Collage of Engineering: Computer Engineering Department
ECCE 537: Network Security

Assignment 1: Documentation

RSA Algorithm

Introduction

This document covers the realization of the Assignment 1 of Network Security course. For this homework we were asked to reproduce an algorithm of encipherment/decipherment.

I chose the RSA algorithm in Python 3. The next part will cover how tu use it and its implementation.

Usage

py RSA_Encryption To execute the program.

Implementation

Encipherment

1. First, we ask the user to enter 2 prime numbers p and q, ***askpq()*** function. Then we calculate n and *φ*n in ***nphiden()*** function: n is equal to p*q and *φ*n to (p-1) * (q-1).
2. Then, to determine the public key we need to find e. We will then make a loop that looks for p, q <e <φn and over another loop that continues until the PGCD of e and φn = 1.
3. This is the ***founde()*** and ***pgcd(a,b)*** functions.
4. Finally, to encipherment the string we will change each character to its ASCII equivalent and then apply the formula: string ^ e % n. This is done in the ***encryp_string(string, n, phiden, e)*** function.

Decipherment

1. We ask the user for the d value ***askd()***.
2. We ask the user the number n and factorize it, we do this in ***factoring(n)***.
3. We need to know *φn*, e and d. For that we use the same method as the encipherment with ***founde()*** and ***pgcd(a, b)*** functions.
4. Then we need to know d, we know that e*d mod n = 1 et p,q<e<φn, we apply that in the ***foundd(e, phiden, p, q)*** function.

Avel Docquin

5. To decipherment the string, we search for each character of it its value in ASCII. For that we apply the formula character ^ d % n = ASCII.
6. We make a while loop who apply this in each character of the string passed in parameter in ***string_decipherment(d, n)*** function and we get the readable string.