

Homework-4

Mustafa Tokat

January 19, 2021

1 Introduction

Thank you for your supports one more time. Indeed, at this process, I have learned a lot of things, I have started to enhance to my digital library, at the same time I also learned where and how to find the things I need. Now, let's solve to below problems.

2 Analysis of Problems

2.1 Problem 1

Consider the prime $p = 9929$ and the primitive element **2**.

2.1.1 Show the steps of the Diffie-Hellman between Alice and Bob for $a = 1983$ and $b = 2014$.

Table 1: Add caption

Alice	(p, q) = (9929, 2)	Bob
a=1983		b=2014
↓		↓
$2^{**}1983 \pmod{9929} = 8580$		$2^{**}2014 \pmod{9929} = 5387$
↓		↓
$5387^{**}1983 \pmod{9929}$		$8580^{**}2014 \pmod{9929}$
↓		↓
K = 7690		K = 7690

2.1.2 What is the value of the agreed secret key?

Result: 7690

2.2 Problem 2

Consider the RSA public and private key pairs: $(e, n) = (17, 902801)$ and $(d, n, p, q, \phi) = (423953, 902801, 911, 991, 900900)$.

I have checked to all values (indeed, to practice).

2.2.1 Given $M_1 = 500000$, compute $C_1 = M_1^e \pmod{n}$.

Let's compute according to above formula:

$$C_1 = 500000^{17} \pmod{902801} = 487730$$

2.2.2 Given $C_2 = 707631$, compute $M_2 = C_2^d \pmod{n}$

Similarly;

$$M_2 = 707631^{423953} \pmod{902801} = 500001$$

2.3 Problem 3

RSA with three primes would also work: $n = pqr$, $\phi(n) = (p-1)(q-1)(r-1)$, $\gcd(e, \phi(n)) = 1$, and $d = e^{-1} \pmod{\phi(n)}$

2.3.1 Setup an example RSA public/private key pair using primes 29, 31, 37, and $e = 17$.

At first, we compute necessary all values;

$$n = p.q.r = 29.31.37 = 33263$$

$$\phi(n) = (p-1)(q-1)(r-1) = 28.30.36 = 30240$$

$$d = e^{-1} \pmod{\phi(n)} = 17^{-1} \pmod{30240}$$

2.3.2 Encrypt $m = 10000$ and then decrypt the ciphertext.

$$C_1 = 10000^{17} \pmod{33263} = 29774 \text{ and,}$$

$$M_1 = 29774^{423953} \pmod{33263} = 10000$$

2.3.3 Explain why RSA with three primes algorithm is not preferred.