A Python based Digital Signature implementing RSA

A PROJECT REPORT

Submitted as a Jth Component for the course

MCA

by

Ruchi Mantri	**20MCA0132**
Dev Sharma	**20MCA0129**
Arka Seal	**20MCA0126**

Under the Guidance of

Dr. Navaneethan C

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology & Engineering

August, 2021

DECLARATION BY THE CANDIDATE

I hereby declare that the project report entitled "**A Python based Digital Signature implementing RSA"** by me to VIT University, Vellore in partial fulfilment of the requirement for the award of the degree of **MCA** is a record of Jth component of project work carried out by me under the guidance of **Dr. Navaneethan C**. I further declare that the work reported in this project has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: Vellore **Signature of the Candidate**

Date: 12-August-2021 Dev Sharma

20MCA0129

***Abstract*-Network Information Security is an important concept for maintain web confidentiality, integrity and authenticity. This domain looks after our digital wellbeing and took up the task of maintaining stability of our digital life. Digital signature can be considered as a live demo of the Authenticity domain.**

Keeping this in mind we plan on developing Digital Signature Algorithm using RSA. To provide authentication for any of the send messages an Encrypted hash value is to be attached with the message acting as the signing component. The receiver further on receiving it verifies the signature to authenticate the sender. We have put all these together with means of simplified Python coding for each and every component with a GUI implementation.

TABLE OF CONTENTS

1.
INTRODUCTION

1.1 Introductory Remarks

Digital Signature is one of the main key factors in providing authenticity in present day digital world. We aim for one such Digital Signature with RSA implementation with our own simple yet effective Hash value analysis and further its RSA encryption technique. We coded the entire paradigm in Python IDLE using tkinter module. So that we have a GUI based Sender Receiver architecture. We used Sender RSA Private Key to encrypt the hash value and the respective RSA Public Key to decrypt on the Receiver's end.

Now, coming to the hash value, it is calculated using a simple but effective hash function on the Message to be send. The speciality of the hash key is it can't be used as a back-tracking component to recover the message; it is only used as an authenticating factor here. This hash value is produced and send attached to the main message by the Sender and on the Receiver this hash value is compared with the original received message's hash value and verified the authenticity of the message. DSA can be implemented without RSA also but we skipped complication and made an easy and simply understood prototype on which further work can be carried on, on integrating with other components or APIs.

2.

Literature Survey and Review

1. An efficient digital signature using self-certified public keys.

In proceedings of the 1st ACM confernce on Computer and Communications 2003, pp.62-73.

Yuan Zhou, Department of Computer Science and Engineering Shanghai Jiao Tong University 1954 Huashang Road, Shanghai 200030, P. R. China

ISSUES IN PREVIOUS-The common problem in all public key schemes is how to guarantee a public key is indeed linked to the liner who claims to be the legitimate owner. The solution to this problem is obviously that public keys must be authenticated.

METHODOLOGY/APPLICATIONS-In this paper, we first analyze the notion of self-certified public keys, which was first introduced by Girault [5], and then we extend it. After that, we will adopt tile extended concept to propose a new signature scheme. The proposed scheme has a property that tile signer's public key cml simultaneously be authenticated in verifying the signature. Compared to earlier self-certified signature schemes, our scheme is more efficient and provable secure.

PROS/CONS-The scheme is efficient, so it can be applied in many low-computation devices, such as cell phone, pages, smart cards etc.

The proposed scheme is not only of level 3, but also efficient. Compared with other schemes based on discrete logarithm problem, the scheme reduces the amount of time-consuming computation.

2. A Review of Digital signature and hash function-based approach for secure routing in VANET

Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021) Surrender Kumar department of CST

ISSUES IN PREVIOUS -The common problem in the old vehicle technology is the safety of the drivers as well as the passengers.

METHODOLOGY/APPLICATIONS- Our research work's main objective is to improve the performance of VANET protocol using digital signature and hash function cryptography algorithm. The Vehicular Adhoc Network (VANET) is a newly created technology for intervehicle communications to accomplish traffic safety and productivity purposes. To improve the performance of VANET using a routing protocol, we propose a secure routing protocol using two strategies of digital signature and hash function for VANET to keep the routing performance from degradation. The proposed research study's specific statement is "Digital signature and hash function-based approach for secure routing in VANET."

PROS/CONS- security and safe message delivery are critical issues. The challenges of providing data security, reducing data risks, and reliability in data accessibility are also presented.

3. Alternative Proposal of Tracking Products Using Digital Signatures and QR Codes.

2010 International Conference on Challenges in Environmental Science and Computer Engineering

Department of Computer Network Systems Instituto de Brasilia, DF – Brazil

ISSUES IN PREVIOUS -n the modern business process of products commercialization, the transport, tracking and appliance delivery inspection are very important factors, so important that large, medium and small-sized companies can lose strategic customers because of mistaken deliveries, deliveries of products with wrong specification of model or technical features.

METHODOLOGY/APPLICATIONS- n the modern business process of products commercialization, the transport, and tracking and appliance delivery inspection are very important factors, so important that large, medium and small-sized companies can lose strategic customers because of mistaken deliveries, deliveries of products with wrong specification of model or technical features.

PROS/CONS-using QR Codes for tracking products, results in a low cost and high feasibility solution from an economic standpoint and computational complexity.

Another issue that must be considered is the secure storage of IDi and Li information in the datacenter, which needs to be developed considering risks and vulnerabilities

4. An E-Commerce Security Solution using MJ2–RSA Digital Signature

E.Madhusudhana Reddy K.Suresh Kumar Reddy M.Padmavathamma Professor, Dept of CSE Research Scholar Prof & Head, Dept of CS Madanapalle Institute of Technology S.V.University S.V.University & Science, Madanapalle-517325 Tirupati-517502 Tirupati-517502 India

ISSUES IN PREVIOUS -The issues in basic RSA technique are the main issues like RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer. It requires a third party to verify the reliability of public keys. Data transferred through RSA algorithm could be compromised through middlemen who might temper with the public key system.

METHODOLOGY/APPLICATIONS- In this article we develop a new Digital Signature Schemes which are extension of some variants of the RSA Digital Signature Schemes. We extend new variant with the help of the properties of Jordan-Totient function [2]. We briefly discuss the possibility and validity of combining new variant with algorithm, java code, test result and graphical performance analysis to obtain a new efficient and general Digital Signature Schemes.

PROS/CONS-This result helps in enhancement of the block size for plaintext and enhances the range of public / private keys. The increase in the size of private key avoids the attacks on private key. This concludes that MJ2-RSA provides more security with low cost.

5. An Improved RSA Signature Algorithm based on Complex Numeric Operation Function

2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)

School of Mathematics and Information Science, East China Institute of Technology, Fuzhou, China

ISSUES IN PREVIOUS -There are many digital signature algorithms established, in which the Hash, DSA and RSA are the common ones. The main restriction of Hash algorithm is the receiver must have a copy of the sender's private key to verify the signature, so the encryption system is easy to be attacked and the signature can be forged. DSA (Digital Signature Algorithm) is another common public key algorithm, but it has no data encryption function, it can only be used for digital signature.

METHODOLOGY/APPLICATIONS- Digital signature can be realized by using RSA algorithm. RSA is widely used in public-key cryptosystem. But running this algorithm needs lots of time and memory. This paper proposes a RSA signature algorithm to fit for the devices with low computational power. The new signature algorithm is based on complex numeric operation function. This paper expounds the fundamental principles of RSA algorithm. The realization of RSA algorithm includes the generation of RSA cryptographic key and the encryption and decryption of data. By using RSA algorithm, we can use the private key of the sender to sign the plaintext and the public key of the receiver to encrypt. For the receiver, he can use his private key to decrypt and the public key of the sender to verify the signature.

PROS/CONS-The random RSA public and private key pair with arbitrary length can be generated effectively by using the C++ large number library design by the algorithm proposed in this paper. A 1024 bits RSA key can be generated within 2 minutes on common PC platform, while the encryption/ decryption operation on data less than 1024 bits can be done within 2 seconds, the efficiency of RSA system is greatly improved, which provides important guarantees for implementation high security RSA algorithm with long keys on PC platform.

6. Design and Implementation of an Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)

2010 International Conference on Challenges in Environmental Science and Computer Engineering

Yasin Genç Dept. of Electrical-Electronics Eng. Gazi University Ankara, Turkey

ISSUES IN PREVIOUS -Information security is one of the issues that gain importance with developing technologies. Digital signature is a concept that has a key role in ensuring information security today. It is used in many areas such as health, banking, commerce, internet of things, electronic voting. Digital signatures are used to provide integrity, authentication, and non-denial.

METHODOLOGY/APPLICATIONS-Digital signatures are increasingly used today. It replaces wet signature with the development of technology. Elliptic curve digital signature algorithm (ECDSA) is used in many applications thanks to its security and efficiency. However, some mathematical operations such as inversion operation in modulation slow down the speed of this algorithm. In this study, we propose a more efficient and secure ECDSA. In the proposed method, the inversion operation in modulation of signature generation and signature verification phases is removed. Thus, the efficiency and speed of the ECDSA have been increased without reducing its security. The proposed method is implemented in Python programming language using P-521 elliptic curve and SHA-512 algorithm.

PROS/CONS-A more efficient and secure version of ECDSA is designed and implemented. The inversion operation that is included in both signature and verification in ECDSA is an expensive and time-consuming operation in modular arithmetic. The duration of the multiplication is much higher compared to addition and subtraction. Hardware-based applications require more time to perform inversion operation in modular arithmetic than software-based applications.

7. Detection of Blind Signature Using Recursive Sum

2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)

Avinash Pandey, Dhruv Mahajan, Shivank Gupta and Vishal Rastogi Jaypee Institute of Information Technology, Noida, India

ISSUES IN PREVIOUS -The Main difference between digital and handwritten signature is that a digital signature cannot be fixed. It can change as per security requirements.

METHODOLOGY/APPLICATIONS-Digital signatures are suitable technology for public key encryption. Acceptance (non-repudiation) of digital messages and data origin authentication are one of the main usages of digital signature. Digital signature's security mainly depends on the keys (public and private). These keys are used to generate and validate digital signatures. In digital signature signing process is performed using signer's secret key. However, any attacker can present a blinded version of message encrypted with signer's public key and can get the original message. Therefore, this paper proposed a novel method to identify blinded version of digital signature. The proposed method has been tested mathematically and found to be more efficient to detect blind signatures.

PROS/CONS-Signer's identity, intent, data integrity, and the nonrepudiation of signed documents is guaranteed by digital signatures. An electronic document signed with a digital signature are similar to other signed paper documents and can also use in court as a proof.

8. Digital Image Authentication and Encryption using Digital Signature

Shahzad Alam, Amir Jamil Department of Computer Engineering, Faculty of Engineering and Technology, Jamia Millia Islamia, New Delhi-110025, India

2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India

ISSUES IN PREVIOUS -In modern era, technology has its own benefits and pitfalls. The major drawbacks include the unethical intrusion over the channels to steal the important information from the sender.

METHODOLOGY/APPLICATIONS-In this paper, a methodology for digital image authentication using digital signature is proposed. The hash of the original image is taken and is encrypted by RSA. The digital signature obtained is concealed in the image. Digital signature is sent along with the encrypted image which decreases the probability of meticulous attack by the intruder. The encrypted image is shuffled using Chaotic Logistic Map to get the final shuffled encrypted image. The use of Logistic Map improves the randomness in the image. For the authentication, a comparator is employed which evaluates correctness of the hash extracted. The simulations have been carried out to examine the proposed authentication and encryption technique.

PROS/CONS-This project successfully transfers the digital signature over the channel without giving the chances of intrusion by the intruder. Even if the image is intruded at the receiver end, the receiver will be able to differentiate between obtained image and original image by comparing the hashes

9. Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)

2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems Yogyakarta, Indonesia, November 08-10, 2017

Rizky Damara Ardy Faculty of Computer Science Dian Nuswantoro University Semarang, Indonesia rizky.damara.ardy@gmail.com

ISSUES IN PREVIOUS -In modern era, technology has its own benefits and pitfalls. The major drawbacks include the unethical intrusion over the channels to steal the important information from the sender.

METHODOLOGY/APPLICATIONS-In this paper, a methodology for digital image authentication using digital signature is proposed. The hash of the original image is taken and is encrypted by RSA. The digital signature obtained is concealed in the image. Digital signature is sent along with the encrypted image which decreases the probability of meticulous attack by the intruder. The encrypted image is shuffled using Chaotic Logistic Map to get the final shuffled encrypted image. The use of Logistic Map improves the randomness in the image. For the authentication, a comparator is employed which evaluates correctness of the hash extracted. The simulations have been carried out to examine the proposed authentication and encryption technique.

PROS/CONS-This project successfully transfers the digital signature over the channel without giving the chances of intrusion by the intruder. Even if the image is intruded at the receiver end, the receiver will be able to differentiate between obtained image and original image by comparing the hashes

10. Implementation of Digital Signature Using AES and RSA Algorithms as a Security in Disposition System of Letter.

1st Annual Applied Science and Engineering Conference

ISSUES IN PREVIOUS - Security letter safeguarded by performing encryption on the file name of the letter, but there was no security for the contents of the letter itself

METHODOLOGY/APPLICATIONS- Activities correspondence is often used by agencies or companies, so that institutions or companies set up a special division to handle issues related to the letter management. Most of the distribution of letters using electronic media, then the letter should be kept confidential in order to avoid things that are not desirable. Techniques that can be done to meet the security aspect is by using cryptography or by giving a digital signature. The addition of asymmetric and symmetric algorithms, i.e. RSA and AES algorithms, on the digital signature had been done in this study to maintain data security. The RSA algorithm was used during the process of giving digital signature, while the AES algorithm was used during the process of encoding a message that will be sent to the receiver. Based on the research can be concluded that the additions of AES and RSA algorithms on the digital signature meet four objectives of cryptography: Secrecy, Data Integrity, Authentication and Non-repudiation. Keywords: Mail, Digital Signature, Cryptography, AES and RSA algorithms.

PROS/CONS- Effect of digital signatures using algorithms AES and RSA algorithms and disposition system of letter meet the four cryptographic purposes, namely secrecy, data integrity, authentication and non-repudiation.

11. Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm

2018 4th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia.

Farah Jihan Aufa, Endroyono, Achmad Affandi, Department of Electrical Engineering Institute Teknologi Sepuluh Nopember Surabaya.

ISSUES IN PREVIOUS – Public key cryptography is widely used. DSA and RSA both are included in public key cryptography to make it even more efficient both RSA and DSA could be combined and the bits which performed better can be chosen among all present in it.

METHODOLOGY/APPLICATIONS- Public key cryptography or asymmetric keys are widely used in the implementation of data security on information and communication systems. The RSA algorithm (Rivest, Shamir, and Adleman) is one of the most popular and widely used public key cryptography because of its less complexity. RSA has two main functions namely the process of encryption and decryption process. Digital Signature Algorithm (DSA) is a digital signature algorithm that serves as the standard of Digital Signature Standard (DSS). DSA is also included in the public key cryptography system. DSA has two main functions of creating digital signatures and checking the validity of digital signatures. In this paper, the authors compare the computational times of RSA and DSA with some bits and choose which bits are better used.

PROS/CONS- In this paper, a combination method of RSA 1024 and DSA 512 has been performed since the computation time is relatively fast. Obtained time for key generation is 33.5% slower than RSA and DSA generation time separately. It has 60% faster computational time in encrypt and signing process. And for decryption and verifying time, it has a 23% faster than RSA and DSA separately. This combination method not only can encrypt messages, but also provide digital signatures for authentication process safely and fast.

12. Security Enhancement of Digital Signatures for Blockchain using EdDSA Algorithm

Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).

Mr. Shaik Johny Basha, Mr. Venkata Srinivasu Veesam, Ms. Tamminina Ammannamma, Ms. Sirisha Navudu, Mr. M.V.V.S. Subrahmanyam.

ISSUES IN PREVIOUS – To provide security in the transactions process of hashing, blockchain technology was using the Elliptic Curve Digital Signature Algorithm (ECDSA). Using the ECDSA Algorithm, if any error has happened, this may lead to identify the private key value that which can acquire matching signatures for various documents.

METHODOLOGY/APPLICATIONS- Blockchain will be the most used technology in the next decade with the key features of distributed ledger and high security. To provide security in the transactions process of hashing, blockchain technology was using the Elliptic Curve Digital Signature Algorithm (ECDSA). To avoid that problem, we suggest using the Edwards-curve Digital Signature Algorithm (EdDSA) Algorithm in generating the hash functions among the transactions, which provides the high-level speed, getting the best performance, and independence in generating the random number. Our suggestion provides improved security while compared to the ECDSA Algorithm.

PROS/CONS- In this paper, we have discussed about blockchain and its types of networks. Followed by the introduction, discussed about the working nature of blockchain i.e., starting from the transaction (initial step) to the complete block added after the transaction. After that, described the Digital Signature, various types and schemes in digital signature. In the next section, discussed about related work of EcDSA algorithm in supply chain management, DNS Networking, etc. Then gave the theoretical analysis of time consumption, performance evaluation with the respective analyzed graphs. In future, we want to work on reducing the power consumption of the EdDSA over the ECDSA and obtain good results in that.

13. Securely Transfer Information with RSA and Digital Signature by using the concept of Fog Computing and Blockchain

2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), 27-28 February, Dhaka

Anika Tabassum, Humayra Anjumee Jeba, S. M. Salim Reza and Dilshad Ara Hossain, Department of Information and Communication Engineering, Bangladesh

University of Professionals, Dhaka, Bangladesh 5Department of ICE, International Islamic University Malaysia (IIUM)

ISSUES IN PREVIOUS – In the modern era of technology, cloud computing has been on the rise in the office management system. However, due to some concerning issues regarding provided security by the cloud, it has been losing its publicity.

METHODOLOGY/APPLICATIONS- With the introduction of fog computing with its advantageous feature of decentralization, this system has replaced traditional cloud systems in various organizations. In this paper, we propose a smart office system which is based on fog computing. Blockchain is implemented to ensure overall system security and user authentication has been conducted by creating wallets in the blockchain system. The overall transaction process has been carried out with the popular bitcoin method. Information sharing has been implemented with the help of RSA algorithm and digital signature scheme.

PROS/CONS- In this paper, we have proposed a demonstration of an office system to share a file in a secure manner between office employees using RSA or public key infrastructure in the blockchain and fog environment. In the proposed architecture, the authentication process is carried out with user entry in the blockchain system. The transaction process between two users is executed with the popular Bitcoin method. The storage system in our proposed architecture is decentralized in nature as fog computing is based on decentralization. In the proposed model, the information process is executed by asymmetric key cryptography which generates both public and private keys. Data confidentiality is maintained in this process as both keys are simultaneously used. With the inclusion of a digital signature, data authenticity and integrity is assured.

14. Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles against Man-In-The-Middle Attack

2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE)

Yucheng Li and Cong Pu Department of Computer Sciences and Electrical Engineering Marshall University, Huntington, WV 25755, USA

ISSUES IN PREVIOUS – Micro aerial vehicles, a.k.a. drones, have become an integral part of a variety of civilian and military application domains, including but not limited to aerial surveying and mapping, aerial surveillance and security, aerial inspection of infrastructure, and aerial delivery. Meanwhile, the security and privacy of drones are gaining significant attention due to both financial and strategic information and value involved in aerial applications. Due to the lack of security features in communication protocols, an adversary can easily interfere with on-going communications or even seize the control of drone.

METHODOLOGY/APPLICATIONS- In this paper, we propose a lightweight digital signature protocol, also referred to as DroneSig, to protect drones from man-in-the-middle attack, where an adversary eavesdrops the communications between Ground Control Station (GCS) and drone, and impersonates the GCS and sends fake commands to terminate the ongoing mission or even take control over the drone. The basic idea of the DroneSig is that the drone will only execute the new command after validating the received digital signature from the GCS, proving that the new command message is coming from the authenticated GCS. If the validation of digital signature fails, the new command is rejected immediately and the Return-to-Launch (RTL) mode is initiated and forces the drone to return to take-off position.

PROS/CONS- In this paper, we proposed a lightweight digital signature protocol (DroneSig) to protect drones from man-in-the-middle attack, where an adversary eavesdrops the communications between Ground Control Station and drone, and impersonates the Ground Control Station and sends fake commands to terminate the ongoing mission or even take control over the drone. The basic idea of the DroneSig is that the drone will only execute the new command after validating the received digital signature from the Ground Control Station, proving that the new command message is coming from the authenticated Ground Control Station. If the validation of digital signature fails, the new command is rejected immediately and the Return-to-Launch (RTL) mode is initiated and forces the drone to return to take-off position.

15. Digital Signature Based on ISRSAC

Authorized licensed use limited to: VIT University. Downloaded on August 01,2021 at 06:22:27 UTC from IEEE Xplore.

Teng Yang, Yanshuo Zhang, Song Xiao, Yimin Zhao, Xidian University, Xi'an 710071, China

ISSUES IN PREVIOUS – Digital signature has recently played an increasingly important role in cyberspace security. Most of them are based on the public key cryptography. Public key cryptography is a mainstream cryptographic algorithm system that has been widely used in cyberspace security in recent years. But the security improvements in this should be made to make it more and more efficient.

METHODOLOGY/APPLICATIONS- The most classic public key cryptography algorithm is RSA and its difficulty is based on the large integer decomposition problem. In 2017, ISRSAC was proposed by M.Thangaval. ISRSAC has made security improvements to the RSA algorithm by increasing the complexity in factoring the value of modulus 'n'. A digital signature algorithm based on ISRSAC algorithm was completed in this paper, and furthermore, a proxy signature algorithm based on ISRSAC and two kinds of multi-signature algorithms were presented, which include sequential multi-signature and broadcasting multi-signature.

PROS/CONS- In this paper, a digital signature scheme based on ISRSAC public key cryptography algorithm is given. Then a proxy digital signature scheme, an ordered multiple digital signature scheme and a broadcast multiple digital signature scheme are constructed.

16. Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud

2212-0173 © 2012 Published by Elsevier Ltd. doi: 10.1016/j.protcy.2012.05.079

K.Govindaa , Dr.E.Sathiyamoorthyb, SCSE,VIT University,Vellore, India

ISSUES IN PREVIOUS – In cloud computing infrastructure Digital identity management is one of the challenging tasks. In order to provide access control in a flexible manner to the users based on their identity and past interaction histories the user is authenticated. At the same time confidentiality of the user must be maintained and interoperability across the multiple business domains can be achieved and minimizing the method of Identifying the user.

METHODOLOGY/APPLICATIONS- When we talk about the GDS scheme the member belongs to the team can sign instead of his team. The signatures are basically anonymous, which leads to the Identity anonymization of the real signer (user) in the group with an exception for the group manager. The signatures are verified by using single group key. Group Signature is valid only when it offers anonymity of the signer to others and traceability to the group manager. This feature of the Group digital signature made it as the part of many security applications.

PROS/CONS- In this paper we proposed a protocol in which the group digital signature is generated using the strong RSA algorithm. In this method the freedom of the member is sacrificed by sending the message through the group manager. In future this protocol will be re modified with member's freedom to send and receive the data directly in the cloud but at the same time we have to keep in mind that traceability of user by the group manager must be maintained.

17. Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE

IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, VOL. 65, NO. 3, AUGUST 2019

Anirban Sengupta, Senior Member, IEEE, E. Ranjith Kumar, and N. Prajwal Chandra

ISSUES IN PREVIOUS – Reusable intellectual property (IP) cores from signal processing and multimedia form an integral part of consumer electronics (CE) systems. However, owing to the value it represents, it needs protection against important threats, such as piracy and illegal claim of ownership.

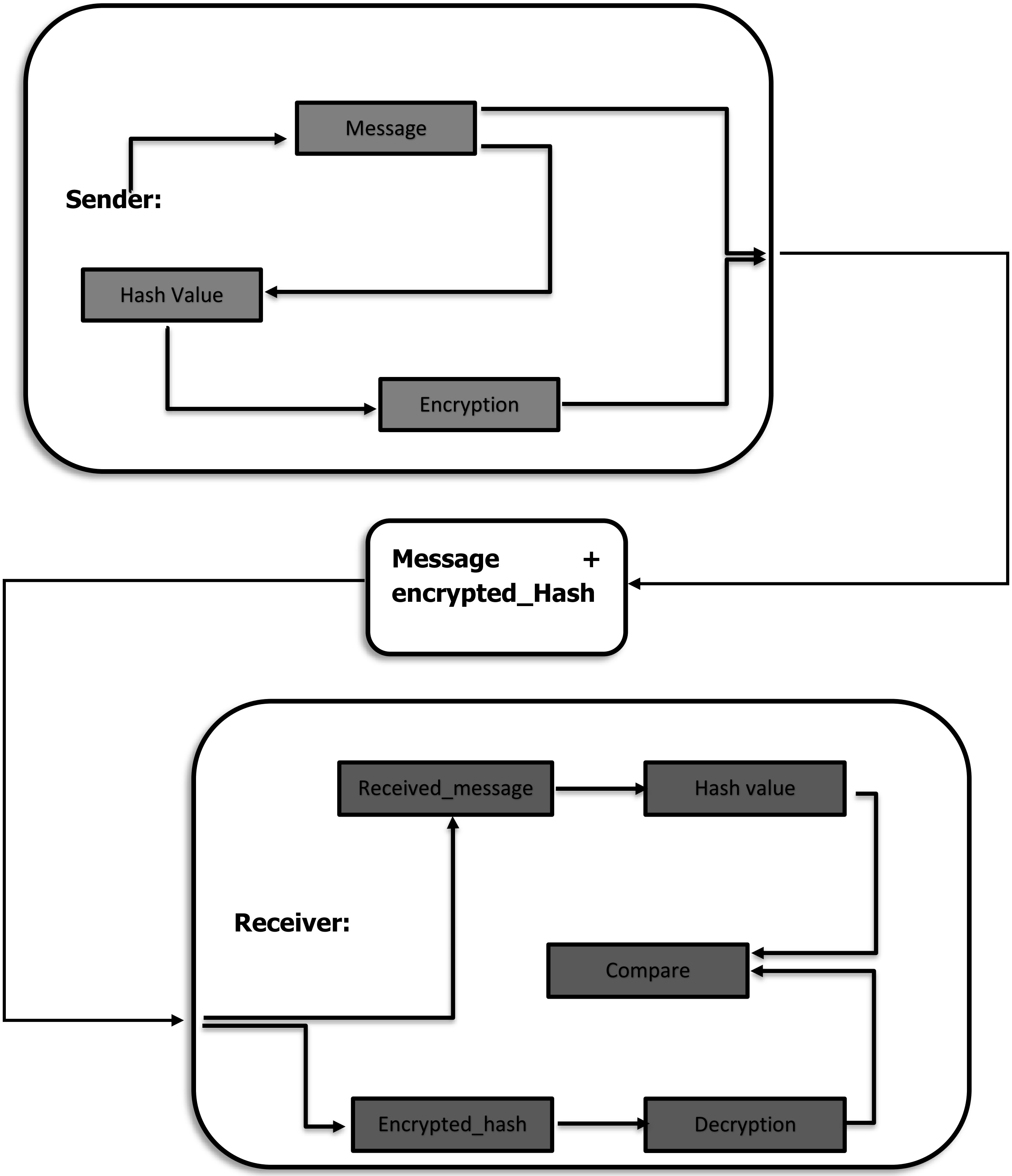
METHODOLOGY/APPLICATIONS- This paper presents a novel multi-level encoding and encrypted-hash-based digital signature for protection of complex reusable IP core used in CE systems. For the first time in the literature, a digital signature-based IP core protection is proposed for digital signal processing (DSP) kernels. The proposed methodology is capable of encoding a DSP kernel application, followed by creating a digest of the encoded application to finally form a digital signature using RSA, which is subsequently implanted into the same design during architectural synthesis. The proposed approach on DSP benchmarks is capable of achieving higher robustness in terms of lower probability of coincidence - indicating stronger proof of authorship. The proposed approach achieves stronger robustness (on average by ~24.8%) as well as requires lesser storage hardware (on average reduction of ~14%) compared to similar prior work.

PROS/CONS- In this paper a novel multi-level encoding and encryptedhash based digital signature for protection of reusable IP cores is presented. The proposed approach yields stronger protection through highly robust digital signature and it is reflected in reduction of Pc value on an average by ~24.8% compared to prior work [4], while significantly lowering the average design overhead incurred in terms of storage hardware by ~13.73%.

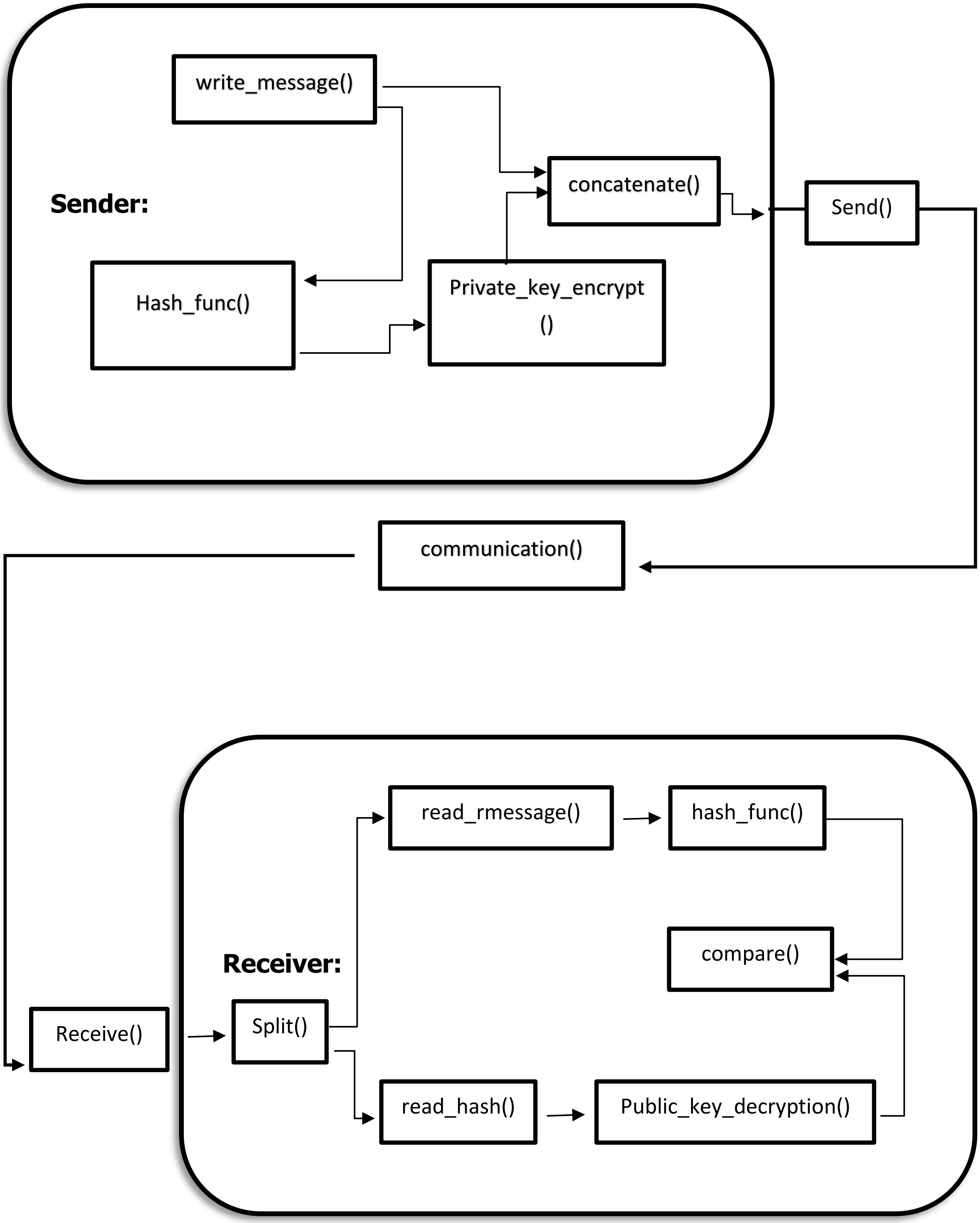
3.

System Details

3.1 System Architecture



3.2 Functional Architecture



4.

System Implementation

4.1 Code and/or Architecture Development

Code for the developed DSA is done below in Python IDLE and later it is deployed using tkinter Python GUI interface.

Python was chosen for:

- Easy and shorter coding related to other languages.
- Easement in GUI interface section.
- Easily available predefined modules for modulus power and prime number (large).

Implementation code:

- Modules imported:

```
from tkinter import *
import sympy
import random
```

- Sender Receiver GUI:

```
senderGUI=Tk()
recieverGUI=Tk()
```

- Extended GCD:

```
def egcd(a,b):
    s=0;old_s=1
    t=1;old_t=0
    r=b;old_r=a

    while(r!=0):
        quotient=old_r//r
        old_r,r=r,old_r-quotient*r
        old_s,s=s,old_s-quotient*s
        old_t,t=t,old_t-quotient*t

    return old_r,old_s,old_t
```

- Modular Inverse:

```
def modularInv(a,b):
    gcd,x,y=egcd(a,b)

    if(x<0):
        x+=b

    return x
```

- Co-Prime Check:

```
def isCoPrime(p,q):
    return gcd(p,q)==1
```

- GCD:

```
def gcd(p,q):
    while q:
        p,q=q,p%q
    return p
```

- Generate Large Prime Numbers:

```
def generateLargePrime(keysize):
    n=sympy.randprime(2**(keysize-1), 2**keysize-1)
    return n
```

- Generate Keys:

```
def generateKeys(keysize=1024):
    e=d=N=0

    p=generateLargePrime(keysize)
    q=generateLargePrime(keysize)

    N=p*q
    phiN=(p-1)*(q-1)

    while True:
        e=random.randrange(2**(keysize-1), 2**keysize-1)
        if(isCoPrime(e,phiN)):
            break

    d=modularInv(e,phiN)

    return e,d,N
```

- RSA Encryption:

```
def encrypt(e,N,msg):
    cipher=""

    for c in msg:
        m=ord(c)
        cipher+=str(pow(m,e,N))+" "

    return cipher
```

- RSA Decryption:

```
def decrypt(d,N,cipher):
    msg=""

    parts=cipher.split()

    for part in parts:
        if part:
            c=int(part)
            msg+=chr(pow(c,d,N))
    return msg
```

- Hash function:

```
def hashing(m):
    h="
    tmp=1
    m=m.upper()
    for i in m:

        h+=str(ord(i))
    #print(h)
    for i in h:
        tmp=int(tmp)          #6566-> 5    tmp=0    =>65+2-> C
        tmp*=int(i)
        if(len(str(tmp))==2):
            tmp=tmp%10
        #print(tmp)

    return chr(tmp+65+len(m))
```

- Main function:

```
def main():
    '''
    p=11 #sympy.randprime(0, 1)
    q=13
    N=p*q
    phiN=(p-1)*(q-1)

    e=13
    d=modularInv(e,phiN)'''
    keysize=32
    e,d,N=generateKeys(keysize)




    return e,d,N
e,d,N=main()
a=StringVar()
senderGUI.title("Sender")
recieverGUI.title("Reciever")

senderGUI.geometry("400x400+100+50")
recieverGUI.geometry("400x400+100+50")

text=Entry(senderGUI,textvariable=a).pack()
sendButton=Button(senderGUI,text='send',fg='black',bg='green',command=send,font=10).pack()
```

- Sender:

```
def send():
    #d,N,enc=main()
    print("Sender....")
    print()
    print()
    msg=hashing(a.get()) #input()#"Arka Seal"
    print("Message: ",a.get())
    print("Hashed value: ",msg)
    enc=encrypt(e,N,msg)
    print("Encrypted Hash value: ",enc)
    b=a.get()+'  ||||   '+str(enc)

    print()
    print()
    print("Message send :",b)
    print()
    print()
    recieve(b)
```

- Reciever:

```
def recieve(msg):
    print()
    print()
    print("Reciever....")
    print()
    print()

    enc=msg.split('  ||||   ')
    msg1=str(enc[0])



    enc=str(enc[1])
    print("Encrypted Hash recieved: ",enc)

```

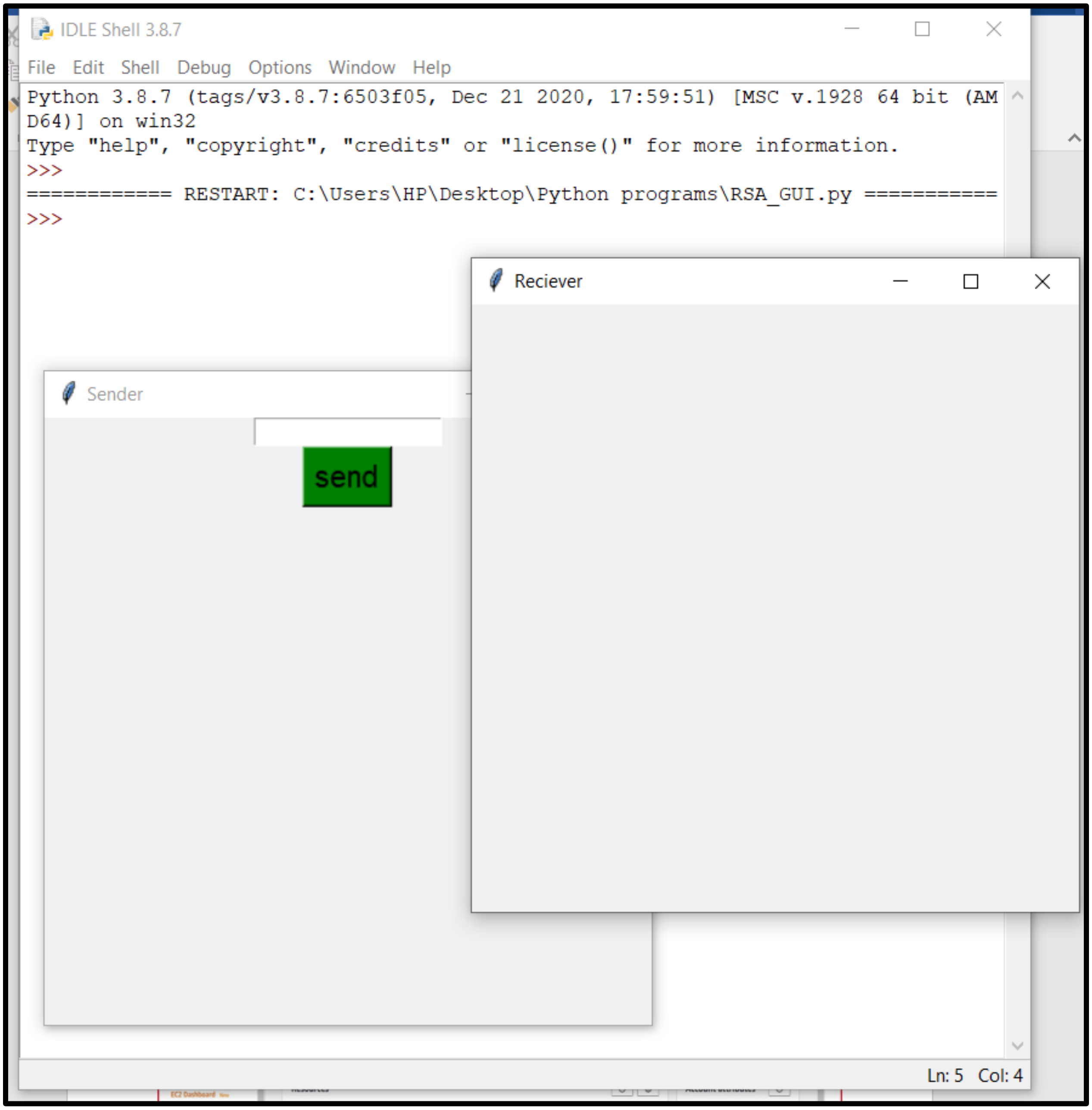
```
recieveLabel=Label(recieverGUI,text=msg,fg='red',bg='yellow',font=10).pac
k()
    dec=decrypt(d,N,enc)
    print("Decrypted Hash value: ",dec)

    if(dec==hashing(msg1)):
        print("Message Hash value: ",hashing(msg1))
        print("as has(recieved message)=decrypted hash value recieve")
        print("Sender authenticated..")
        print("Message recieved: ",msg1)
        recieveLabel=Label(recieverGUI,text='Sender Authenticated, text:
',fg='Black',font=10).pack()

decryptLabel=Label(recieverGUI,text=msg1,fg='green',bg='yellow',font=10)
.pack()
    else:
        recieveLabel=Label(recieverGUI,text='Unauthorised
personel',fg='Black',font=10).pack()
```

4.2 Test Results

After initial execution of code:

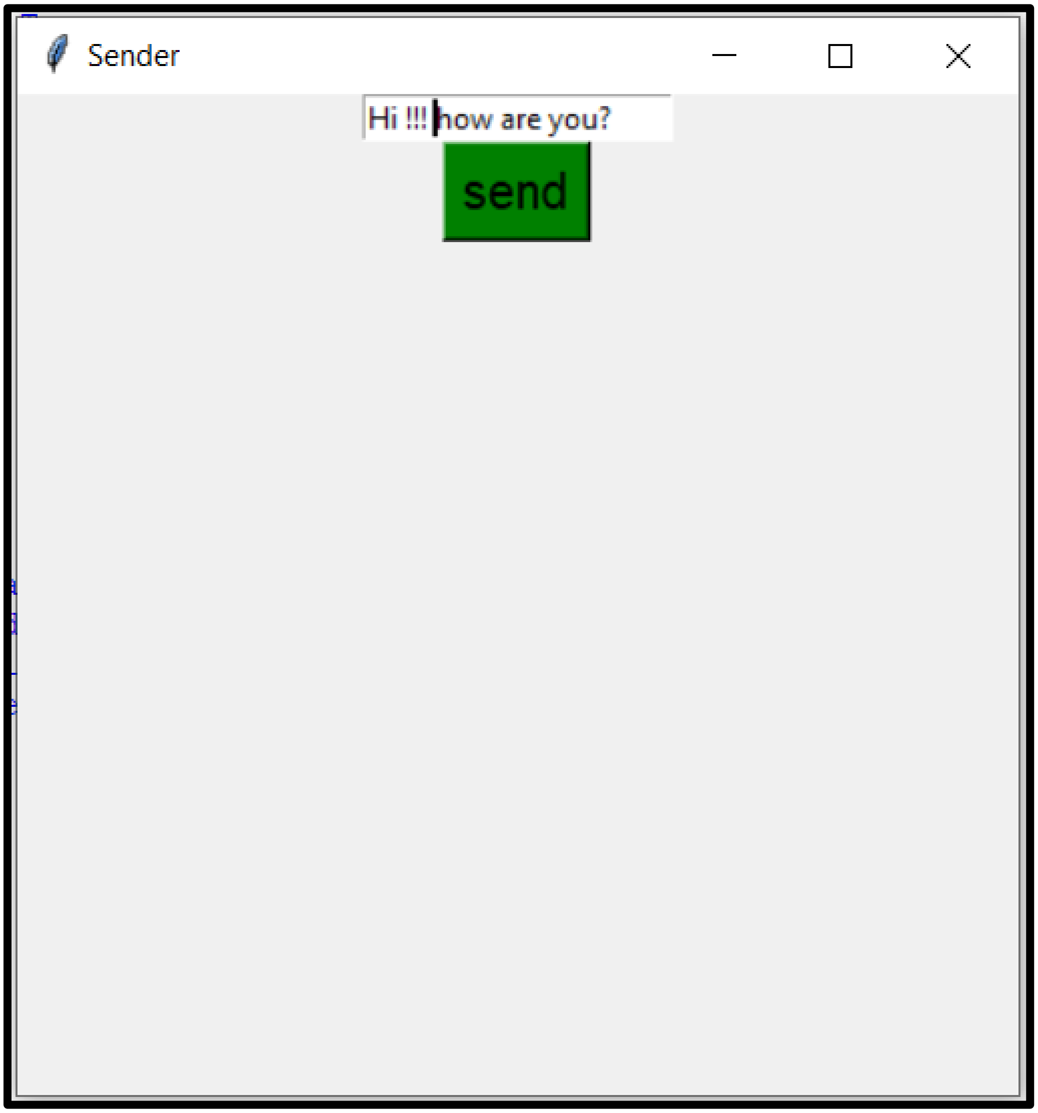


```
Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============ RESTART: C:\Users\HP\Desktop\Python programs\RSA_GUI.py ===========
>>>
```

Figure 1: Empty Sender Receiver GUI as a result of execution (initially)

Sender Window GUI:

Sender sending the message token concatenated with the calculated RSA private key encrypted hash value.

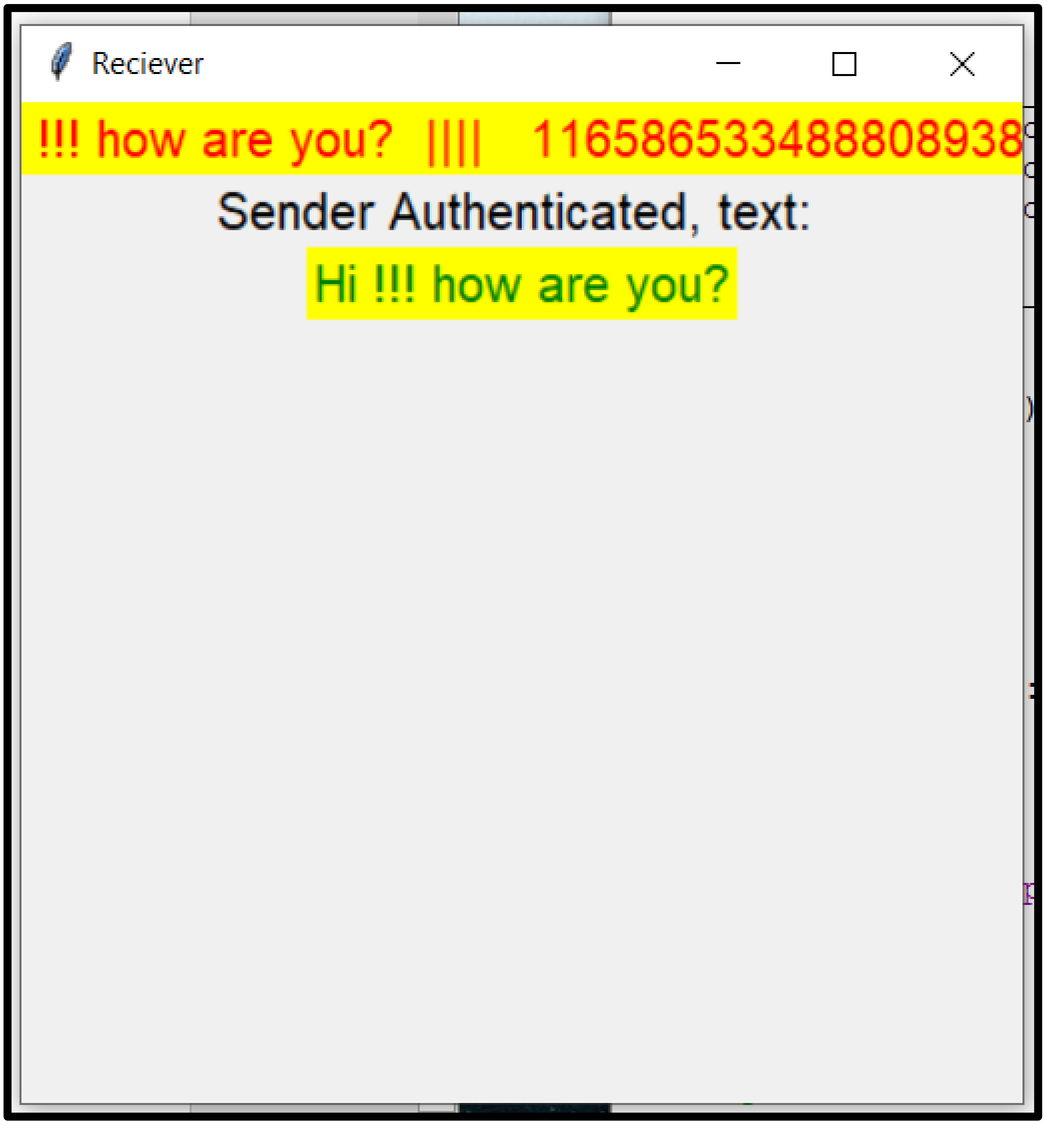


Hi !!! how are you?

Figure 2: Sending Token Message from Sender GUI

Receiving Window GUI:

Message Receiving and authenticating using the hash value and itd decryption.



!!! how are you? |||| 1165865334888089З8

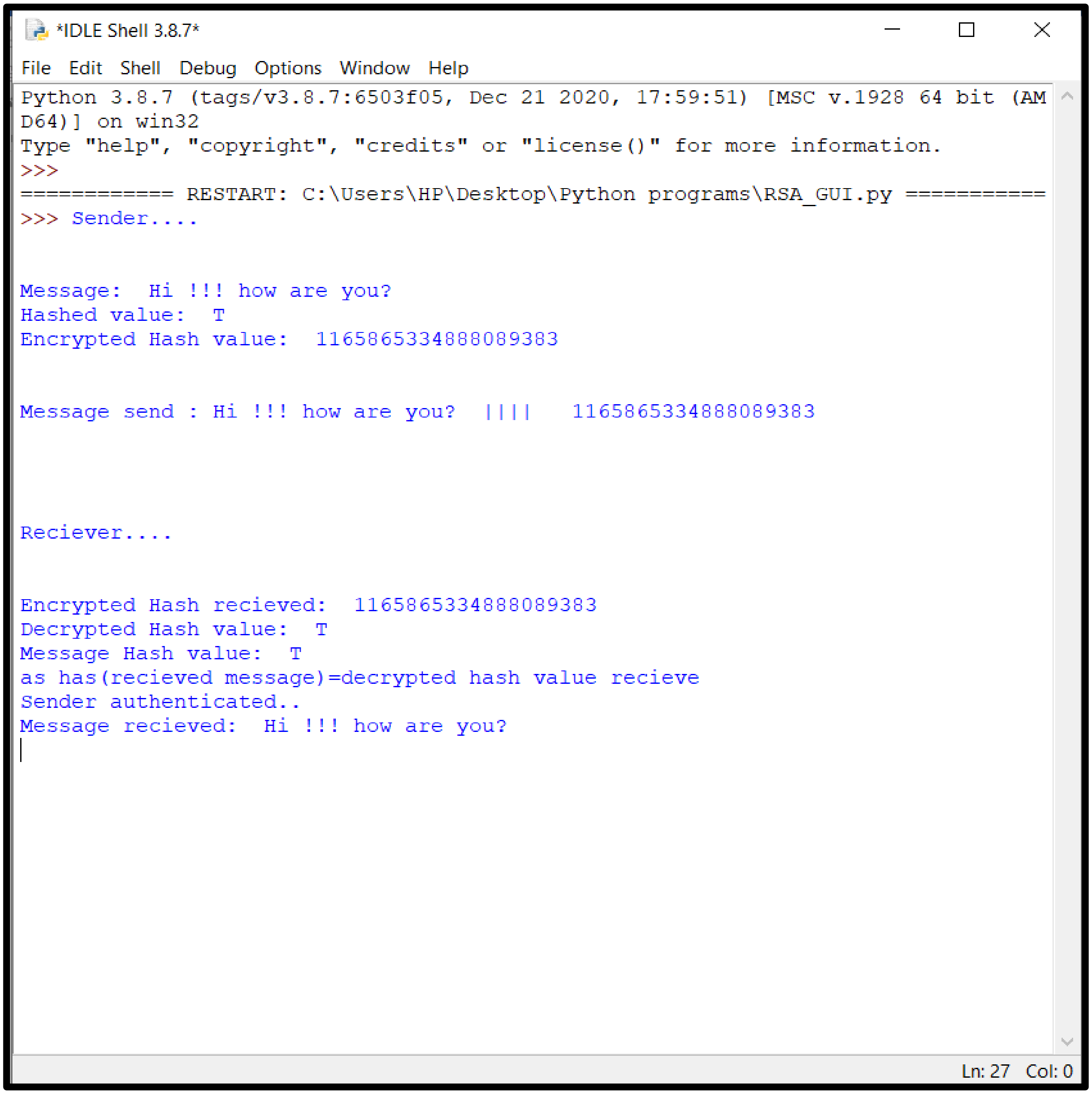
Sender Authenticated, text:

Hi !!! how are you?

Figure 3: Receiver authenticating the received message by verifying the Hash value

IDLE Execution window:

Internal DSA processing with Hash value, encryption, decryption and concatinated message sending and receiving



```
Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
============ RESTART: C:\Users\HP\Desktop\Python programs\RSA_GUI.py ===========
>>> Sender....


Message:  Hi !!! how are you?
Hashed value:  T
Encrypted Hash value:  11658653348880089383


Message send : Hi !!! how are you?  ||||   11658653348880089383




Reciever....


Encrypted Hash recieved:  11658653348880089383
Decrypted Hash value:  T
Message Hash value:  T
as has(recieved message)=decrypted hash value recieve
Sender authenticated..
Message recieved:  Hi !!! how are you?
```

Figure 4: Internal processing- I. Hash value calculation, ii .Encrypting hash Value, iii. Concatenating, iv .Sending message token, v. Receiving message token, vi. Decrypting Hash value, vii .hash value calculation of the test part of the token received and viii. Comparing both hash value for authentication.

5.

Discussion and Future Scope

5.1 Discussion

Our implementation involves a RSA key size of 1024 bits making it almost uncrackable and the hash function used also works uniquely as instead of finding any numerical value it insists on finding a character value, like any letter or any alphanumeric value based on the hash calculation, the message length and a fixed numeric constant to make its corresponding encrypted texts more complex.

5.2 Future Scope

It can be further implemented using another set of RSA key pair by the receiver for adding the Confidentiality factor, so that the message send is kept undetected or harmless by any intruder.

Furthermore, it can be compared with pre-existing Digital Signatures Algorithms to further make it more useable and reduce its limitations hence found.

6.

Conclusion

DSA is a well-equipped algorithm for Authentication and Integrity of the message and Sender but it lacks some of the main features like Confidentiality. Authenticity is confirmed by the Public Key of the sender and Integrity by the matching Hash value of the message.

Further work can be implemented by using another Receiver side RSA encoding to achieve Confidentiality of the token message from intruders.

7.

REFERENCES

1. Yuan Zhou (2003) ‘An efficient digital signature using self-certified public keys.’ In proceedings of the 1st ACM conference on Computer and Communications.

2. Surrender Kumar (2021) ‘A Review of Digital signature and hash function-based approach for secure routing in VANET’ proceedings of the International Conference on Artificial Intelligence and Smart Systems.

3. Shin Scho (2010) ‘Alternative Proposal of Tracking Products Using Digital Signatures and QR Codes’ International Conference on Challenges in Environmental Science and Computer Engineering.

4. E.Madhusudhana Reddy K.Suresh Kumar Reddy M.Padmavathamma Professor(2019),’ An E-Commerce Security Solution using MJ2–RSA Digital Signature’ , 16 International Conference on Electrical Engineering Electronics, Computer .

5. Thanayut Seetongchuen, Paruj (2019) ‘An Improved RSA Signature Algorithm based on Complex Numeric Operation Function’ 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

6. Yasin Genç (2010),’ Design and Implementation of an Efficient Elliptic Curve Digital Signature Algorithm (ECDSA) International Conference on Challenges in Environmental Science and Computer Engineering.

7. Avinash Pandey, Dhruv Mahajan, Shivank Gupta and Vishal Rastogi (2021), ‘Detection of Blind Signature Using Recursive Sum’ 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

8. Shahzad Alam, Amir Jamil, Shahzad Alam, Amir Jamil (2015), ‘Digital Image Authentication and Encryption using Digital Signature’, 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India.

9. Rizky Damara Ardy (2017), ‘Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)’, 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems Yogyakarta, Indonesia.

10. Shin Chy (2010),’ Implementation of Digital Signature Using AES and RSA

Algorithms as a Security in Disposition System of Letter', 1st Annual Applied Science and Engineering Conference.

11. Farah Jihan Aufa, Endroyono, Achmad Affandi (2018), 'Security System Analysis in Combination Method: RSA Encryption and Digital Signature Algorithm', 2018 4th International Conference on Science and Technology (ICST), Yogyakarta, Indonesia.

12. Mr. Shaik Johny Basha, Mr. Venkata Srinivasu Veesam, Ms. Tamminina Ammannamma, Ms. Sirisha Navudu, Mr. M.V.V.S. Subrahmanyam (2020), 'Security Enhancement of Digital Signatures for Blockchain using EdDSA Algorithm', Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks.

13. Anika Tabassum, Humayra Anjumee Jeba, S. M. Salim Reza and Dilshad Ara Hossain (2021), 'Securely Transfer Information with RSA and Digital Signature by using the concept of Fog Computing and Blockchain', 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), Dhaka

14. Yucheng Li and Cong Pu (2020), 'Lightweight Digital Signature Solution to Defend Micro Aerial Vehicles Against Man-In-The-Middle Attack', 2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE).

15. Teng Yang, Yanshuo Zhang, Song Xiao, Yimin Zhao, Xidian (2021), 'Digital Signature Based on ISRSAC', Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks.

16. K.Govindaa, Dr.E.Sathiyamoorthyb (2012), 'Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud

17. Anirban Sengupta (2019), 'Embedding Digital Signature Using Encrypted-Hashing for Protection of DSP Cores in CE', IEEE TRANSACTIONS ON CONSUMER ELECTRONICS