УДК 681.3

ШИФРУВАННЯ ДАНИХ НА ОСНОВІ ПЕРЕСТАНОВОК

Науковий керівник - д.т.н., професор Лужецький В.А.
Нетяга І.В.

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: $C= c_1\|c_2\|...\| c_n$.

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 $0 < a, b \le n-1$

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