

ЗАГАЛЬНИЙ ПІДХІД ДО КОМБІНОВАНИХ ШИФРІВ

Главчев М.І., Новікова А.В.

Національний технічний університет

"Харківський політехнічний інститут", м. Харків

Створення нових криптоалгоритмів дуже складний і математично трудомісткий процес.

Альтернативним джерелом створення нових криптосистем є можливість комбінування з існуючих, перевірених фахівцями, алгоритмів.

До способів створення можна віднести наступне:

1) Використання послідовно різних криптоалгоритмів з ключем заданої довжини.

2) Повторне використання одного алгоритму з різними ключами.

3) Різні алгоритми і різні ключі.

Можливо, як варіант, – це використання симетричних алгоритмів, які мають відмінні функції шифрування і дешифрування з різними ключами (як робиться в потрійному DES).

Головна проблема, що виникає при створенні комбінованих шифрів, – це оцінка їх криптостійкості.

На підставі існуючих вимог до криптосистем, якість шифрування має бути не гірше самого слабкого з алгоритмів.

У якості напрямку розробки представляється доцільним використовувати симетричні блокові і потокові шифри, створені Роном Рівестом з наступних причин:

1) Ці шифри зарекомендували себе досить надійними і стійкими до криптоатаки.

2) Вони дозволяють підтримувати ключі однакової довжини.

3) Ці шифри дозволяють реалізацію як апаратну, так і програмну.

В системі пропонується використовувати єдиний ключ для всіх шифрів, який також буде визначати послідовність використання в криптосистемі обраних алгоритмів.

Послідовність використання криптоалгоритмів буде обчислюватися на підставі хеш-перетворення самого ключа.

Представляє труднощі оцінка якості криптосистеми з урахуванням комбінування алгоритмів і в порівнянні з однозначною послідовністю. Вона буде залежати від довжини ключа, від криптостійкості кожного алгоритму, від кількості раз використання алгоритму (повторне використання рекомендується з іншим ключем) і варіантів комбінаторної послідовності застосовуваних алгоритмів.