Advanced Software Engineering Techniques - State of the Art

Cotan Paul Adrian, Kelesidis Evgnosia Alexandra

January 2020

1 Introduction

Even if most people don't notice the importance of cryptography, it has been used by many times during our history in a such important situations starting from the roman empire with the well known Ceasar's cypher.

Nowadays one of the most used types of cryptography is known as public-key cryptography. In this paper we will focus on a subfield of it, named *identity-based encryption* or *IBE*, which was proposed by Adi Shamir in 1984.

Even if Shamir was not able to give us any example of IBE, his idea was used by Clifford Cocks, who created in 2001 such an example. In the same year, Dan Boneh and Matthew K. Franklin also proposed another IBE scheme.

2 Clifford Cocks IBE scheme

2.1 Utility

The identity-based encryption scheme proposed by Clifford Cocks is mostly used for encrypting short messages such as passwords and is based on the hardness of the quadratic residuosity problem.

2.2 Negative features

Clifford Cocks proposed a scheme where the encryption is made bit by bit, so the speed is heavily affected by the size of the message and, moreover, the cipher text size is much larger than the size of the message.

2.3 Techniques and methodologies

For the entire process, Clifford's scheme uses hash functions, a RSA modulus and the Jacobi Symbol. In the next part we will describe in short all of these parts.

A hash function is any function that can be used to map data of arbitrary size to fixed-size values.

The RSA modulus comes from the RSA cryptosystem which was officially proposed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It is based on the hardness of the factorization problem. To describe this problem we need to choose two big prime

numbers (let's say bigger than 2^{512}) and calculate $n = pq$. Just knowing the value of n doesn't give you any information about its primality or about its divisors. In this case n is a RSA modulus.

To define the Jacoby symbol we should firstly define Legendre symbol.

Let's take $f : \mathbb{Z} \times \{t \in \mathbb{N} : t \text{ prime}\} \to \{-1, 0, 1\}$, defined as:

$$f(p,q) = \begin{cases} 1, & \text{if } p \text{ is a quadratic residue modulo q;} \\ 0, & \text{if } q|p; \\ -1, & \text{otherwise;} \end{cases} .$$

In this case, $f(p,q) = \left(\frac{p}{q}\right)_L$, it is called the Legendre symbol of p over q.

Now we can define Jacoby symbol in the following manner:

$$\left(\frac{m}{n}\right)_J = \left(\frac{m}{p_1}\right)_L^{a_1} \cdot \left(\frac{m}{p_2}\right)_L^{a_2} \cdot \cdots\cdot \left(\frac{m}{p_k}\right)_L^{a_k},$$

where $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots\cdot p_k^{a_k}$.

Now we are able to define Quadratic Residuosity Problem (QRP). Knowing the numbers m and n and the fact that $\left(\frac{m}{n}\right)_J = 1$ we should determine whether m is a quadratic residue modulo n (n is not prime, so $\left(\frac{m}{n}\right)_L$ is not defined) without the knoledge of the divisors of n.

3 Our target

During this semester we want to implement Cocks' scheme using java 11 on windows 10 platform. For this we will use BouncyCastle, which is a cryptographic library and SHA-512 for hashing.

4 Table of Contents

[1] Clifford Cocks - *An Identity Based Encryption Scheme based on Quadratic Residues*, 2001

[2] A. Shamir - *Identity Based Cryptosystems and Signature Schemes Advances in Cryptology* - Proceedings of Crypto '84.

[3] H Cohen - *A Course in Computational Algebraic Number Theory* Springer-Verlag graduate texts in mathematics 138, 1993

[4] Ferucio Laurentiu Tiplea, Sorin Iftene, George Teseleanu, Anca-Maria Nica - *On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography*