Podstawy Ochrony Danych – laboratorium AGC
Implementacja publicznego systemu kryptograficznego w oparciu o algorytm RSA.

Cel

Zapoznanie się z algorytmem RSA. Praktyczne zastosowanie algorytmu do publicznego systemu kryptograficznego.

Realizacja

Ćwiczenie polega na przygotowaniu prostej implementacji algorytmu RSA wg poniższego schematu:

generowanie klucza:

czynność	przykład
wybieramy dwie liczby pierwsze p i q	$p = 31$, $q = 19$
obliczamy $n = p \cdot q$	$n = 589$
obliczamy $phi = (p - 1)(q - 1)$;	$phi = 540$
generujemy e jako liczbę względnie pierwszą z phi czyli taką, która jest liczbą pierwszą i dla której największy wspólny dzielnik z phi wynosi 1	$e = 7$
generujemy d w taki sposób, aby spełniona była zależność: iloczyn e i d przystaje do 1 modulo phi. Co oznacza, że phi dzieli wyrażenia $e \cdot d - 1$.	$d = 463$

Para e i n stanowią klucz publiczny, natomiast para d i n jest kluczem prywatnym.

szyfrowanie wiadomości:

czynność	przykład
$c = m \text{ ^ } e \bmod n$; gdzie c oznacza wiadomość zaszyfrowaną, a m wiadomość jawną.	$m = 8$ $c = 8 \text{ ^ } 7 \bmod 589 = 312$

deszyfrowanie wiadomości:

czynność	przykład
$m = c \text{ ^ } d \bmod n$; gdzie c oznacza wiadomość zaszyfrowaną, a m wiadomość jawną.	$c = 312$ $m = 312 \text{ ^ } 463 \bmod 589 = 8$

Zadania

1. Przygotować dwie czterocyfrowe liczby pierwsze p i q.
2. Wygenerować dwa klucze: klucz prywatny i klucz publiczny.
3. Przygotować wiadomość składającą się z 50-ciu znaków.
4. Zaszyfrować wiadomość kluczem publicznym.
5. Odszyfrować wiadomość kluczem prywatnym.
6. Porównać pierwotną wiadomość z wiadomością odszyfrowaną.
7. Zwrócić uwagę, że wiadomość była szyfrowana kluczem publicznym (jawnym). Każdy kto chce otrzymywać wiadomości zaszyfrowane w tym systemie zatrzymuje dla siebie klucz prywatny (tajny), a upowszechnia klucz publiczny. Jeżeli ktoś (A) chce wysłać wiadomość zaszyfrowaną do kogoś (B), powinien użyć klucza jawnego B, gdyż wtedy B odczyta ją kluczem tajnym, który jest znany tylko jemu.

Pytania

1. Jakie elementy algorytmu są trudne w realizacji?
2. Co stanowi o bezpieczeństwie i jakości tego algorytmu szyfrowania?

Sprawozdanie

Sprawozdanie powinno zawierać:

1. Założenia – jak duże liczby pierwsze mogą być wykorzystane w programie?
2. Opis metod użytych do wyznaczania e i d.
3. Opis realizacji zadań (programu i jego składowych) i wartości uzyskane podczas ich realizacji.
4. Odpowiedzi na pytania.
5. Wnioski.