

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**

**Key Generation**

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

* n = p \* q \* r \* s

1. Calculate t (Totient of Product of Primes)

* t = (p -1) \* (q - 1) \* (r - 1) \* (s - 1)

1. Select e (Encryption Key) such that:

* gcd(t, e) = 1
* 1 < e < t

1. Calculate for d (Decryption Key)

* d = e – 1 mod t

1. Public key KU ={e,n}
2. Private Key KR ={d,N}.

**Encryption Process**

1. Rivest-Shamir-Adleman Cryptography

C= M ^ e mod n

Where:

C = Ciphertext

M = Message

e = Encryption Key

n = Product of the 4 prime numbers)

1. Atbash Cryptography

**Decryption Process**

Formula: M= C ^ d mod n

Where:

C = Ciphertext

M = Message

e =

n =