Лабораторна робота № 6.

Система шифрування RSA.

Криптографічна система RSA (Rivest, Shamir, Adleman) належить до криптографічних систем із відкритим ключем. її стійкість зумовлена великими проблемами при знаходженні розкладання великих простих чисел на множники.

Для того, щоб організувати передачу шифрованих повідомлень за допомогою криптосистеми RSA, необхідно зробити таке:

1. За допомогою спеціальних алгоритмів згенерувати два великих простих числа p і q, які необхідно тримати в таємниці.

2. Повідомити відправнику повідомлень (або розмістити у відкритому каталозі) число $n = pq$ (модуль криптосистеми), а також випадкове ціле число e, взаємно просте з функцією Ейлера для цього модуля, добутком $\varphi(n) = (p-1)(q-1)$.

3. Для розшифровки повідомлень, зашифрованих на відкритому ключі n, e, отримувачу необхідно мати число d, яке є мультиплікативним оберненим числа e за модулем $(p-1)(q-1)$, тобто $de = 1 \bmod \varphi(n)$. Знайти таке число дуже просто, оскільки найбільший спільний дільник e і $\varphi(n)$ якраз і дорівнює одиниці за вибором e.

Отже, відправник знає свій закритий ключ, n, e, а отримувач, окрім того, знає ще й свій секретний ключ d.

Довільне відкрите повідомлення можна зобразити у вигляді послідовності цілих чисел із деякого інтервалу. Будемо вважати, що відправник передає секретне повідомлення у вигляді $X_1,\ldots,X_n$, $0 < X_i < n-1$, для всіх i від 1 до k.

Відправник для кожного блока X_i вираховує

$$C_i = (X_i^e) \bmod n \qquad (1)$$

і передає C_i відкритим каналом зв'язку.

Маючи n, e і C_i, отримувач може розшифрувати повідомлення, використовуючи співвідношення

$$X_i = (C_i^d) \bmod n \qquad (2)$$

Розглянемо як приклад випадок $p = 3$, $q = 11$, $n = 3 \times 11 = 33$, $e = 7$, $d = 3$. Легко переконатися, що кожне з чисел $e = 7$ і $d \times e = 21$ взаємно просте з $(p-1)(q-1) = 20$. Для передачі повідомлення $X = 2$ відправнику треба обчислити $C = (2^7) \bmod 33 = 29$. Отримувач може розшифрувати повідомлення за допомогою такої операції: $X = (29^3) \bmod 33 = 2$.

Завдання роботи.

1. Зашифруйте повідомлення X за допомогою алгоритму RSA для таких значень параметрів:

а) $p = 3$, $q = 11$, $d = 7$, $X = 5$;

б) $p = 3$, $q = 11$, $d = 3$, $X = 9$;

в) $p = 7$, $q = 11$, $d = 17$, $X = 8$;

г) $p = 11$, $q = 13$, $d = 11$, $X = 7$;

д) $p = 17$, $q = 31$, $d = 7$, $X = 2$.

2. Асиметрична криптосистема, що використовує RSA, має публічний ключ $e = 5$, $n = 35$. Зловмисник перехопив зашифроване повідомлення $C = 10$. Обчисліть приватний ключ та розшифруйте повідомлення.

3. Сформулюйте відповідні пари публічних і приватних ключів для криптосистеми RSA для значень модуля $n_1 = 377$, $n_2 = 451$.