MINI PROJECT
ON

SECURED DATA COMMUNICATION USING HOMOMORPHIC ENCRYPTION

Outline

- Introduction
- Objectives
- Block Diagrams
- Mathematical models – RSA, Pallier and BCP Algorithms
- Simulation Results
- References

Introduction

- Cryptography – enables users to communicate in a secured manner over unsecured channel
- Homomorphic encryption – special class of cryptography wherein the data is processed in the encrypted domain itself
- Degree of security and authenticity are assured
- Highly useful for privacy preserving applications – voting, rating, healthcare etc.

Objectives

- To develop a mathematical model for Homomorphic encryption using RSA, Paillier and BCP algorithms
- To compare the performance based on the time required to encrypt and decrypt the data
- To implement and validate a Homomorphic Encryption system to perform data processing in encrypted domain

Block Diagram

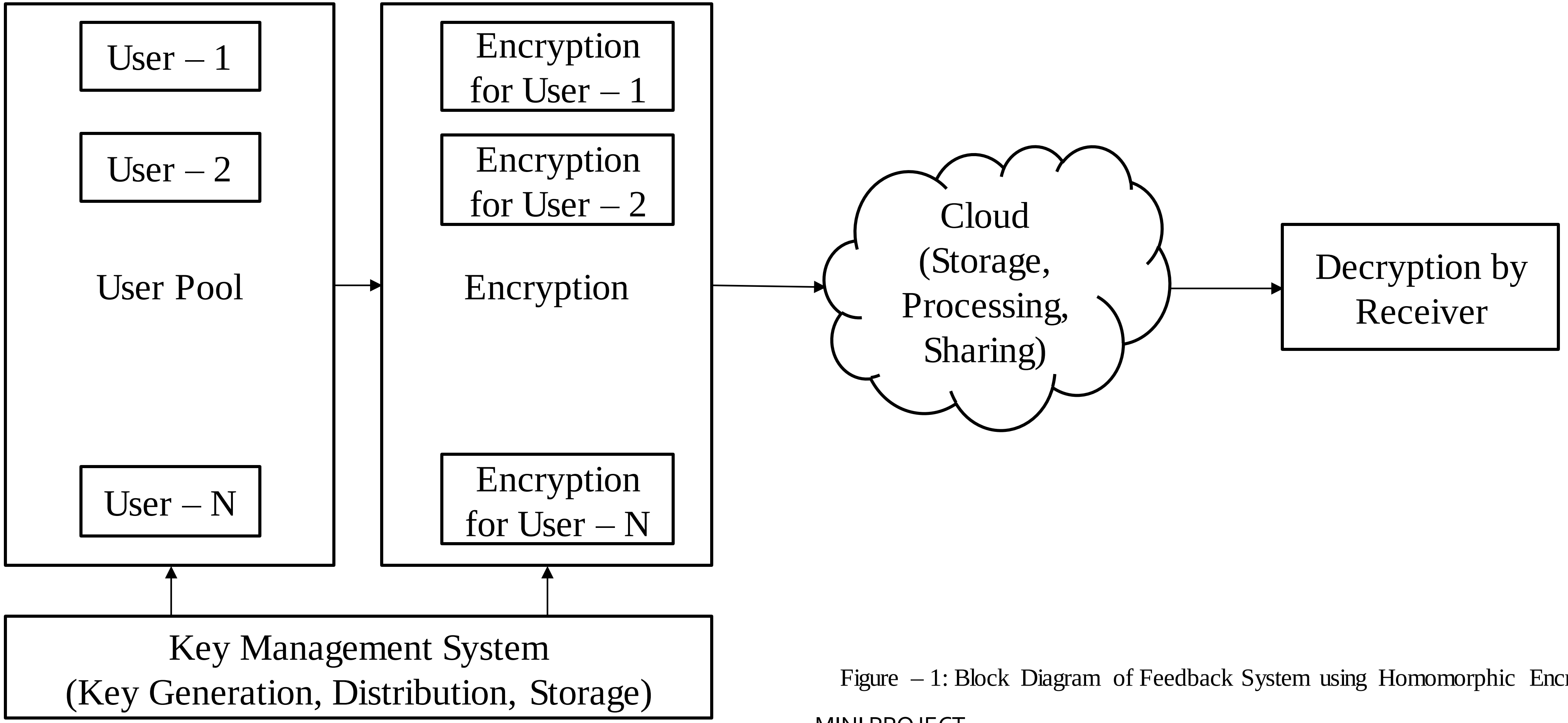

Figure – 1: Block Diagram of Feedback System using Homomorphic Encryption

RSA Algorithm

- Proposed by Rivest, Shamir & Adleman of MIT in 1977
- Best known & widely used public-key scheme
- Based on exponentiation over Galois Field using large numbers
- Security is due to the cost of factoring large numbers

RSA Algorithm – Mathematical Model

- **Key Generation:**
  - Select p and q — p and q both are prime, $p \neq q$
  - Calculate $n = p \times q$
  - Calculate $\emptyset(n) = (p-1)(q-1)$
  - Select integer e — $\gcd(\emptyset(n), e) = 1; 1 < e < \emptyset(n)$
  - Calculate d — $d \equiv e^{-1}$
  - Public Key — $PU = \{e, n\}$
  - Private Key — $PR = \{d, n\}$

RSA Algorithm – Mathematical Model

- **Encryption:**
  - Plain Text $M < n$
  - Cipher Text $C = M^e mod\, n$
- **Decryption:**
  - Cipher Text C
  - Plain Text $M = C^d\ mod\, n$

Pallier Algorithm – Mathematical Model

- **Key Generation:**
  - Select p and q — p and q both are prime, $p \neq q$
  - Calculate N $= p \times q$
  - Calculate $\lambda = LCM((p-1),(q-1))$
  - Select $g \epsilon Z_N$ — gcd $\left[\left(\frac{g^{\lambda}\ mod\ N^2 - 1}{N}\right), N\right] = 1$
  - Select r — $r \ni |$ gcd$(r, N) = 1$
  - Public Key — $PU = \{N, g\}$
  - Private Key — $PR = \{\lambda\}$

Pallier Algorithm – Mathematical Model

- **Encryption:**
  - Plain text $\mathrm{M} < N$
  - Cipher text $C = g^M r^N \ mod\ N^2$
- **Decryption:**
  - Cipher Text C
  - Plain Text $m = \frac{L(C^\lambda \ mod\ N^2)}{L(g^\lambda \ mod\ N^2)} \ mod\ N$

$L(u) = \frac{u-1}{N}$

BCP Algorithm – Mathematical Model

- **Key Generation:**
  - Select p and q — p and q both are prime, $p \neq q$
  - Calculate $\mathrm{N} = p \times q$
  - Calculate $\lambda = LCM((p-1)(q-1))$
  - Select random α — $\alpha \epsilon Z_{N^2}^{*}$
  - Select random a — $a \epsilon [1, ord(g)]$
  - Select g in $Z_{N^2}^{*}$ — $g = \alpha^2 \, mod \, N^2 \ni | \gcd(g, N^2) = 1$
  - Select random r — $r \epsilon Z_{N^2}^{*}$

BCP Algorithm – Mathematical Model

- **Key Generation:**
  - Calculate h — $h = g^a \, mod \, N^2$
  - Public Key — $PU = \{N, g, h\}$
  - Private Key — $PR = \{a\}$

BCP Algorithm – Mathematical Model

- **Encryption:**
  - Plain text m
  - Cipher text $A = g^r \ mod \ N^2$

    $B = \ h^r(1 + mn) \ modN^2$

- **Decryption – 1 :**
  - Cipher Text A, B
  - Plain Text $m = \frac{\left(\frac{B}{A^a} - 1\right) mod \ N^2}{N}$

BCP Algorithm – Mathematical Model

- **Decryption – 2 :**
  - Cipher Text A, B
  - Plain Text $m = \frac{(D-1) \; mod \; N^2}{N} \pi \; mod \; N$

$D = (\frac{B}{g^{\gamma}})^{\lambda(N)}$

$\gamma = ar \; mod \; N$

$\pi = \lambda^{-1} \; mod \; N$

Type of Homomorphism

Table 1: Type of Homomorphism

Type	RSA	Pallier	BCP
Additive	✗	✓	✓
Multiplicative	✓	✗	✗

Simulation Result – RSA Algorithm

Table 2: Computation time of RSA Algorithm

Key Size (bits)	Key Generation (s)	Encryption Time(s)	Decryption Time (s)
1024	0.48868393898010254	0.001001119613647461	0.025989294052124023
2048	11.12609577178955	0.0010037422180175781	0.1738135814666748
4096	203.83345890045166	0.0010001659393310547	1.2043821811676025

Simulation Result – RSA Algorithm

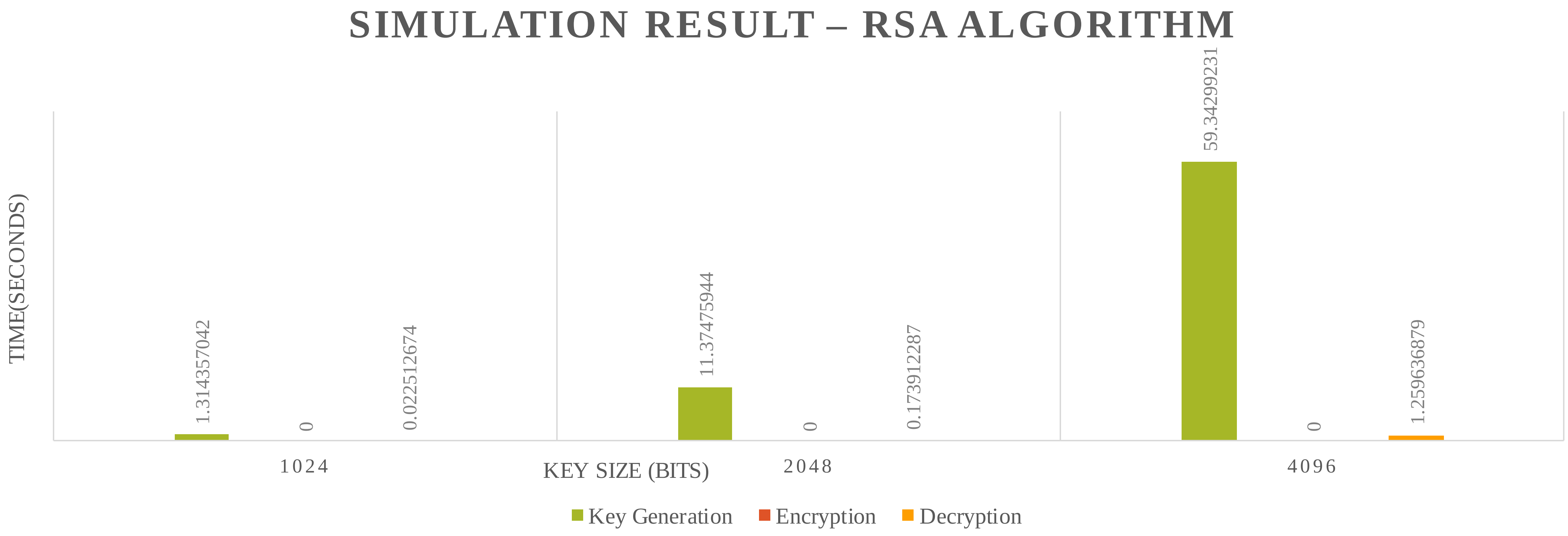

Figure – 2: Simulation Results of RSA Algorithm for different key sizes

Simulation Result – Pallier Algorithm

Table 3: Computation time of Pallier Algorithm

Key Size (bits)	Key Generation (s)	Encryption Time(s)	Decryption Time (s)
1024	0.3499119281768799	0.22691941261291504	0.11163926124572754
2048	32.09730863571167	3.613178253173828	1.7914764881134033
4096	307.2839524745941	10.992461919784546	5.7242114543914795

Simulation Result – Pallier Algorithm

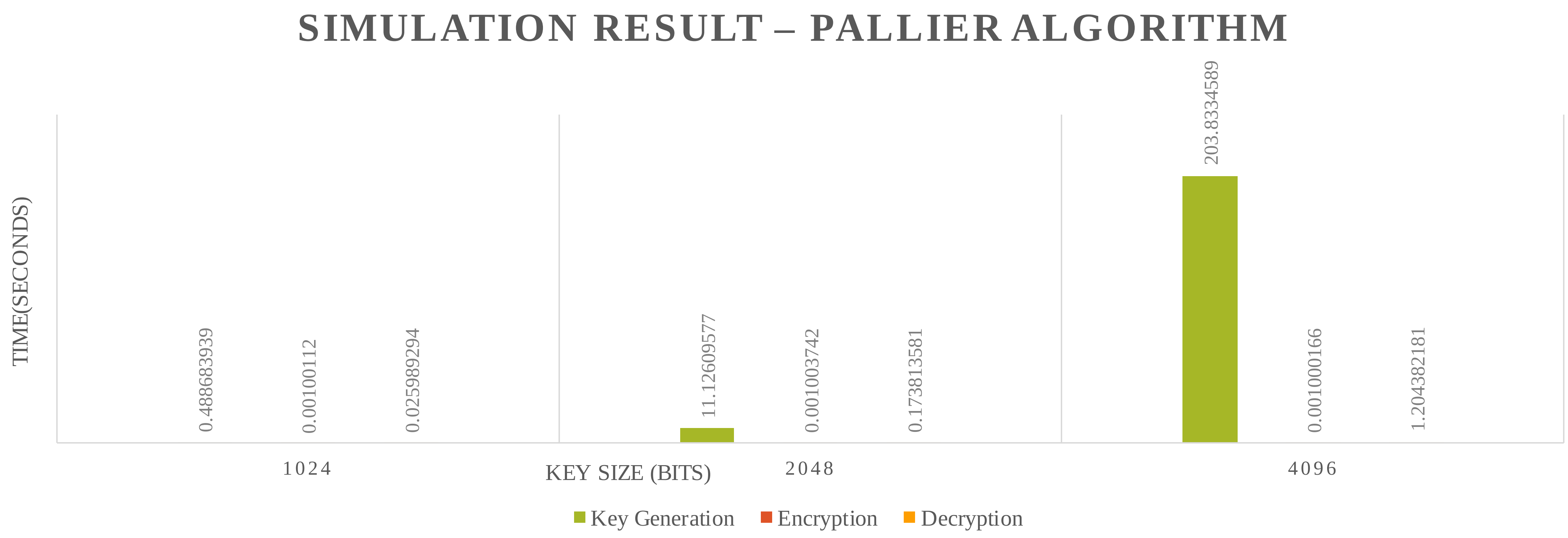

Figure – 3: Simulation Results of Pallier Algorithm for different key sizes

Simulation Result – BCP Algorithm

Table 4: Computation time of BCP Algorithm

Key Size (bits)	Key Generation (s)	Encryption Time(s)	Decryption Time (s)
1024	2.8257832527160645	0.755664587020874	0.7897679805755615
2048	33.3765070438385	4.686594486236572	4.754042863845825
4096	324.53938579559326	13.682634830474854	9.430419206619263

Simulation Result – BCP Algorithm

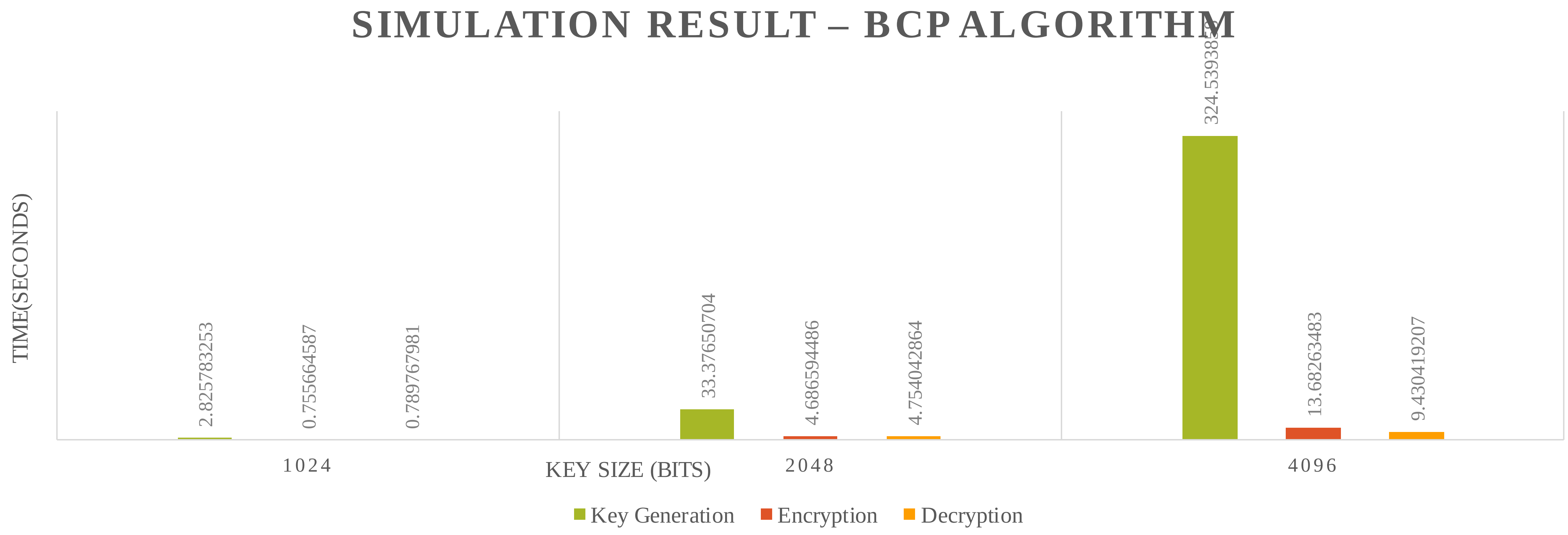

Figure – 4: Simulation Results of BCP Algorithm for different key sizes

References

References

THANK YOU