспірант
Вінницький національний технічний університет
asja87@gmail.com

Відповідно до реалізацій функцій шифрування виділяють блокові шифри (БШ) побудовані на основі мереж Фейстеля (Feistel network), чергування процедур перестановок і підстановок (SP-мереж), структури «квадрат» (Square) та керованих операцій.

Як правило, алгоритми зашифрування та розшифрування блокових шифрів є ітераційними і складаються з послідовності R перетворень (раундів). Ці перетворення описуються однією і тією ж функцією $F()$, але в якості аргументів використовуються результати попереднього перетворення і раундовий ключ k_r, який отримуються із загального секретного ключа k. Тобто алгоритм блокового шифру є детермінованим (ДБШ).

Зображення узагальненої схеми раундового перетворення ДБШ представлено на рис.1, де k_r – раундовий ключ; m – вхідне повідомлення; m_j – блок вхідного повідомлення; $F(.)$ – функція раундового перетворення; c_j – блок криптограми після r-го раунду.

Оскільки набір і послідовність виконання операцій є детермінованими, криптографічна стійкість розглянутих блокових шифрів визначається розміром ключа, складністю виконуваних операцій або кількістю раундів, у разі використання простих операцій.

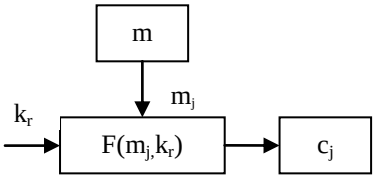

Рис.1 Узагальнена схема раунду перетворення ДБШ

Для зменшення кількості раундів, а отже підвищення швидкості шифрування, у разі використання набору простих операцій, пропонується застосовувати недетермінновану послідовність операцій (з точки зору зловмисника), яка визначається секретним ключем.

Таким чином, блоковий шифр на основі псевдонедетермінованих послідовностей криптопримітивів (ПНБШ) складається з відомих перетворень, що дозволяє теоретично оцінити стійкість шифру, відповідно до правила Керкоффа, але порядок їх застосування визначається секретним ключем і тому є недетермінованим процесом з точки зору криптоаналітика.

Загальний вигляд раундового перетворення ПНБШ представлено на рис. 2, де Q – ознака виділена з раундового ключа k_r; m_j^* – блок вхідного повідомлення сформований відповідно до ознаки; B – базові операції; $\Phi()$ – раундова функція ПНБШ побудована з базових операцій у відповідності до ознаки; c_j^* – блок криптограми після r-го раунду перетворення ПНБШ.

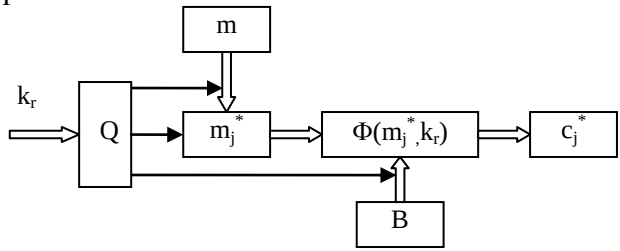

Рис.2 Узагальнена схема раунду перетворення ПНБШ