Комп’ютерний практикум №2 (7)

**Тема:** Шифрування з відкритим ключем на основі алгоритму RSA

**Мета:** Ознайомитись з використанням криптопровайдерів .Net для побудови асиметричної криптосистеми

**Базові відомості**

Шифр RSA отримав назву на честь його розробників Ріверса (Ron Rivers), Шаміра (Adi Shamir) і Адлемана (Leonard Adleman).

В RSA системі використовуються наступні факти з теорії чисел:

1. Задача перевірки числа на простоту є порівняно простою.
2. Задача розкладання числа n=p\*q, де p і q – прості числа, на множники є дуже складною задачею, якщо ми знаємо тільки n, а p і q – великі числа (**задача факторизації**).

Основні повідомлення між сторонами В і А в протоколі RSA представляються наступною діаграмою:

A↔B: N=PQ, P,Q -прості;

B: f=(P-1)(Q-1); d<f, взаємно просте з f ; cd mod f=1;

B→A: d;

A:m; A→B: e=md mod N

B: y; B→A: m’=ec mod N;

Алгоритм гарантує, що m’=m. Пара чисел (c,N) є секретним, а (d,N) –публічним ключем сторони В.

**Хід виконання роботи**

1. Відшукайте в Інтернет-ресурсах чисельний приклад з використання алгоритму RSA (наприклад, в Вікіпедії ) та опрацюйте його.
2. Розробіть інтерфейс криптографічної системи для шифрування з використанням RSA, передбачивши окремий діалог для формування відкритого ключа.
3. Розробіть методи, які б забезпечували:
4. Генерацію пари «відкритий –закритий» ключі.
5. Шифрування з використанням відкритого ключа.
6. Розшифрування з використанням закритого ключа.
7. Перевірте правильність роботи системи на основі використання даних з чисельного прикладу.