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

©Автори статей, 2011
©Упорядкування, Вінницький національний технічний університет, 2011

УДК 681.3

ШИФРУВАННЯ ДАНИХ НА ОСНОВІ ПЕРЕСТАНОВОК

В. А. Лужецький, д.т.н., професор;
І. В. Нетяга, студент
Вінницький національний технічний університет
netyaga.inna@mail.ru

Клод Шеннон у своїй роботі про системи секретного зв'язку показав, що шифрування даних може бути реалізовано за допомогою операцій перестановок та підстановок (замін).

В сучасних блокових шифрах реалізуються достатньо прості перестановки і основна увага приділяється реалізації підстановок. Недоліком операцій перестановок є те, що достатньо просто здійснити злам правила перестановки, використовуючи всього n (кількість блоків тексту) текстів, що нав'язуються для зашифрування.

У потокових шифрах реалізуються тільки операції підстановок шляхом накладання гами. Відомо, що при наявності частини відомого відкритого тексту, можна отримати частину гами і в разі нестійкого генератора гами отримати всю гаму. Тому на практиці використовують достатньо складні генератори гами, щоб ускладнити процедуру зламу гами. Однак таке ускладнення може бути досягнуте шляхом перестановки блоків вікритого тексту. У свою чергу накладання гами на вікритий текст запобігає реалізації атаки на правило перестановок. Отже, спільне використання перестановок усіх блоків відкритого тексту та накладання гами на ці блоки забезпечує можливість побудови блокового шифру, який буде стійким до відомих атак. Саме такий блоковий шифр пропонується авторами доповіді.

При зашифрування відкритий текст M представляється як конкатенація n блоків однакової довжини: $M= m_1 \| m_2 \| ... \| m_n$. Гама теж розглядається як конкатенація n блоків гами: $G= g_1 \| g_2 \| ... \| g_n$.

За правилом перестановки P:

$$P=\begin{pmatrix} 1 & 2 \dots i \dots n \\ j_1 & j_2 \dots j_i \dots j_n \end{pmatrix} \quad (1)$$

зчитується j_i –й блок відкритого тексту і на нього накладається і-й блок гами. Таким чином одержується і-й блок зашифрованого тексту: $C_i= m_{ji} \oplus g_i$.

Повністю зашифрований текст представляється як конкатенація блоків зашифрованого тексту: $C= c_1 \| c_2\| ... \| c_n$.

При розшифруванні закритий текст розбивається на n блоків.За правилом перестановки P1 визаначається номер блоку, який буде зчитуватися і-м по порядку. На і-й блок закритого тексту накладається і-й блок гами і одержується блок відкритого тексту, номер якого j_i, який визначається правилом перестановки 1: $c_i \oplus g_i = m_{ji}$.

Розрядність блоків відкритого тексту і гами може бути різною, яка визначається розрядністю апаратури за допомогою якої реалізується шифрування.

Для генерування гами може бути використаний регістр зсуву з лінійним зворотнім зв’язком за умови, що довжина гами буде наперед більшою довжини даних, що підлягають шифруванню.

Генерування правила перестановки здійснюється за формулами:

$$j_i = ((n-1) \cdot a_i \oplus b) \bmod(n),$$

де

$$a_i = (a_{i-1} \oplus 1) \bmod(n), \quad a_0 = a,$$

де $0 < a, b \leq n-1$

Складовими сектретного ключа є код початкового стану регістра зсуву з лінійним зворотнім зв’язком та коди чисел a та b.