УДК 004.

ІНФОРМАЦІЙНА СИСТЕМА ПАРАЛЕЛЬНОГО ШИФРУВАННЯ ДАНИХ МЕРЕЖЕВОГО ТРАФІКУ

Черепанська І.Ю
д.т.н., доцент, професор кафедри
комп'ютерних технологій і моделювання систем
Поліський національний університет
Складанівський Денис Валерійович
Поліський національний університет

XXI століття – століття інформаційних технології, тому і найбільш актуальною темою в цьому столітті стала робота з інформацією, і головним завданням став саме захист інформації. Суть роботи полягає в захисті переданих даних і збільшенні швидкості обробки за допомогою декількох етапів шифрування. Іза стрімкого розвитку інформаційних технологій з'явилися і люди які намагаються вкрасти корисну інформацію з погано захищених користувачів. Тому і почали розробляти методи і технології захисту комп'ютерних мереж. Якщо розглядати схему паралельного шифрування даних то можна виділити два етапи перший це попереднє переміщування інформації з використанням SHUFFLE алгоритму. Другий етап – паралельне шифрування алгоритмом RSA на n вузлах, де вузли це персональний комп'ютер в мережі (рис 1).

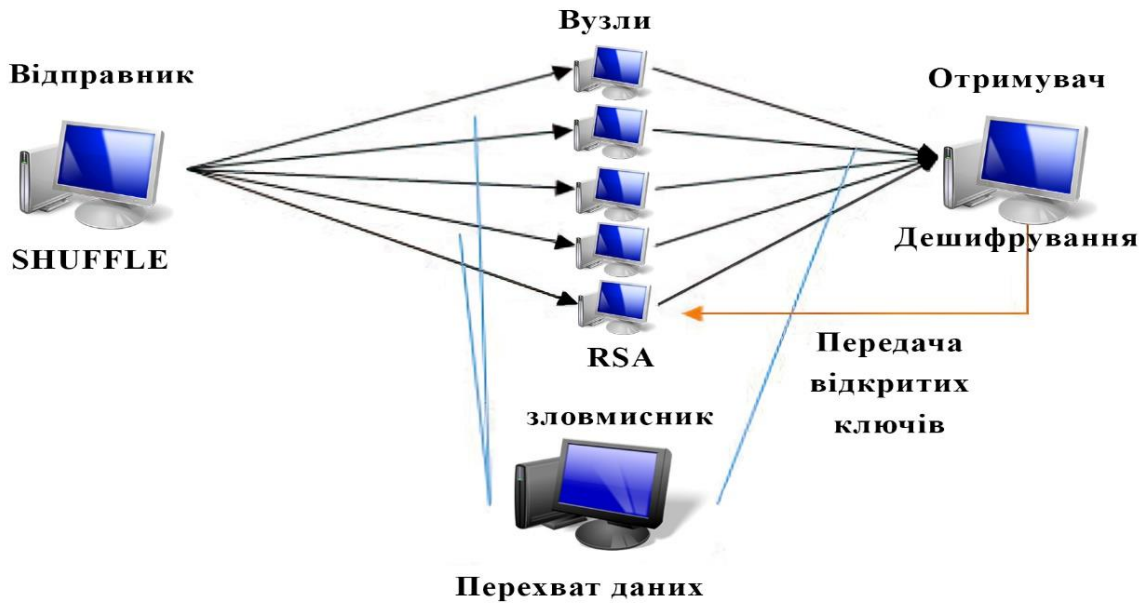

Рис.1. Схема паралельного шифрування даних з можливістю перехоплення інформації

Алгоритм RSA являється асиметричним, тому його швидкість роботи набагато нижча ніж у симетричних але його рівень безпеки вищий. Паралельне шифрування частин інформації сильно підвищує швидкість шифрування, а також підвищує захищеність даних, тому що якщо зловмисник отримає навіть декілька частин інформації на якому із двох етапів, він не зможе отримати повноцінної інформації яка несе сенс для отримувача.

Криптологія має дуже велику роль в сучасному світі, розвиток електронно-обчислювальної техніки дає зловмисникам все більше можливостей для дешифрування інформації. Кожен раз

алгоритми шифрування повинні покращуватися і до них висуваються все більш сурові умови, а кожен новий метод повинен перевірятися на кількість вразливостей які були раніше. А так як паралельне шифрування даних підвищує і швидкість і захищеність даних то цю систему можна вважати не тільки актуальною, але і перспективною на багато років вперед.

У XX столітті наука криптологія була розділена на дві частини: криптосинтез і криптоаналіз. Криптосинтез забезпечував захист інформації, а криптоаналіз шукає шляхи взлому систем. Це створило проблеми в сучасній криптографії так як розвивались дві частини, в результаті у кожного метода шифрування є як свої плюси так і мінуси. З вищесказаного можна зробити висновок про те, що зараз в криптографії актуальні проблеми ускладнення криптосистем, підвищення стійкості алгоритмів, а також зменшення розмірів блоків даних.

Однією із важливих функціональних характеристик алгоритмів шифрування є швидкість шифрування і криптостійкість. Результати моделювання показують, що технологія паралельного шифрування може підвищити ефективність передачі інформації і значно підвищити її безпеку. Для шифрування одержувач генерує n парних ключів один для шифрування, а другий для дешифрування і виробляє їх передачу на вузли. Після отримання частини тексту кожен вузловий комп'ютер виробляє шифр-текст і передає його в точку прийому інформації, для подальшої дешифрування і збору цільного тексту.

При паралельній шифрування даних швидкість залежить від декількох факторів:

1. довжина тексту;
2. використана мова(англійська, російська);
3. довжина ключа;
4. кількість вузлів.

Результати вимірювання швидкості шифрування текстів при зміні різних чинників представлені в табл. 1. Вимірювання швидкості проводилися на декількох текстах рівної довжини, але різного змісту.

Таблиця 1

Швидкість шифрування при різній кількості вузлів, с

	без вузлів	2 вузла	4 вузлів	8 вузлів	16 вузлів
Текст англійською довжиною 1600	0,042	0,029	0,022	0,0206	0,0201
Текст українською мовою довжина 1400	0,040	0,030	0,027	0,0263	0,0231

Висновки. Інформаційна система паралельного шифрування даних мережевого трафіку можна вважати не тільки актуальною, але і перспективною на багато років вперед. Розвиток електронно-обчислювальної техніки дає змогу покращити алгоритми шифрування. Криптосинтез і криптоаналіз дає змогу знаходити слабкі місця в алгоритмах і в майбутньому покращити або уникнути слабкі місця коду.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петров А.А. Комп'ютерна безпека. Криптографічні методи захисту. - М .: ДМК, 2000. - 449 с.

2. Яковлєв А.В. Криптографічний захист інформації: навчальний посібник / Яковлєв А.В., Безбогов А.А., Родін В.В., Шамкін В.Н. - Тамбов: Вид-во Тамбо. держ. техн. ун-ту, 2006. - 140 с.