46-та наукова конференція молодих дослідників ОНПУ-магістрантів
"Сучасні інформаційні технології та телекомунікаційні мережі". Одеса: ОНПУ, 2011, вип. 46.

АЛГОРИТМИ БЛОЧНОГО ШИФРУВАННЯ НА ОСНОВІ DES

Чудновський О.В.

Науковий керівник – зав. каф. «Інформаційної безпеки»

док. техн. наук, проф. Мазурков М.І.

Алгоритм DES був офіціальним стандартом шифрування в США на протязі 23-х років, доки його не змінили на AES(Rijndael). Причиною цьому була дуже мала довжина ключа – всього 56 біт, який у 1998 році був зламаний організацією Electronic Frontier Foundation всього за 3 дні методом простого перебору. А з застосуванням новітніх технологий час взлому алгоритму можно значно зменьшити.

У 1978 році Уітфілд Діффі, Мартін Хеллман та Уолт Тачманн створили симметричний алгоритм шифрування Triple DES (3DES) на основі алгоритму Des, в якому виключили головну ваду останнього – закороткий ключ. В 3DES застосовуються три різних ключа, загальною довжиною 168 біт. Швидкість роботі цього алгоритму втричі меньша за звичайній DES, проте для його розшифрування потрібно в мілліарди разів більше часу, ніж для зламу DES.

Збільшити кріптостійкість шифру DES можно також додавши зайві блоки в кожен раунд циклу шифрування. Вже є розробки по трьох та чотирьох рівневим алгоритмам на основі DES. Вони мають більшу кріптостійкість за двохрівневій аналог. Ми пропонуємо збільшити кількість блоків в одному раунді до п’яти(два блоки перестановки, два блоки підстановки та один блок скремблювання), та зменьшити кількість раундів до десяти. Проте це може призвести до того, що такий алгоритм буде майже ідентичним по кріптостійкості до звичайного двохрівневого DES. Залишається тільки дослідити як буде впливати на шифруваня додатковий блок скремблювання, бо пара блоків перестановки та пара блоків підстановки можуть давати той саме результат що і один блок підстановки та

один блок перестановки в двохрівневому DES, за виключенням більших потреб в часі на шифрування, адже за умови того, що раундів буде 10 – це буде еквівалентом до 20-ти раундів двохрівневого Des, не рахуючи потреб блоків скремболювання.

У 1984 році Рональд Лінн Рівест розробив алгоритм DESX, в якому використовуються 3 підключа (64+56+64 бит), перший підключ використовується для змінення блокіів, складання по модулю 2; другий — для шифрування; третій — для змінення шифрованного тексту по модулю 2. Швидкість алгоритму DESX приблизно рівна швидкості DES. DESX достатньо стійкиі, має аппаратну реалізацію та широко використовується. Цей алгоритм також є виправленим DES, з більшою загальною довжиною ключа (184 біта) і він виключає можливість зламу методом простого перебору ключа.

На наш час стандартом шифрування США є AES(Rijndael), створений Вінсентом Рейном та Йоаном Дейманом за участі Ларса Кнудсена.