

## SIES (Nerul) College of Arts, Science and Commerce

**NAAC Re-Accredited ‘A’ Grade**

**Sri Chandrasekarendra Saraswathy Vidyapuram, Plot 1-C, Sector V, Nerul, Navi Mumbai-400 706.**

## PROJECT REPORT ON

***Cryptography***

***(hashing,digital signature & checksum)***

# Submitted By:

**Darren Dsouza**

**(ROLL NO:02)**

**[ MSc Computer Science Part-1 (SEM-1) ] 2022-2023**

## Subject: Software Defined Networking

## Project Guide : Prof. Flosia Simon



What is Cryptography?

-Cryptography is technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it.

-Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.

What is Hashing?

-Hashing is the process of transforming any given key or a string of characters into another value**.**

What is Digital signature?

- A digital signature is an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents.

What is checksum ?

-A checksum is a value that represents the number of bits in a transmission message and is used by IT professionals to detect high-level errors within data transmissions.

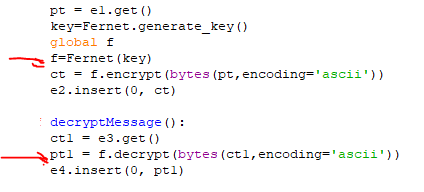
-It is also used in cryptography check data has not been altered.

Types of Hashing**:**

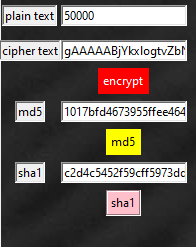
Symmetric encryption:

****

-In this project demonstration,I have first implemented symmetric encryption using fernet encryption which uses a single key for encryption of data.below is an image showing the use of a single key.



MD5 & SHA1:

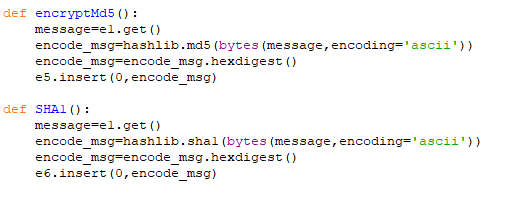
****

One of the prominently used encryption methods:MD5 & SHA1

The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function producing a 128-bit hash value.The above image shows the output in hexadecimal notation.

SHA1 takes an input and produces a 160-bit (20-byte) hash value known as a message digest

Below is the code for the function:

****

Digital Signature using rsa algorithm:



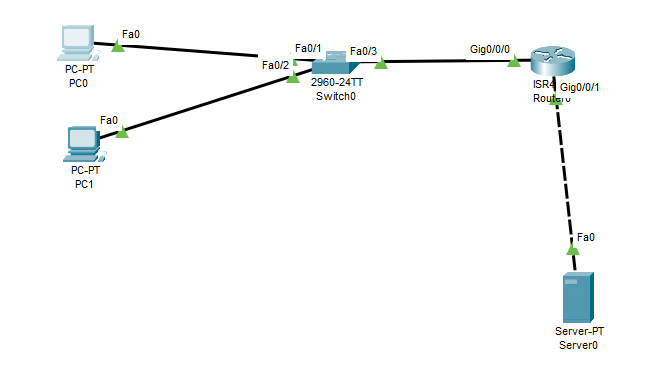
The Rsa algorithm is used to demonstrate asymmetric key encryption. We use crypto.publickey module to have a pair of public and private keys.

below are the images to show how the messages are encrypted and decrypted:



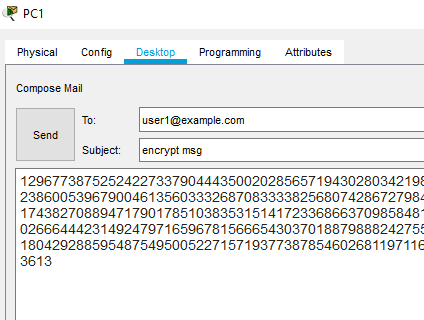
****

SMTP for message passing:

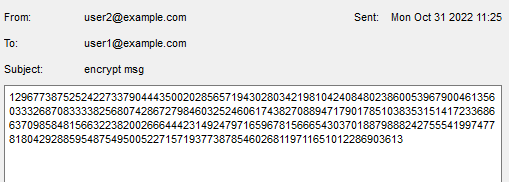


The above network is created in cisco where we use an smtp server to exchange the digital signature between two hosts and show the encryption and decryption using the keys.

sending message from user2:



Message received to user1:

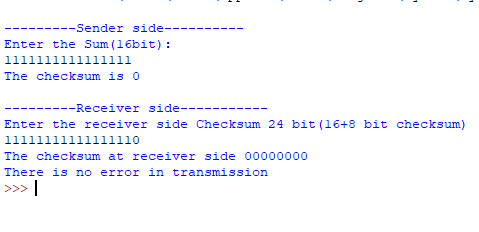


The signature received is decrypted using the public key and the message is correct:

****

*\*hashing,digital signature together helps in maintaining the CIA(confidentiality,Integrity and authenticity of the Messages being shared\**

Checksum:



The checksum is implemented in python which verifies the correctness of packet being exchanged between sender and receiver.the message received is correct only if the checksum at receiver is 0.

below image shows an example of error in transmission

