УДК 681.3.04::681.3.05
Попівчак В.– ст. гр. СІ-42
*Тернопільський національний технічний університет імені Івана Пулюя*

## КРИПТОГРАФІЧНИЙ АЛГОРИТМ “RSA”

Науковий керівник: к.т.н., ст. викладач Яцишин В.В.

Криптоалгоритм RSA запропонували в 1978 р. три автори: Р. Райвест (Rivest), А. Шамір (Shamir) і А. Адлеман (Adleman). Він став першим алгоритмом з відкритим ключем, який може працювати як в режимі шифрування даних, так і в режимі електронного цифрового підпису. Безпека алгоритму RSA побудована на принципі складності факторизації. Алгоритм використовує два ключі — відкритий і секретний, разом вони утворюють пари ключів Відкритий ключ використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним йому секретним ключем.

Криптоалгоритм RSA визнаний стійким при достатній довжині ключів. Сьогодні довжина ключа – 1024 біта вважається прийнятним варіантом. В асиметричній криптосистемі RSA кількість використовуваних ключів пов'язана з кількістю абонентів лінійною залежністю (у системі з N користувачів використовуються 2N ключів), а не квадратичною, як в симетричних системах.

Слід зазначити, що швидкодія RSA істотно нижча швидкодії DES, а програмна і апаратна реалізація криптоалгоритму RSA набагато складніша, ніж DES. Тому криптосистема RSA, як правило, використовується при передачі невеликого об'єму повідомлень та ЕЦП.

При підписанні електронного документу його початковий зміст не змінюється, а додається блок даних – електронний цифровий підпис[1]. Отримання цього блоку можна розділити на два етапи. На першому етапі за допомогою програмного забезпечення і спеціальної математичної функції обчислюється так званий «відбиток повідомлення» (message digest). На другому етапі відбиток документа шифрується за допомогою програмного забезпечення та особистого ключа автора.

У 2011року співробітникам RSA Security було розіслано листи з вкладеними у них електронними таблицями. Таблиця містила вкладений флеш файл, який використовує уразливість нульового дня, що дозволило захопити управління над комп'ютером співробітника. Після цього злочинець встановив на комп'ютері адаптований варіант інструменту віддаленого адміністрування, за допомогою якого було зібрано конфіденційну інформацію з інших машин в мережі .

Атака на алгоритм проводилася шляхом штучного виклику помилок за допомогою зміни напруги на процесорі. В результаті з'являлися помилки в комунікації з іншими клієнтами, і вдавалося отримати невелику частину ключа, а як тільки було зібрано достатньо частин, ключ був відновлений в режимі офлайн.

*Література:*

1. Романец Ю.В., Тимофеев П.А, Шальгин В.Ф. Защита информации в компьютерных системах и сетях – М.: «Радио и связь», 1999.