УДК 004.021
Пйонтко Н. – ст. гр. СН-41
Тернопільський національний технічний університет імені Івана Пулюя

МІЖНАРОДНИЙ АЛГОРИТМ ШИФРУВАННЯ ДАНИХ (IDEA)

Науковий керівник: асист. Боднарчук І.О.

З давніх-давен людство старалося захистити приватну інформацію від стороннього впливу: несанкціонованого розкриття інформації, можливої несанкціонованої зміни інформації і т. д. Особливо важливим був і є захист інформації при її передачі від відправника до отримувача. Для захисту використовувався і використовується цілий ряд заходів, одним з яких є шифрування, що включає в себе заміну символів (елементів) повідомлення, у відповідності з певними правилами, їх перестановку. З розвитком комп'ютерних технологій захист інформації вийшов на абсолютно новий рівень, адже використовуючи величезні обчислювальні можливості, можна створювати не лише дуже складні алгоритми шифрування, а й розробляти ефективні алгоритми взлому захисту. Проте незважаючи на ускладнення алгоритмів шифрування в їх основі як і раніше лежать принципи заміни елементів повідомлення за певним правилом на інші елементи або/і їх перестановка.

Метою нашого дослідження є вивчення і аналіз алгоритму шифрування IDEA, який є міжнародним стандартом для захисту інформації.

IDEA являє собою симетричний (використовує один і той же ключ для шифрування і дешифрування) блочний (здійснює обробку блоків даних розміром декілька байт) алгоритм шифрування.

Алгоритм шифрування IDEA розроблений і запатентований швейцарською фірмою Ascom. Перші версії алгоритму було створені в 1990 році. В 2000 році цей алгоримт був визнаним як міжнародний стандарт захисту інформації.

В своїй роботі IDEA використовує блоки даних розміром 64 біти і криптографічний ключ довжиною 128 біт (така довжина ключа забезпечує велику криптографічну стійкість при взломі шифру методом простого перебору ключа). Внутрішні перетворення даних базуються в основному на трьох математичних операціях: побітове "виключаюче або", додавання цілих чисел по модулю 2^{16} і множення цілих чисел по модулю $2^{16}+1$. Крім цих перетворень використовується також перестановка бітів блоку. Процес шифрування поділений на так звані раунди (етапи). Кожен раунд здійснює виконання в певній послідовності вище зазначених математичних операції і завершувальних перестановок. Застосування цих різних по своїй суті математичних операцій забезпечує високу складність перетворення вхідного потоку даних, що значно ускладнює його криптоаналіз.

Завдяки використовуваним у алгоритмі перетворенням його можна легко реалізувати апаратно за допомогою інтегральних схем. Апаратна реалізація алгоритму забезпечує набагато більшу швидкодію роботи, ніж при програмній реалізації. Ця особливість широко використовується при апаратному шифруванні потоку даних у мережах.

Підсумовуючи, можна стверджувати, що міжнародний алгоритм шифрування IDEA є стійким до криптоаналізу алгоритмом, як з точки зору простого перебору ключа (потрібно перебрати 2^{128} ключів), так і з точки зору виявлення іншим методів взлому шифру (стійкий до диференціального криптоаналізу). IDEA використовується багатьма компаніями для передачі даних між своїми підрозділами і при передачі даних від сервера до клієнта. Цей алгоримт є чудовим рішення задачі захисту інформації.