Dokumentacja szyfr RSA

Szyfr ten polega na podaniu dwóch liczb pierwszych do których następnie jest dobrany klucz e za pomocą funkcji znajdz\_e który razem z iloczynem tych liczb pierwszych daje nam klucz publiczny ,klucz prywatny jest generowany za pomocą klucza publicznego przy pomocy funkcji RSA.

Funkcja znajdz\_e(p,q):

Funkcja znajdz\_e przyjmuje wartości p i q które są różnymi liczbami pierwszymi następnie oblicza t=(p-1)\*(q-1) i za pomocą pętli for(zaczynającej się od 13 idącej do t) sprawdza potencjalne klucze e (potencjalne e są oznaczone jako i) warunkami takimi jak:

-czy e jest dodatnie

-czy e jest względnie pierwsze do t

-czy reszta z dzielenie t i o(dzielenia całkowitego t i e) jest różna od zera

-czy r2 reszta z dzielenie e i r (reszta z dzielenia t i e) jest różna od jeden lub zero

-czy dzielenie całkowite r i r2 jest różne od 1

-czy dzielenie całkowite e i r jest różne od 1

-czy reszta z dzielenia e i r jest różna od zera

-czy reszta z dzielenia r i o2 (dzielenie całkowite e i r) jest różna od zera

Jeżeli wszytkie te warunki zostaną spełnione liczba zostaje dodana do tablicy z dostępnymi e dla danej pary liczb pierwszych:

Funkcja następnie zwraca tą tablice

Funkcja RSA(p,q,e)

Argumenty:

p,q – dwie różne liczby pierwsze

e – klucz znajdujący się w tablicy zwracanej przez funkcje znajdz\_e(p,q)

Funkcja ta oblicza N=p\*q t = (p-1)\*(q-1) oraz oblicza klucz d za pomocą t oraz klucza e następnie porządkuje ona (e,N) w klucz publiczny i (d,N) w klucz prywatny. Funkcja ta zwraca klucz publiczny oraz klucz prywatny w dwu elementowej tablicy.

Funkcja Szyfr(e,N,tekst) i Deszyfr(d,N,zasz):

Funkcja Szyfr przyjmuje:

e – klucz e który bierzemy z klucza publicznego

N – iloczyn liczb pierwszych który bierzemy z klucza publicznego

tekst - tekst który chcemy zaszyfrować

Funkcja Deszyfr przyjmuje:

d – klucz d który bierzemy z klucza prywatnego

N – iloczyn liczb pierwszych który bierzemy z klucza prywatnego

zasz – zaszyfrowany tekst który chcemy odszyfrować

Obie funkcje zwracają tekst który wcześniej został zaszyfrowany albo odszyfrowany przy pomocy klucza.

(Kiedy podamy bardzo duże liczby pierwsze prawdopodobnie wyjdziemy poza zakres tablicy ASCII ponieważ stosowane są wtedy bardzo duże liczby)

(Nie działa dla polskich znaków)

Działanie programu:

Kiedy odpalimy program , program poprosi nas aby podać 2 różne liczby pierwsze w wypadku podania liczby złożonej program wyświetli nam błąd „podane liczby nie są pierwsze”. Po podaniu liczb pierwszych program zwróci nam tablice z dostępnymi kluczami e (dla bardzo małych liczb takich jak 2 i 3 może nie być klucza ponieważ e musi mieć co najmniej wartość 13) w razie jakby dana liczba nie miała żadnego klucza e wyświetli się błąd „Dla podanych liczb pierwszych nie ma klucza e”. Po podaniu klucza e z tablicy program wyświetli nam menu gdzie mamy wybrać wartość od 1 do 5:

W wypadku wybrania „1” program wyświetli nam klucz prywatny i publiczny:

W wypadku wybrania „2” program poprosi nas o podanie tekstu do zaszyfrowania a następnie wyświetli zaszyfrowany tekst

W wypadku wybrania „3” program poprosi nas o podanie tekstu do odszyfrowania a następnie wyświetli odszyfrowany tekst

W wypadku wybrania „4” program weźmie tekst z pliku(wiadomość do zaszyfrowania.txt) oraz zaszyfruje go a następnie wyświetli zaszyfrowany tekst

W wypadku wybrania „5” program weźmie tekst z pliku(zaszyfrowana wiadomość.txt) oraz odszyfruje go a następnie wyświetli odszyfrowany tekst

W wypadku podania żadnej z powyższych wartości program wyświetli błąd „Podaj cyfrę od 1 do 5”

Program Odbieranie i dostawanie klucza.py

Ten program ma na celu pokazanie że można komuś przekazać klucz publiczny żeby zaszyfrować wiadomość a następnie odszyfrować go kluczem prywatnym.

Program posiada tylko dwie funkcje Szyfr i Deszyfr które działają tak samo jak w poprzednim programie.

Aby program działał w zmiennej klucz trzeba podać klucz prywatny lub publiczny a w zmiennej tekst do odszyfrowania lub zaszyfrowania

Po uruchomieniu program się pyta czy wartość jaką podałeś w zmiennej klucz to klucz prywatny czy publiczny.

Jak odszyfrować wiadomość z pliku „zaszyfrowana wiadomość.txt”?

Aby odszyfrować wiadomość z pliku proszę użyć tych samych wartości p,q,e które są podane w pliku „Liczby pierwsze i klucz e użyty podczas szyfrowania plików.txt”

Lub użyj w programie „Odbieranie i dostawanie klucza.py” wpisz w zmienną klucz ,klucz prywatny z pliku „Liczby pierwsze i klucz e użyty podczas szyfrowania plików.txt”.