Central Washington University

Introduction to Computer Security

Spring 2019

Project 2 Report

Author:
Hermann Yepdjio

Instructor:
Dr. Razvan Andonie

May 1, 2019

Contents

1 Results

1.1 Part 1

Alice's RSA public key is (N, e) = (33, 3) and her private key is d = 7
a)

if Bob encrypts the message M = 19 using Alice's public key, the cipher text C is
C = M^e mod N = 19^3 = 6859 = 28 mod 33. C = 28.
Alice can decrypt C to obtain M by doing the following
M = C^d mod N = 28^7 = 13492928512 = 19 mod 33. M = 19

b)

If S is the result when Alice digitally signs the message M = 25, then
S = M^d mod N = 25^7 = 6103515625 = 31 mod 33 S = 31

If Bob receives M ans S, to verify the signature he just have to unsign S using Alice's public key and see if he obtains M as follow
M = $\{S\}_{alice}$ = 31^3 = 29791 = 25 mod 33 M = 25

1.2 Part 2

Public Key = (18, 30, 7, 26) and n = 47

a) Find the private key, assuming m = 6

x.6 mod 47 = 18 ≡ x = 3.
x.6 mod 47 = 30 ≡ x = 5.
x.6 mod 47 = 7 ≡ x = 9.
x.6 mod 47 = 26 ≡ x = 20.

private key = (3, 5, 9, 20)

b) Encryption of M = 1101 (given in binary)

$18 + 30 + 26 = 74 = 27 \bmod 47$

1.3 part 3

Output after running the C code:
Point P = (2 , 7) is on the elliptic curve E.
What Alice sent to Bob is : (153 , 36)
What Bob sent to Alice is : (103 , 153)
The shared secret is : (137 , 54)

2 Observations

It was more convenient to solve Part 1 and part 2 of this assignment by hand while it was easier to solve part 3 by writing a program that would do it.