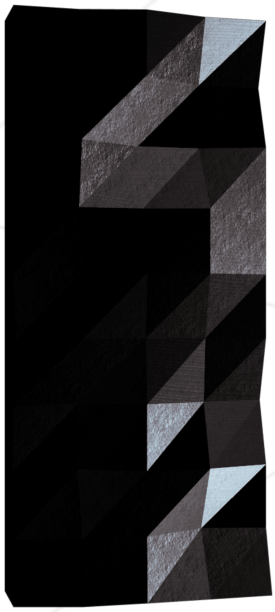

Cybersecurity Bootcamp | 42 Madrid

coRSAir

Summary: Cryptography block: Vulnerable Ciphers

Version: 1

Contents

Chapter I

Introduction

This project introduces specific concepts about the strength of the RSA algorithm and its potential vulnerabilities. Although the algorithm is considered strong enough for the computational power of current devices, certain ways of using it can lead to serious security problems.

Chapter II

Prologue

He had been taking care of Captain Burt's birds, and talking to him about them. Because of that, we had become closer. I still called him Sir, nonetheless. But I had shown him that he could relax with me and that I would still jump right away when he gave me an order. For all this he answered my questions, when they were not too many, and he taught me how to use the astrolabe. Essentially, it He used to try to measure the angle of the sun at night. Once you know that and the date, you know the latitude. The further north you are, the further The sun rises south and is lowest at noon in winter. If you know the date, the table gives you the latitude. Some stars can be used the same mode. There are many problems with this system, as I could see. In First of all, it's hard to get a good measurement unless you give the chance that you are on a rock. When the sea is calm, You take three measurements and find the mean. When it's chopped, ya you can forget.
And that's not all. When the weather is bad and you can't see the sun, you don't know can measure. And besides, your compass is pointing to magnetic north, no to the real There are also tables for compass deviation, but you have to know your position to use them. So what I used to do (I'm going too fast again) was to check the magnetic orientation with the polar Star. If this starts to sound complicated, you'll see later. I have only given you the relevant points.
Once you have found your latitude, you still need to know your longitude, and the only thing we can do is measure our speed with the basket and record it in the notebook every hour. The basket has a rope with knots to measure speed. You throw her behind the boat, look at the small hourglass and count the knots.

Of course, everything changes when the earth is close. you orient with objects on the navigation chart, which gives you your position as long as when the letter is correct and you have not chosen wrong the island, the mountain, or whatever. By the time I had learned half of all this, we were already very, very far from Veracruz. So good night!

Excerpt from "Confessions of a Pirate", Gene Wolfe, 2007

Chapter III

General instructions

For this project, you must use C as the language. The list of allowed functions is as follows:

- All functions of `<math.h>`
- All functions of `<string.h>`
- The *openssl* library
- Everything that is permitided in the exercice header.

Chapter IV

Mandatory Part

Security in asymmetric cryptography using RSA keys is based on the premise that it is computationally very difficult to factor the two prime factors of a number. *"Multiplying two prime numbers p and q to get n"* is a simple operation, and its complexity does not increase dramatically as the numbers grow:

[1736640013 1230300287 = 2136588706409583731]

In contrast, the inverse operation, *"given a number n obtain its two prime factors"*, is an operation that becomes computationally infeasible when the numbers involved are large enough.

To generate the key pair, the RSA algorithm creates a public and private key using this concept. Simplifying the generation of the keys, the randomly chosen primes p and q are multiplied to create the modulus n that will be used in both the private and public keys. This module n is public but the prime factors p and q are not.

[? · ? =2136588706409583731]

If we have two certificates generated in a system whose random number generator is weak and therefore in which the entropy is minimum... This may have increase the probability of repetitions of prime numbers during different generations, thus it might have been the case in which two modules share the same factor p or q.

[n1 = p1 · q1] [n2 = p1 · q2]

Chapter V

Exercice 1 - coRSAir

Nombre de función	`corsair`
Archivos a entregar	`*.c, *.h`
Funciones autorizadas	`printf, snprintf, write, read, open, close, malloc, free`
Descripción	`Cryptography block: Vulnerable Ciphers`

With this information, you will create a tool that:

- Reads the public key of these certificates and get the modulus and exponent and then calculates the rest of the necessary data.
- Constructs the private key from two primes and their product, and from there, gets the symmetric key encrypted with it.
- Decrypts the message!

Chapter VI

Bonus Part

The evaluation of the bonuses will be done `IF AND ONLY IF` the mandatory part is `PERFECT`. Otherwise, the bonuses will be totally `IGNORED`.

You can enhance your project with the following features:

- Detailed and clear documentation of all the theoretical foundations behind the project.
- Proprietary implementation of a library or set of functions in C to operate with large integers.
- Everything that comes to your mind... you will be able to justify everything during the defense.

Chapter VII

Peer evaluation

This project will be corrected by other students. Turn in the files inside the Git repository and make sure everything works as expected.