C++ Implementation of Cryptography Algorithms

Ghaith Arar, Amanda Ly, *Student Member, IEEE,* and Neel Haria
Stevens Institute of Technology
Hoboken, NJ 07030, USA
Email: garar@stevens.edu, aly@stevens.edu and nharia@stevens.edu

***Abstract*—Cybersecurity has gotten increasingly significant in the past few years and with the rise in the widespread use of technology, there has also been a rise in cybercrime and cyber-attacks. These cybersecurity threats consist of but are not limited to malware, phishing, data leakage, hacking, structured query language injection, denial-of-service attacks, and domain name system tunneling. Cybersecurity is important because it pertains to protecting user's sensitive data and personal information; however, securing information is a challenge. Cryptography is an integral part of modern world information security to make the virtual world a safer place. Cryptography is a process of making information unintelligible to an unauthorized person. Hence, providing confidentiality to genuine users. This paper will look into various cryptography algorithms and implement the Rivest–Shamir–Adleman (RSA) algorithm, and Diffie-Hellman key exchange using C++.**

***Index Terms*—Rivest–Shamir–Adleman (RSA), Diffie-Hellman, Data Encryption, Cryptography, Data Decryption.**

I. Introduction

INFORMATION security plays an important role in protecting digital information against security threats and keeps information secret by protecting it from unauthorized access. Cryptography involves secret writing between two or more people so that others looking in cannot decipher what is being said or shared. There are two types of cryptosystems based on the number of keys involved: a symmetric key cryptosystem and an asymmetric key cryptosystem. Cybersecurity experts define cryptography in five components and the underlying technology of cryptography involves the encryption of plain text and the decryption of cipher text. Encryption is the process of conversion of data, called plain text, into an unreadable form, called cipher text, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so that it can be understood by the people who are authorized to read the data [1]. The idea is that a recipient of plain text would not need special knowledge or equipment to understand what is being communicated, and the decryption algorithm decodes the cipher text to the original understandable plain text. This is all done with a set of keys - secret information known by members of the group that parameterize the encryption and decryption.

The remainder of this paper is organized as follows. Section II will discuss the related works pertaining to cryptography. Section III discusses the different cryptography algorithms. Section IV presents the team's novel implementation of RSA and Diffie-Hellman key exchange using C++. Section V will discuss the observations of our implementation and the paper will be concluded in section VI.

II. Related Work

Texttextext sample text Texttextext sample text Texttextext sample text Texttextext sample text Texttextext sample text

III. Cryptography Algorithms

TexttextextTexttextextTexttextextTexttextextTex

A. Symmetric Algorithms

blah blah knowledge part 1

1) AES: Advanced Encryption Standard

2) DES: Data Encryption Standard

B. Asymmetric Algorithms

Asymmetric encryption, also known as public-key cryptography, is a relatively new method, compared to symmetric encryption, and uses two keys to encrypt plain text. Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in the symmetric encryption model, eliminating the need to share the key by using a pair of public-private keys. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know. This algorithm uses a key generation protocol to generate a key pair so both the keys are mathematically connected with each other. The benefits of asymmetric cryptography is the elimination of key distribution, an increased security due to the lack of key transmission and the use of digital signatures. The main disadvantage is the slower computation/processing speed compared to symmetric cryptography. Types of asymmetric cryptosystem [2]. RSA, Elliptic Curve Cryptosystem (ECC), Diffie-Hellman, and Digital Signature Algorithm (DSA) are some of commonnly used asymmetric algorithms.

1) RSA: RSA, also known as the Rivest–Shamir–Adleman algorithm, was founded in 1977 and is the most common public key algorithm in cryptography world. RSA is named for its inventors, Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman, who created it as faculty at the Massachusetts Institute of Technology. Even though, applying the algorithm is relatively simple, it lies behind powerful math theorems to ensure its strength. The security of RSA relies on the difficulty of factoring the product of two large prime numbers.

2) Diffie-Hellman: info info info

3) ECC: Elliptic Curve Cryptosystem

4) DSA: Digital Signature Algorithm

IV. Implementation

this is where we put our code and explain it.

A. Pseudo Code:

```
int x = prime number
int y = prime number
int phi = x * y
int e = findcoprime(phi)
int d = 1 mod (phi)/e
public_key = (e,n) private_key = (d,n)
```

B. Steps:

1) Generating the Keys:: (i) Select two large prime numbers, x and y. The prime numbers need to be large so that they will be difficult for someone to figure out. (ii) Calculate n = x*y (iii) Calculate the **totient** function i.e. phi(n) = (x-1)(y-1)(n)=(x1)(y1). (iv) Select an integer e, such that e is co-prime to phi(n) and 1¡e¡phi(n). The pair of numbers(n,e) makes up the public key. (v) Calculate d such that e.d = 1 mod $\phi(n)$

2) Encryption: Given a Plain-text P, represented as a number the Cipher text C is calculated as C = P$^{n}modn$

3) Decryption: Using the private key(n,d) the plain-text can be found using P = C$^{d}modn$

C. GMP-Library

V. Discussion

this is where we discuss our observations about our implementations and what future works can be done it.

VI. Conclusion

This paper is about ...

References

[1] A. Kahate, *Cryptography and network security*. Tata McGraw-Hill Education, 2013.

[2] K. Brush, L. Rosencrance, and M. Cobb, “What is asymmetric cryptography and how does it work?” 2020. [Online]. Available: https://searchsecurity.techtarget.com/definition/asymmetric-cryptography