Project Team Members :

Awanit Ranjan (181CO161) awanitranjan.181me214@nitk.edu.in
Rutwik Mulay (181CO144) rutwik.181co144@nitk.edu.in
Kshitij Raj (181CO129) kshiteejraj.181co129@nitk.edu.in

Design and Implementation of securing data using Cryptography and Steganography

ABSTRACT : The establishment of a secure channel between two imparting parties is turning into a troublesome issue because of the probability of attacks and other unintentional changes during a functioning correspondence over an insecure network. Nonetheless, the security of secret information can be made sure by utilizing either cryptography or steganography. Former deals with changing over a plaintext (message) into an incoherent configuration, while latter transferring a message in a way that it will make not make any sense to any other individual aside from the expected beneficiary. Thus, the point of this work is to design and build-up models by hiding a piece of secret information by embedding that into an image or audio or video more likely image in our case, by exploiting advantages of using cryptography and steganography.

PROPOSED WORK / METHODOLOGY : First, we take the original data and encrypt it into ciphertext by utilizing the proposed symmetric cryptography method in which we will break the 128 bits into 4 equal groups of 32 bit each this 32-bit block will be undergone some circular shift and xor operations with secret keys . (These ideas are inspired by [1] and [2]). After this, the encrypted data will be embedded in a Cover Image by use of proposed steganography strategy which is utilizing least significant bit (LSB) [In this we are thinking of going with a mixture of LSB-1, LSB-2, LSB-3 (i.e storing at first, second, and a third bit from the least significant side) alternatingly.] to finally create a new image which is a stego content this is sent over the channel and at receiver side the same process will occur but in reverse, starting from extracting encrypted content from stego and finally decrypting using proposed decryption algorithm again inspired by [1] and [2]. Although ideas are inspired, we will use our own proposed architecture for encryption and decryption finally converting into an application for sending data over insecure channels.

PROJECT DELIVERABLE : A Python based application with use of flask a microservice based framework to demonstrate the combination of cryptography that is based on symmetric key and steganography that is based on modified LSB which helps to provide security to confidential data over an unsecured network.

REFERENCES

[1] Marwa E. Saleh Abdel Magied A. Aly Fatma A. Omara. CSE from Minia University, *Data Security Using Cryptography and Steganography Techniques*. International Journal of Advanced Computer Science and applications, 2016.

[2] Ms. Hemlata Sharma, Ms. MithleshArya, and Mr. Dinesh Goyal. Department of CSE *Secure Image Hiding Algorithm using Cryptography and Steganography. 2013.*