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 004.056.55

ШИФРУВАННЯ В РЕЖИМІ ПСЕВДОВИПАДКОВОГО ЗЧЕПЛЕННЯ БЛОКІВ ДАНИХ

О. В. Дмитришин, аспірант
Вінницький національний технічний університет
olexanderdm@gmail.com

На сьогоднішній день, одним із ефективних засобів боротьби із перекрученням та несанкціонованим доступом до інформації є шифрування даних, зокрема використання симетричних блокових шифрів. Методи блокового шифрування дозволяють забезпечити конфіденційність даних та можуть бути використані в методах контролю цілісності інформації і автентифікації джерела інформації тощо.

З метою усунення недоліків, що характерні будь-якому шифру, незалежно від його конструктивних особливостей, застосовують базові режими блокового шифрування, які описано в стандарті США «SP 800-38A 2001 Edition – Recommendation for Block Cipher Modes of Operation. Methods and Techniques».

Проте, режими електронної кодової книги (ECB), зчеплення блоків зашифрованого тексту (CBC) і режим зворотного зв'язку за зашифрованим текстом (CFB) є потенційно вразливими до атак на основі пар відкритих та відповідних зашифрованих текстів. Окрім того, використовуючи атаку «дня народження» і атаку зустрічі по середині до режимів CBC та CFB можна знайти такі n-бітні пари зашифрованих текстів $(C_{j-1}, C_j) = (C_{i-1}, C_i)$, що значення n-бітних пар відповідних відкритих текстів P_i та P_j $(i<j,\ i\geq 1)$ будуть рівні між собою. Це в свою чергу дозволяє на підс-

таві відомих пар відкритих і зашифрованих текстів дізнаватися про зміст даних нових зашифрованих текстів, а в межах одного зашифрованого тексту виконувати спробу порушувати цілісність зашифрованого тексту за рахунок модифікації зашифрованого тексту між *i*-м та *j*-м блоками.

Для підвищення стійкості режиму CBC пропонується використовувати псевдовипадкове зчеплення поточного блоку відкритого тексту із попередніми блоками відкритого тексту або зашифрованого тексту.

Процес зашифрування і-го блоку даних полягає у виконанні таких перетворень:

$$P_0 = IV,\ C_0 = E_K(IV),$$
$$C_i = E_K(H_i),$$
$$H_i = P_i \oplus H_{i-1} \oplus V(s_i, P_{i-1}, C_{i-1}),$$

а розшифрування

$$H_i = D_K(C_i),$$
$$P_i = H_i \oplus H_{i-1} \oplus V(s_i, P_{i-1}, C_{i-1}),$$

де $E_K()$, $D_K()$ – відповідно функції зашифрування та розшифрування n-бітного блоку даних;

K – n-бітний секретний ключ;

H_i – i-й n-бітний вхідний блок даних, $H_0 = 0$;

$V()$ – функція відображення $2n$-біт в n-біт;

s_i – i-й біт з виходу генератора псевдовипадкових послідовностей $s_i \in \{0, 1\}^2$. Якщо $s_i = 0$, то

$$V(s_i = 0, P_{i-1}, C_{i-1}) = P_{i-1},$$

якщо $s_i = 1$, то

$$V(s_i = 1, P_{i-1}, C_{i-1}) = C_{i-1};$$

IV – n-бітний вектор ініціалізації.

Запропонований режим забезпечує можливість протидіяти атаці «дня народження» і атаці на основі пар відкритих та відповідних зашифрованих текстів за рахунок поширення помилок, коли зміна в і-му блоці даних поширюється на всі подальші блоки відкритого тексту і за рахунок маскування значення блоку даних, що зашифровується..