

University of San Carlos

School of Arts and Sciences

Department of Computer, Information Sciences, and Mathematics

Talamban Campus, Cebu City, Philippines

IT 3104N – Information Assurance and Security

**PROJECT: CRYPTOGRAPHY**

**Submitted by:**

Van AJ Vanguardia

**Submitted to:**

Godwin Monserate

**30 November 2022**

**Overview**

The project is a hybrid of a modified RSA (Rivest-Shamir-Adleman) and Atbash cryptography. The RSA was modified using four keys of prime numbers (p, q, r, s) instead of two (p, q) in which improves the .

**Key Generation**

1. Choose four prime numbers where P, Q, R, S are distinct
2. Calculate N (Product of the 4 prime numbers)

* Let N = p \* q \* r \* s

1. Calculate T (Totient of Product of Primes)

* Let T = (p -1) \* (q - 1) \* (r - 1) \* (s - 1)

1. Select e (encryption) such that:

* 1 < e < T
* Coprime of N and T

1. Select d (decryption) such that:

* d = de(mod T) = 1

1. Generate public key

* Let KU = {e, N}

1. Generate private Key

* Let KR = {d, N}

**Encryption Process**

1. Modified Rivest-Shamir-Adleman – Encryption

Formula: C = M ^ e mod N

Where:

C = Ciphertext

M = Message

e = Encryption

N = Product of the 4 prime numbers

1. Modified Atbash

Formula: N – L

Where:

N = Total number of the alphabet (26)

L = Length of the alphabet

Formula: REV(S)

S = String of atbash characters

REV = A function that reverses the string

**Decryption Process**

1. Modified Atbash

First Phase: Normal Atbash

Formula: N – L

Where:

N = Total number of the alphabet (26)

L = Length of the alphabet

Second Phase: Reversal of Atbash

Formula: REV(S)

S = String of atbash characters

REV = A function that reverses the string

1. Rivest-Shamir-Adleman Cryptography – Decryption

Formula: M = C ^ d mod n

Where:

M = Message

C = Ciphertext

e = Encryption

N = Product of the 4 prime numbers