**Лабороторна работа №8**

**Тема:** Криптоалгоритм “RSA”

**Мета:** Відпрацювання та закріплення теоретичних відомостей з криптоалгоритму “RSA”

**Короткі відомості:**

RSA (абревіатура від прізвищ Rivest, Shamir і Adleman) - криптографічний алгоритм з відкритим ключем, який базується на обчислювальної складності задачі факторизації великих цілих чисел.

Криптосистема RSA стала першою системою, придатною і для шифрування, і для цифрового підпису. Алгоритм використовується у великій кількості криптографічних додатків, включаючи PGP, S / MIME, TLS / SSL, IPSEC / IKE і інших.

Алгоритм створення відкритого і секретного ключів

**RSA-ключі генеруються наступним чином:**

1. Вибираються два різних випадкових простих числа ***p*** і ***q*** заданого розміру (наприклад, 1024 біта кожне).
2. Обчислюється їх добуток ***n = p \* q***, яке називається модулем.
3. Обчислюється значення функції Ейлера від числа ***n***:

***Ф (n)=(p-1) \* (q-1)***

1. Вибирається ціле число e ***(1 <e < Ф(n))***, взаємно просте зі значенням функції ***Ф(n).***

Число ***e*** називається відкритою експонентою (англ. public exponent)

Зазвичай в якості ***e*** беруть прості числа, що містять невелику кількість одиничних біт в двійковій запису, наприклад, прості з чисел Ферма: 17, 257 або 65537, так як в цьому випадку час, необхідний для шифрування з використанням швидкого зведення в ступінь буде менше.

Занадто малі значення ***e***, наприклад 3, потенційно можуть послабити безпеку схеми RSA.

5. Обчислюється число ***d***, мультиплікативного зворотне до числа ***e*** по модулю ***Ф(n)***, тобто число, яке задовольняє порівняння:

***d \* e = 1 (mod Ф(n).***

Число ***d*** називається секретною експонентою. Зазвичай воно обчислюється за допомогою розширеного алгоритму Евкліда.

6. Пара ***(e, n)*** публікується в якості відкритого ключа RSA (RSA public key).

7. Пара ***(d, n)*** грає роль закритого ключа RSA (RSA private key) і тримається в секреті.

Шифрування і розшифрування

Припустимо, Боб хоче послати Алісі повідомлення ***m***.

Повідомленнями є цілими числами в інтервалі від ***0*** до ***n-1***,



**Алгоритм шифрування:**

Взяти відкритий ключ ***(e, n)*** Аліси

Взяти відкритий текст ***m***

Зашифрувати повідомлення з використанням відкритого ключа Аліси:

***c = E (m) = m ^ e mod n***

**Алгоритм розшифрування:**

Прийняти зашифроване повідомлення ***c***

Взяти свій закритий ключ ***(d, n)***

Застосувати закритий ключ для розшифрування повідомлення:

***m = D (c) = c ^ d mod n***

**Висновок:** Асиметричною називається система в якій використовується один ключ для шифрування, а другий для дешифрування. Перевагами асиметричного шифрування є відсутність передачі ключа дешифрування і неможливість визначити його по відкритому ключу. Обидва ключі генеруються отримувачем повідомлення. Недолік асиметричного шифрування полягає в низькій швидкості кодування.

Математична основа криптостійкості шифра RSA полягає у складності розкладання більших чисел на множники (факторизації чисел) та зведення в ступінь по модулю квазіпростого числа, а недоліком використання RSA є використання кінцевих полів, а також реалізація алгоритму RSA потребує операцій з великими числами.

Щоб вирахувати розмір алфавіту ***n*** потрібно зведення простих чисел ***n*** і ***q.***

Число ***e*** повинно бути взаємно простим з ***f(n).*** Функцію Ейлера необхідно вираховувати для того щоб знайти пару ключів ***e*** і ***d****.*Для того щоб дізнатись секретний ключ ***d*** необхідно дізнатись ***p*** і ***q*** де ***p\*q=n.*** Секретний ключ ***d*** можна визначити із цієї формули ***e\*d mod f(n)=1***.

Інверсія це коли результат шифрування співпадає з шифрованим повідомленням.