**Study of Encryption algorithms and implementation using IPsec tunneling**

**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.

**Keywords:**

DES, 3DES, AES, Encryption, Decryption

**Introduction:**

The ultimate goal of a successful encryption algorithm is to provide the network, security from unauthorised access. The actual meaning of Cryptography comes from ‘kryptos’ which means ‘Secret’ and ‘graphy’ which means ‘writing’. So Cryptography deals with writing messages secretly so that it promotes data integrity. This can be done through various ways like setting up a firewall, using various encryption protocols. Cryptography consists of a collection of techniques put together to ensure authentication, confidentiality and access control.

The goals of Cryptography are:

1. Confidentiality
2. Authentication
3. Integrity
4. Non repudiation
5. Access control

The main concept of Cryptography consists of two parts. Encryption and Decryption. During Encryption, a readable plain text is converted into an unreadable Cipher text using a ‘key’. This ‘key’ is called as ‘Cipher’. The number of bits of the Cipher depends upon the type of algorithm used. The Cipher text doesn’t have a syntax or format. It is simply a set of random integers and alphabets combined together. During the Decryption process, the same ‘key’ is used and the Cipher text is converted to the original plain text as it is. Hence, here the ‘key’ is the secret to both encryption and decryption process.

**MD5 Algorithm**

The MD5 algorithm stands for Message Digest algorithm 5. This was invented by Ronald Rivest in 1991. There are two types of hashing in MD5 algorithm. The type 5 and type 7 are those two types. The idea behind the type 7 algorithm is providing the plain text a hash function and converting it into a 128 bit MD5 hash. Also it can be easily decrypted so it’s not reliable. On the other hand type 5 hashing can be enabled using a keyword called ‘Secret’. The type 5 MD5 encryption is always a better option and can be seen below

|  |
| --- |
| Before Password Encryption |
| After Password Encryption |

**Data Encryption Standard (DES)**

The DES Algorithm or Data Encryption Standard Algorithm is initially developed by International Business Machines Corporation (IBM) and endorsed by National Bureau of Standards in 1975. The DES is a product block cipher consisting of 16 iteration (or) rounds of permutation process are cascaded. The block size is 64 bits but only 56 bits can be chosen by the user which are the key bits. The rest 8 bits are the check bits (or) parity bits. This algorithm later, was ruled out by a more encrypted standard called Advanced Encryption Standard (AES) which was better in providing security and reliability.

**Triple DES (3DES)**

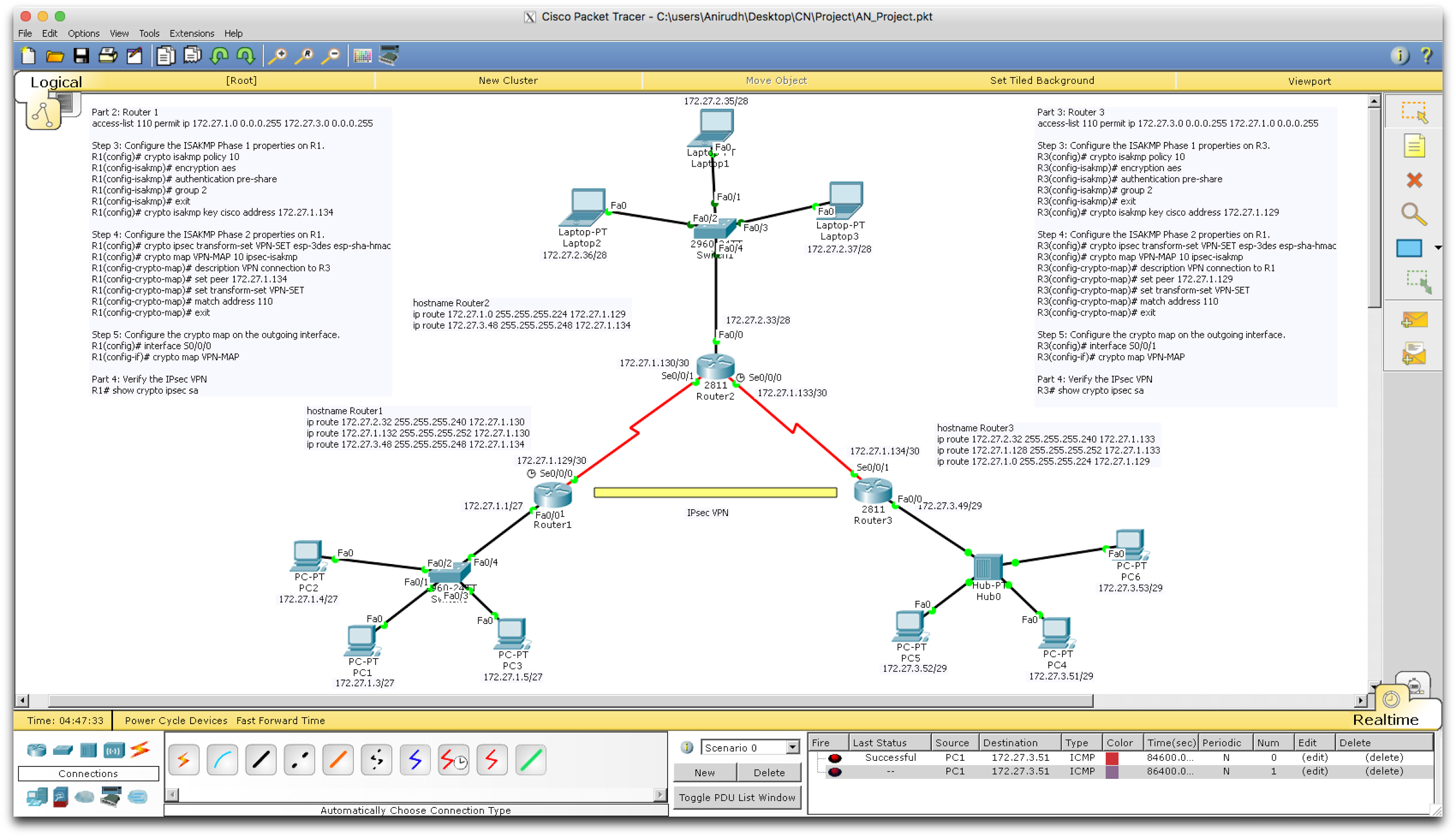
The 3DES or Triple Data Encryption Algorithm (TDEA) was developed by International Business Machines Corporation (IBM) in 1978 so as to overcome the obvious flaws from the DES. The DES initially used 56-bit key which wasn’t enough to encrypt sensitive data. The new algorithm simply extends the key count to 168 which is three times of 56. Hence it uses 3 keys K1, K2 and K3 each 64 bit long. In this encryption technique, K1 is used during encrypting the plain text, K2 is used during decrypting the cipher text and the final plain text is then encrypted again with K3. But the disadvantage faced with this model is it was slower than the DES even though it provided adequate security.

**Advanced Encryption Standard (AES)**

AES is the new encryption standard which replaced DES in 2001. The main advantage of this algorithm is that it supports any combination of data (128 bits) and any key length of 128, 192 and 256 bits. This algorithm is also referred to as AES-128, AES-192, AES-256 where the number depends on the length of the key. This algorithm goes 10 iterations for 128 bit keys, 12 iterations for 192 bit keys, 14 iterations for 256- bit keys in order to generate the Cipher text during Encryption or to retrieve the plain text during Decryption. This standard was advantageous over the remaining as it provided excellent security and fast.

The above encryption algorithms and many like these can be implemented in a Cisco Packet Tracer by setting up a IPsec VPN tunnel between two sites.

Here, the Routers 1 and 3 are in two different sites and are connected by establishing an IPsec VPN



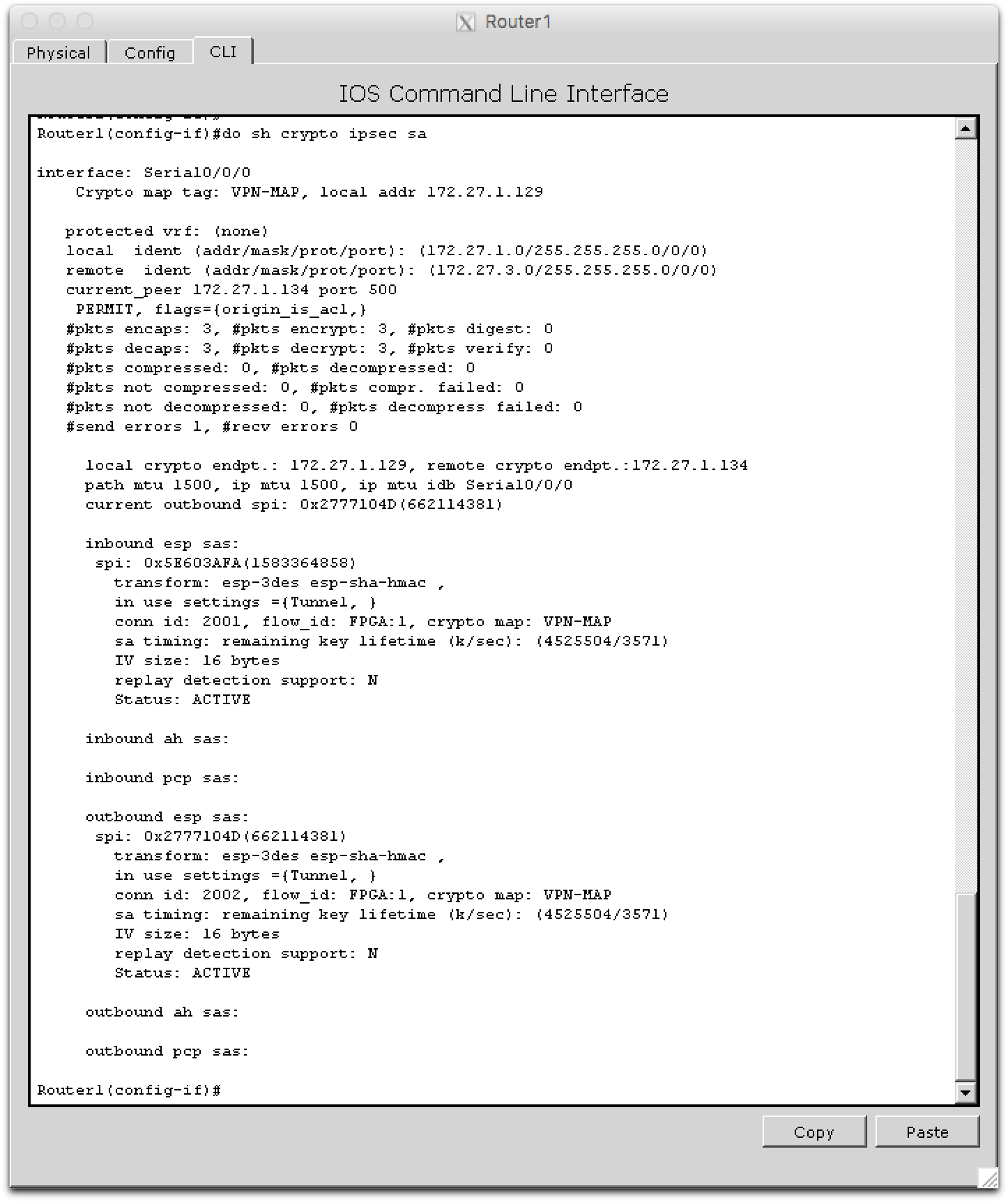
The first objective in creating a well established VPN is to set up the tunnel. This can be done by using ‘access-list 110 permit ip [source network] [destination network].

The next step is to set up the IPsec. The ISAKMP phase 1 and 2 properties are to be configured on the respective routers. The phase 1 involves creating policy and setting up 5 different properties. These are normally called as HAGLE which stand for ‘Hashing, Authentication, Group available, Lifetime, Encryption type’. After configuring the tunnel with these properties, a password has to be set which involves key [key name] [address].

The phase 2 involves configuring the hashing algorithm, which algorithm is to be used for encryption and authentication for integrity and also giving the transform-set a name.

After configuring both the routers with the required configurations, and after pinging a PC in on network to a PC in another network, a final show command ‘Show crypto ipsec sa’ shows the encryption involved, Number of packets encrypted, Number of packets decrypted, Number of packets failed, send errors, receive errors.

The output of the router will be in the form



**Conclusion and Future Scope:**

This paper presents a of the popular Encryption algorithms such as DES, 3DES, AES. As the use of internet is growing rapidly, the security threats also increase day by day. So to provide security to the network and data, different encryption methods are used. Each and every type of algorithm is unique and has its own pros and cons. A combination of algorithms can be used to secure our data effectively. At the end all the techniques are useful for encryption in one or the other field. According to a research done, AES proved to be the efficient encryption in terms of speed, time, data throughput.

**References:**

1. New Data Encryption Standard Algorithm

[Anchugam, K](http://search.proquest.com.online.library.marist.edu/indexinglinkhandler/sng/au/Anchugam,+K/$N?accountid=28549); [Tamilselvi, M](http://search.proquest.com.online.library.marist.edu/indexinglinkhandler/sng/au/Tamilselvi,+M/$N?accountid=28549). [International Journal of Computer Science and Network Security](http://search.proquest.com.online.library.marist.edu/pubidlinkhandler/sng/pubtitle/International+Journal+of+Computer+Science+and+Network+Security+$28IJCSNS$29/$N/1026368/DocView/1350974054/fulltext/ABAF634D02294D32PQ/1?accountid=28549)

1. <https://en.wikipedia.org/wiki/MD5>
2. Data Encryption Standard (DES), William L. Hosch <http://academic.eb.com.online.library.marist.edu/levels/collegiate/article/475339>
3. [A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security](http://research.ijcaonline.org/volume67/number19/pxc3887224.pdf), Gurpreet Singh; Supriya, International Journal of Computer Applications
4. <http://www.cisco.com/>