НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп'ютерний практикум №3 з курсу
Методи Реалізації Криптографічних Механізмів

Реалізація основних асиметричних криптосистем

Виконав студент
групи ФІ-22мн
Кушнір О.С.

Перевірив:
Селюх П.В.

Київ — 2022

1 МЕТА КОМП'ЮТЕРНОГО ПРАКТИКУМУ

Дослідження можливостей побудови загальних та спеціальних криптографічних протоколів за допомогою асиметричних криптосистем.

2 ПОСТАНОВКА ЗАДАЧІ

Реалізація сліпого цифрового підпису із допомогою криптосистеми RSA, за допомогою бібліотеки криптографічних примітивів системи PGP v.6.5.2.

3 ХІД РОБОТИ

Сліпий підпис (англ. blind signature) — різновид електронного цифрового підпису, особливістю якого є те, що сторона, яка підписує, не може точно знати вміст підписаного документа. Поняття «сліпий підпис» придумано Девідом Чаумом в 1982 році, ним же запропонована перша реалізація через алгоритм RSA. Безпека схеми сліпого підпису ґрунтувалася на складності факторизації великих складених чисел. З тих пір було запропоновано велику кількість інших схем.

Обираємо r - так щоб $(r, n) = 1$

$m' = mr^e \mod n$

$s' = m'^d \mod n$

$s = s'r^{-1} \mod n$

$s = s'r^{-1} \mod n$

$s = (m')^d r^{-1} \mod n$

$s = m^d r^{ed} r^{-1} \mod n$

$s = m^d r r^{-1} \mod n$

$s = m^d \mod n$

ВИСНОВКИ

PGP не є зручним стандартом для реалізації сліпого цифрового підпису бо не має методів для коректної перевірки сігнатур сліпого підпису, не має множення за модулем, та множення на обернений.