**ABSTRACT**

Cryptography is the science of using mathematics to encrypt and decrypt information. Encryption is the process in which data (plaintext) is translated into something that appears to be random and meaningless ciphertext to store on insecure media or can also be transmitted on an insecure network (like the Internet) and it cannot be read by anyone except the intended recipient. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key (a number, word, or phrase) to encrypt and decrypt data. To encrypt, the algorithm mathematically combines the information to be protected with a supplied key. The result of this combination is the encrypted data. Data Encryption Standard (DES) key algorithm can be used to encrypt the data. Decryption is the process in which the ciphertext is converted back to plain text. To decrypt, the algorithm performs a calculation combining the encrypted data with a supplied key. The result of this combination is the decrypted data. If either the key or the data is modified, the algorithm produces a different result. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. Ron rivest, Adishamir, and Leonard adleman (RSA) algorithm that involves Key generation, encryption and decryption steps can also be applied in this project. The main encryption algorithms that will be used in the project are DES, Triple Data Encryption Standard Algorithm (3DES), Advanced Encryption Standard (AES). These algorithms are studied in detailed by establishing a VPN IPsec site to site configuration on Cisco Packet Tracer. Confidentiality, authentication, integrity, access control and availability of the data will be maintained using these techniques and algorithms.

ANIRUDH NAGULAPALLI