Homework-4

Mustafa Tokat

January 18, 2021

1 Introduction

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.

2.1.2 What is the value of the agreed secret key?

2.2 Problem 2

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

2.2.1 Given M1 = 500000, compute C1 = Me 1 (mod n).

2.2.2 Given C2 = 707631, compute M2 = Cd 2 (mod n)

2.3 Problem 3

RSA with three primes would also work: n = pqr, ϕ(n) = (p-1)(q-1)(r-1), gcd(e, ϕ(n)) = 1, and d = e -1 (mod ϕ(n))

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

2.3.2 Encrypt m = 10000 and then decrypt the ciphertext.

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