Sprawozdanie z Laboratorium 2 – RSA

1. Założenia

W programie liczy pierwsze są z przedziału od 1000 do 9999 (4 cyfrowe). W rzeczywistości używa się znaczeni większych liczb pierwszy (co zwiększa bezpieczeństwo algorytmu)

2. Opis metod użytych do wyznaczania e i d

Do wyznaczenia liczby e wybierana jest losowo liczba z przedziału [2, n-1], gdzie n to liczba dla której szukamy liczby względnie pierwszej. Następnie wylosowana liczba sprawdzana jest przy pomocy math.gnd.

Do wyznaczenia liczby d używam d = pow(e, -1, phi).

3. Opis realizacji zadań (programu i jego składowych) i wartości uzyskane podczas ich realizacji.

Program zaczyna od wyznaczenia wszystkich liczb pierwszych czterocyfrowych. Następnie losowane z tej listy są liczby p i q, a kolejno wyliczane są liczby n, phi, e oraz d. Następnie podana jest wiadomość do zaszyfrowania (To jest tekst jawny i on będzie zaszyfrowany (RSA)) mający 50 znaków. W pętli każdy znak jest szyfrowany i dodawany do tablicy znaków zaszyfrowanych. W tym miejscu występuje wypisanie na konsole zaszyfrowanej wiadomości. Następnie następuje proces deszyfracji i również wypisanie odszyfrowanej wiadomości

Oto przykładowy przebieg algorytmu:
p = 1223
q = 9739
n = 11910797
phi = 11899836
e = 3192797
d = 677525
message = „To jest tekst jawny i on będzie zaszyfrowany (RSA)”
zaszyfrowana wiadomość = [11817996, 4225236, 3916750, 1503411, 5589062, 4890085, 7543858, 3916750, 7543858, 5589062, 9471970, 4890085, 7543858, 3916750, 1503411, 6918483, 6230115, 7845371, 3217889, 3916750, 1927289, 3916750, 4225236, 7845371, 3916750, 7988038, 3843920, 2796089, 9285893, 1927289, 5589062, 3916750, 9285893, 6918483, 4890085, 9285893, 3217889, 9532505, 5899104, 4225236, 6230115, 6918483, 7845371, 3217889, 3916750, 7775397, 3141398, 6825729, 8571656, 7684364]
odszyfrowana wiadomość = „To jest tekst jawny i on będzie zaszyfrowany (RSA)”

4. Odpowiedzi na pytania

1. Jakie elementy algorytmu są trudne w realizacji?
   Odp.: Generowanie odpowiednio dużych liczb pierwszych
2. Co stanowi o bezpieczeństwie i jakości tego algorytmu szyfrowania?
   Odp.: O bezpieczeństwie i jakości algorytmu stanowią odpowiednio duże liczby pierwsze

5. Wnioski

Implementacja algorytmu RSA pozwala na bezpieczne szyfrowanie i deszyfrowanie danych, ale wymaga użycia dużych liczb pierwszych dla rzeczywistego bezpieczeństwa. Klucz publiczny (e, n) może być używany do szyfrowania przez każdego, ale tylko właściciel klucza prywatnego (d, n) może odszyfrować wiadomość.