УДК 004

О.С. Черняков
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ФОРМАЛЬНА МОДЕЛЬ І КЛАСИФІКАЦІЯ ШИФРІВ

O.S. Cherniakov

FORMAL MODEL AND CLASSIFICATION OF CHIPHERS

Введемо формальне визначення шифру і його складових частин [1]. Нехай T, C і K - кінцеві безлічі можливих відкритих текстів, шифротекстів та ключів. Зазвичай кожна з цих множин являє собою множину слів в деякому алфавіті, причому алфавіти відкритих текстів, шифротекстів і ключів можуть розрізнятися. Для більшості сучасних систем шифрування відкриті тексти, шифротексти і ключі являють собою слова в алфавіті {0,1}, тобто послідовності нулів та одиниць.

Процедура шифрування задається функцію Ek: T → C, яка відображає перетворення безлічі відкритих текстів в безліч шифротекстів залежно від деякого ключа ключа k.

Аналогічно, процедура розшифрування Dk: C → T також залежить від ключа k і відображає перетворення безлічі шифротекстів в безліч відкритих текстів.

Так як одержувач завжди повинен мати можливість по шифротексту відновити вихідний текст, то при будь-якому k з K функції Ek і Dk повинні задовольняти умові: Dk ° Ek = I, де I - тотожне відображення T в T.

Тут необхідні деякі пояснення. У багатьох криптографічних системах передбачається, що відкритий текст, шифротекст і ключ - це цілі числа. Таке припущення зручно для побудови і обґрунтування алгоритмів шифрування і розшифрування, оскільки числові функції добре вивчені.

Також часто при реалізації алгоритмів шифрування і розшифрування буває зручно вважати, що довжина ключа, використовуваного для перетворення тексту, дорівнює довжині самого тексту або залежить від довжини тексту якимось певним чином. Очевидно, що якщо ключ використовується для шифрування кількох текстів, його довжина не може залежати від довжини кожного конкретного тексту.

У цьому випадку перед шифруванням тексту роблять так: на основі даного секретного ключа фіксованої довжини з допомогою певного алгоритму формують ключ шифрування, що має необхідну довжину, і саме отриманий ключ шифрування використовують для перетворення тексту.

Найпростішим способом сформувати ключ шифрування потрібної довжини є періодичне повторення символів секретного ключа. Наприклад, з секретного ключа k = (k1, k2, ..., kn) можна отримати ключ шифрування (k1, k2, ..., kn, k1, k2, ..., kn, k1, k2, ..., kn, k1 ...) довільної довжини.

Основною вимогою при реалізації криптосистеми є використання криптостійкого алгоритму шифрування, бо саме він виступає гарантом стійкості системи до різного роду несанкціонованих дій з боку порушника. Тому вибір алгоритму вважається одним з найважливіших завдань при побудові криптостійкої системи захисту інформації.

Література

1. Алферов А.П.,Зубов А.Ю.,Кузьмин А.С.,Черемушкин А.В. Основы криптографии: Учебное пособие. — М.: Гелиос АРВ, 2001. — 480 с.