Isonumber based Iso-Key Interchange Protocol for Network Communication

Mamta S. Dani[1], Akshaykumar Meshram[2*], Rupesh Pohane[3] and Rupali R. Meshram[4]
*Corresponding Author:
[1, 2,*]Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur-441110, M.S., India
[3]Department of Applied Mathematics, Suryodaya College of Engineering and Technology, Nagpur-440027, M.S., India
[4]Department of Mathematics, Kamla Nehru Mahavidyalaya, Nagpur-440024, M.S., India

Summary
Key exchange protocol (KEP) is an essential setup to secure authenticates transmission among two or more users in cyberspace. Digital files protected and transmitted by the encryption of the files over public channels, a single key communal concerning the channel parties and utilized for both to encrypt the files as well as decrypt the files. If entirely done, this impedes unauthorized third parties from imposing a key optimal on the authorized parties. In this article, we have suggested a new KEP term as isokey interchange protocol based on generalization of modern mathematics term as isomathematics by utilizing isonumbers for corresponding isounits over the Block Upper Triangular Isomatrices (BUTI) which is secure, feasible and extensible. We also were utilizing arithmetic operations like Isoaddition, isosubtraction, isomultiplication and isodivision from isomathematics to build iso-key interchange protocol for network communication. The execution of our protocol is for two isointegers corresponding two elements of the group of isomatrices and cryptographic performance of products eachother. We demonstrate the protection of suggested isokey interchange protocol against Brute force attacks, Menezes et al. algorithm and Climent et al. algorithm.

Keywords:
Cryptography, Block Isomatrix, Isomathematics, Isonumber, Isounit.

1. Introduction

Now a days, the security is main concern in large open network. To set up a private channel among two users' needs to interchange a mutual secret key [2]. It is feasible in limited and small network but not possible in large and broad networks like internet. The public-key cryptography (PKC) offers a technique to permit secret session keys to be interchange over an unprotected network in which each user holds key pair comprising of a non-secret key and a secret key such that only non-secret keys are published in network. Diffie–Hellman offered first feasible PKC in 1976 [3]. Number theory problems are the attraction in cryptographic researcher to build prominent PKC in which at least two user, user-I utilize the user-II non-secret key and encrypts the information and then transmits to user-II. After getting the encrypted text, the user-II can decrypt the information with utilizing of his/her secret key [4].

Meshram C. [5-8] developed certain PKC schemes which are depends on solving discrete logarithm problem and integer factoring problem along with its generalization. Moreover offered specific designs for identity-based cryptography [09-15]. Blake I. and Climent J., independently study the Elliptic Curve discrete logarithm problem which is one of the main problems where PKC are constructed [16-17]. Meshram A. [18-20] proposed certain cryptographic schemes based on suzuki 2-group and dihedral group.

Recently, Meshram C. [21] introduce Quadratic Exponentiation Randomized PKC based on Partial Discrete Logarithm Problem. Meshram A. recommended $\mathcal{KEP}$ constructed on isoring isopolynomials coefficient [22]. Dani M. recommended $\mathcal{SISK}$ based $\mathcal{KEP}$ for protected transmission [23] and $\mathcal{KEP}$ based on $\mathcal{SIFK}$ [24]. Thatere A. recommended isoryptosystem constructed on $\mathcal{SIFK}$ [25].

2. Motivations and Organization

In this article, we have proposed an isokey interchange protocol based on isonumbers for corresponding isounits over $\mathcal{BUTI}$. The primary thought of this article is to examine, for two isointegers $\hat{a}$ and $\hat{b}$ with elements of the group of isomatrices $\hat{\mathcal{H}}_1$ and $\hat{\mathcal{H}}_2$, the cryptographic performance of products of the nature $\hat{\mathcal{H}}_1^{\hat{a}}$ $\hat{\mathcal{H}}_2^{\hat{b}}$.

The rest of the article is coordinated in various sections. In section 3, we have reviewed the prerequisite background for article. Section 4, describes the suggested isokey Interchange Protocol. Section 5, investigate the security analysis of suggested isokey Interchange Protocol. Finally, in section 6, we have concluded the article.

Manuscript received February 5, 2022
Manuscript revised February 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.2.27