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

БЛОКОВИЙ ШИФР НА ОСНОВІ ПЕРЕСТАНОВОК ТА ПІДСТАНОВОК

В. А. Лужецький, д.т.н., професор;
І. С. Горбенко, студент
Вінницький національний технічний університет

Запропоновано блоковий шифр, в основу якого покладено новий підхід, що передбачає використання перестановок блоків різної довжини та гамування на основі псевдовипадкової послідовності операцій.

Алгоритм зашифрування складається з двох етапів: передобчислення та власне зашифрування. На етапі передобчислення визначається кількість блоків різної довжини, на які буде розбиватись повідомлення в процесі шифрування. Розрядність блоку може бути від 1 до 8 байтів.

Етап зашифрування складається з операцій перестановки та гамування. Оскільки перестановці підлягає кількість блоків, яка є змінною (залежить від довжини повідомлення і псевдовипадкового характеру довжини блоків), то жоден з відомих генераторів псевдовипадкових послідовностей (ПВП) не може бути використаний для формування правил перестановок, оскільки не завжди можна підібрати параметри стійкого генератора для заданого періоду послідовності для одних типів генераторів або не існує загальних методик побудови генераторів інших типів. Тому пропонується оригінальний метод генерування ПВП, який є основою правил перестановок.

Цей метод полягає в такому. Нехай кількість блоків N, їх номери $n_i \in \{1,2,...,N\}$. Послідовність номерів блоків

розбивається на дві групи – $G_0 = \{1,..., \left]\frac{N}{2}\right[\}$ та $G_1 = \{\left]\frac{N}{2}\right[+ 1,..., N\}$. Черговий номер блоку визначається символом s_i ПВП, що вказує на групу, з якої вибирається цей номер. Якщо символ ПВП «0», то номер вибирається з групи G_0, а якщо «1», то з групи G_1.

Операції гамування реалізується з використанням двох генераторів, один з яких формує безпосередньо гаму, а другий – код, що відповідає виконуваній операції. Використовується 8 операцій, за якими здійснюється накладання гами:

$$b \oplus g;\ \overline{b \oplus g};\ (b+g) \bmod 2^8;\ (\bar{b}+g) \bmod 2^8;\ (b+\bar{g}) \bmod 2^8;$$
$$(\overline{b+g}) \bmod 2^8;\ (b-g) \bmod 2^8 \text{ або } (g-b) \bmod 2^8.$$

Розшифрування, так само, як і зашифрування, складається з двох етапів: передобчислення та власне розшифрування. Оскільки алгоритм блокового шифрування симетричний, то розшифрування складається з тих самих операцій, що й зашифрування, але у зворотному порядку.

Секретний ключ блокового шифру складається з таких частин:

1) параметри генератора ПВП для визначення довжин блоків;
2) параметри генератора ПВП для реалізації правил перестановки;
3) параметри генератора ПВП гами;
4) параметри генератора ПВП кодів операцій для гамування.

Криптографічна стійкість запропонованого блокового шифру забезпечується перестановками блоків різної довжини та псевдовипадковою послідовністю набору операцій накладання гами.