IPSec Protocols:

- IPSec is a security VPN term, which is stands for Internet Protocol Security.
- IPSec is an open standard that enables secure and encrypted communication.
- IPSec is an open standard, almost all Firewall and Router vendors support them.
- IPSec is suit of protocols that provide data confidentiality, integrity, & authentication.
- IPSec is used both for remote access VPNs and Site-to-Site Virtual Private Networks.
- IPSec is used to build VPNs over the Internet or over any other non-secure networks.
- IPSec (Internet Protocol Security) works at the Network Layer of OSI reference Model.
- In IPSec VPN, only unicast IP traffic can pass through the Virtual Privat Network tunnel.
- IPSec encrypting & authenticate Internet Protocol packets between participating devices.
- IPsec is a framework that helps us to protect Internet Protocol traffic on Network Layer.

IPSec Features:

Confidentiality:

- By encrypting data, nobody except the sender & receiver will be able to read the data.
- Encryption algorithms protect data so it cannot be read by a third party while in transit.
- It mean the data will keep as secret using encryption algorithm Like DES, 3DES, AES etc.

Integrity:

- IPSec Integrity provide to make sure that nobody changes the data in packets.
- Receiver can authenticate packets sent by sender to ensure data has not been altered.
- By calculating hash value, the sender & receiver will be able to check data is not alerted.
- IPSec integrity insure that the data has not been altered during the transmission.
- Internet Protocol Security (IPSec) Integrity using hash algorithm such as MD5 and SHA.

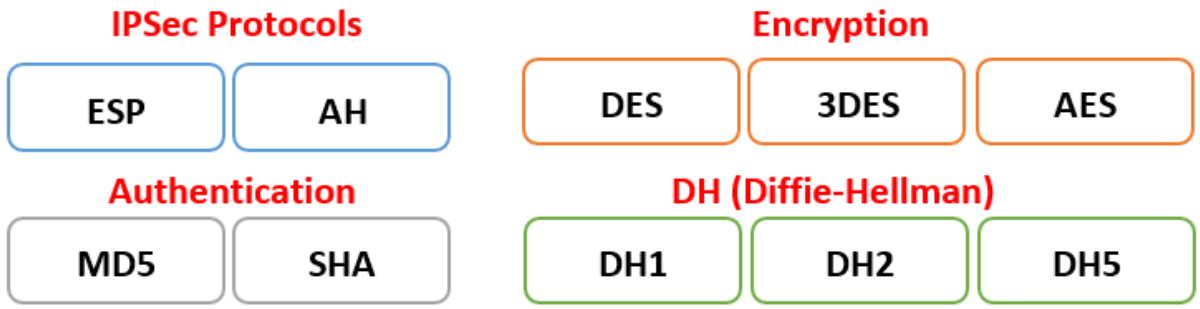
Authentication:

- Authentication means both devices will authenticate each other before data exchange.
- Authentication algorithms verify the data integrity and authenticity of a message.
- IPSec Authentication using Pre-Shared or Certificate (PKI) to authenticate peer.
- The IPSec receiver can authenticate the source of the IPSec packets sent.
- IPSec Authentication make sure that we are really talking with the device we intend to.

Anti-Replay:

- Attacker could try to capture these packets and send them again.
- Each packet is unique, has not been duplicated or intercepted.
- By using sequence numbers, IPsec will not transmit any duplicate packets.
- It means that if the data arrive late it will consider as alter & it will be drop.

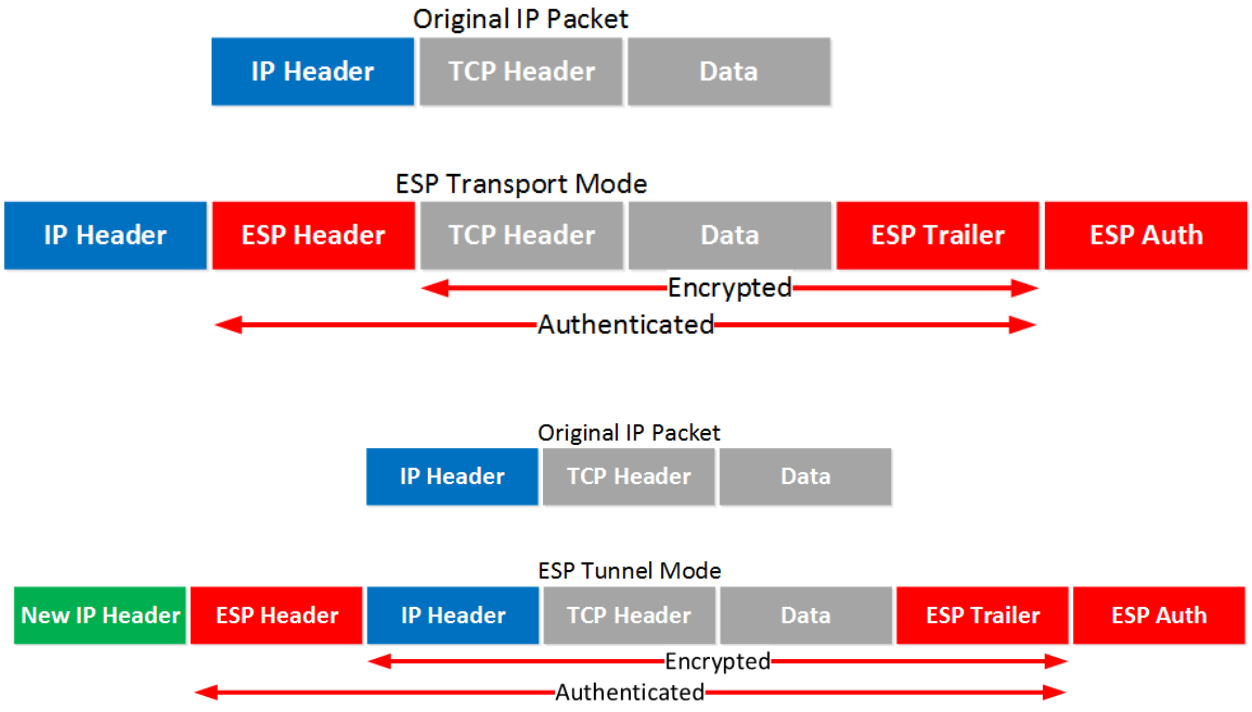
 Created by Ahmad Ali E-Mail: ahmadalimsc@gmail.com , Mobile: 056 430 3717



IPSec Protocols:

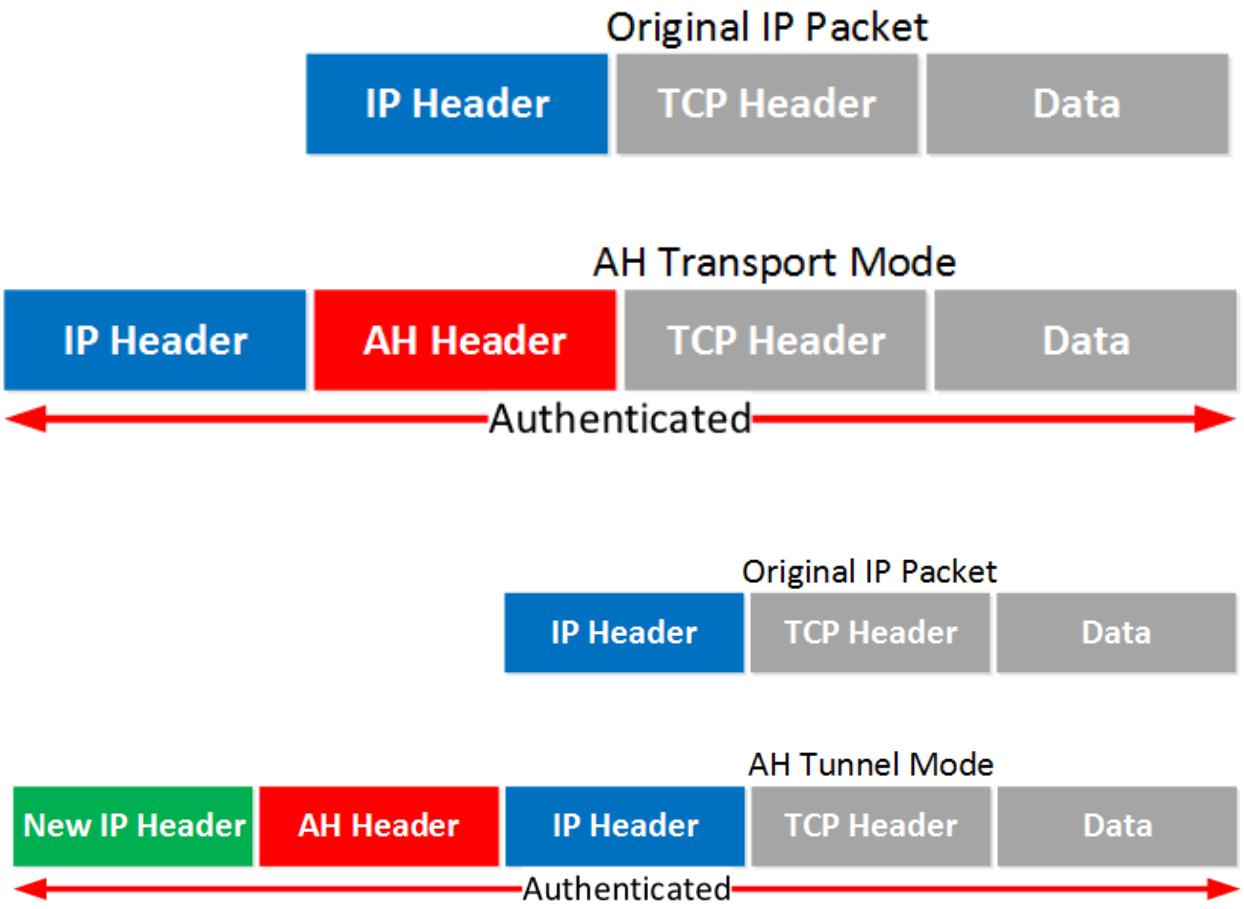
Encapsulating Security Payload (ESP):

- IPSec uses ESP to provide Data Integrity, Encryption and Authentication.
- Internet Protocol Security uses ESP to provide also Anti-Replay functions.
- IPSec implementations uses DES, 3DES and AES for Data Encryption.
- ESP authenticates the data within the VPN, ensuring Data Integrity.
- ESP (Encapsulating Security Payload) provides all IPsec features.
- ESP (Encapsulating Security Payload) use IP protocol number 50.
- ESP (Encapsulating Security Payload) work with NAT using NAT-T.
- ESP protocols support two modes of use Transport and Tunnel.
- In Transport Mode, it use the original IP header & insert an ESP header.
- In Tunnel Mode, it use a new IP header, which is useful for site-to-site VPNs.
- Same to transport mode but add new header, original header is also encrypted.



Authentication Header (AH):

- IPSec uses AH to provide Data Integrity and Authentication functions.
- IPSec uses AH to provide Anti-Replay functions for IPSec VPN.
- IPSec Authentication Header (AH) does not provide any Data Encryption.
- AH is used to provide Data Integrity services to ensure Data is not tampered.
- Authentication Header (AH) use IP protocol number 51.
- Authentication Header (AH) does not works with NAT.
- Authentication Header (AH) does not use NAT-T.
- AH, protocols also support two modes of use Transport and Tunnel.
- Transport mode is simple, it just adds an AH header after the IP header.
- With tunnel mode, it add new IP header on top of the original IP packet.

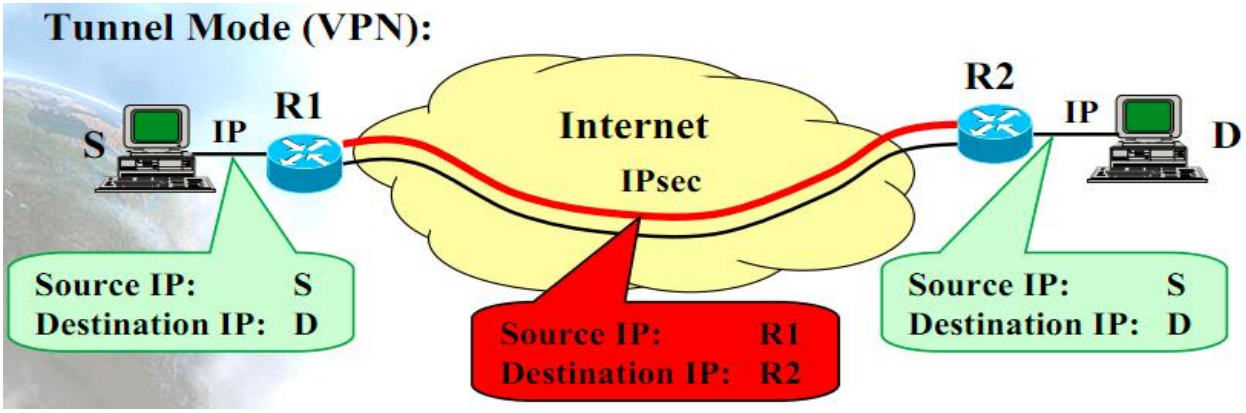


IPSec Modes:

- There is two modes of IPSec, Tunnel Mode and Transport Mode:

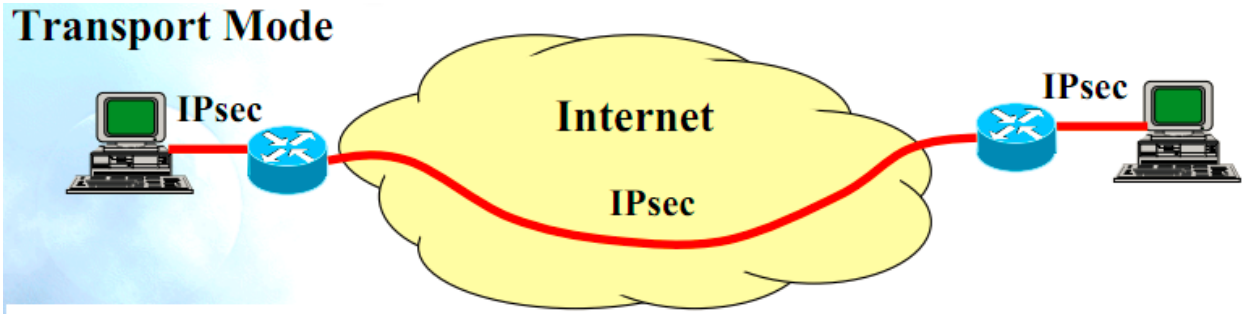
Tunnel Mode:

- In Tunnel Mode, the entire packet is encrypts and authenticates by IPSec.
- IP Security (IPSec) tunnel mode is the default mode on most Cisco devices.
- The packet is then encapsulated to form a new IP packet header information.
- IP Security (IPSec) Tunnel Mode protect Layer 3 and upper Layer data.
- IPSec Tunnel Mode is used in Site-Site VPN, Remote-Access VPN and GETVPN.
- Tunnel mode is more secure and encrypts both the header and the payload.
- Tunnel mode is used to encrypt traffic between secure IPSec Gateways.



Transport Mode:

- IPSec only encrypts and/or authenticates the actual payload of the packet.
- In Transport mode, the header information remains unchanged.
- IPSec Transport mode is used for end-to-end communications.
- IPSec Transport mode is used for communication between client & server.
- IPSec Transport mode is used for communication between a workstation.
- Normally, encrypted Telnet or RDP session from workstation to server.
- IPSec Transport mode protect Layer 4 and upper Layer data.
- IPSec Transport Mode will use the original IP header.
- IPSec transport mode is used when another tunneling protocol like GRE is used.
- IPSec Transport Mode is used in Dynamic Multipoint Virtual Private Network.



IPSec Authentication:

MD5 Hashing:

- Hashing is the technique to ensure the integrity.
- MD5, which stands for Message Digest algorithm 5.
- The Message Digest (MD5) is a cryptographic hashing algorithm.
- MD5 hash is typically expressed as a 32-digit hexadecimal number.
- MD5 or message digest algorithm will produce a 128-bit hash value.
- Input data can be of any size or length, but the output size is always fixed.
- MD5 algorithm generates a fixed size (32 Digit Hex) MD5 hash.
- The hash is unique for every file irrespective of its size and type.

SHA Hashing:

- SHA, stands for Secure Hash Algorithm, is cryptographic hashing.
- SHA used to determine the integrity of a particular piece of data.
- The Secure Hashing Algorithm comes in several flavors.
- SHA-1 and SHA-2 are two different versions of that algorithm.
- SHA1 produces a 160-bit (20-byte) hash value.
- SHA2 has option to vary digest between 224 bits to 512 bits.
- SHA224 produces a 224-bit (28-byte) hash value.
- SHA256 produces a 256-bit (32-byte) hash value.
- SHA384 produces a 384-bit (48-byte) hash value.
- SHA512 produces a 512-bit (64-byte) hash value.

IPSec Encryption:

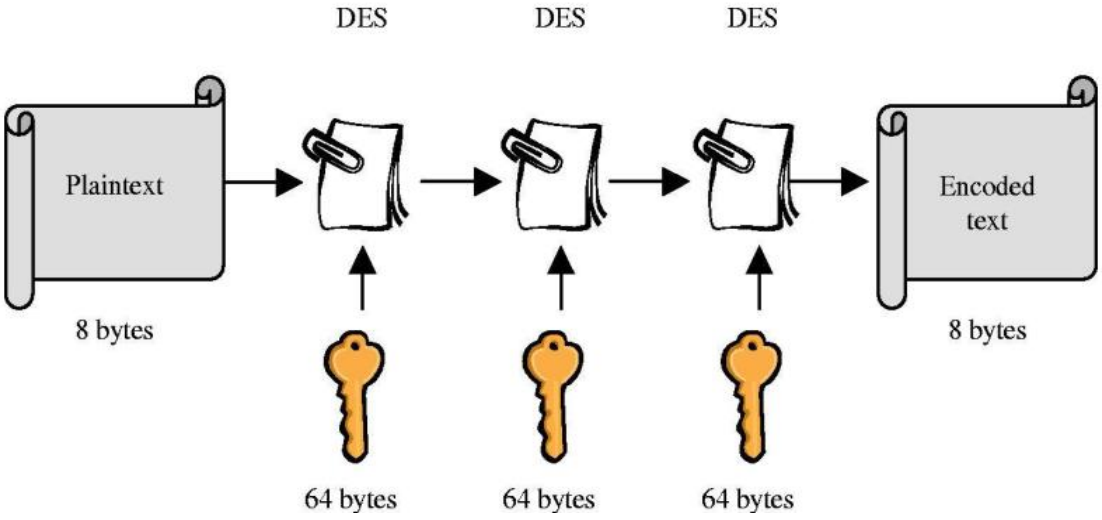
IPSec provide many Encryption methods mostly used are DES, 3DES & AES.

DES Encryption Algorithm:

- DES stands for Data Encryption Standard, its Encryption Algorithm.
- DES was developed by IBM in 1970s but was later adopted by the NIST.
- DES (Data Encryption Standard) key length is 56 bits & block size is 64-bit length.
- Data Encryption Standard uses 56-bit key, ensuring high-performance encryption.
- DES is not a secure encryption algorithm and it was cracked many times.
- DES is one of the most widely accepted, publicly available cryptographic systems.
- DES (Data Encryption Standard) is used to encrypt and decrypt packet data.
- DES turns clear text into ciphertext with an encryption algorithm.
- The decryption algorithm on the remote end restores clear text from ciphertext.
- DES shared secret keys enable the encryption and decryption on both sides.
- DES (Data Encryption Standard) is the weakest of the three algorithms.

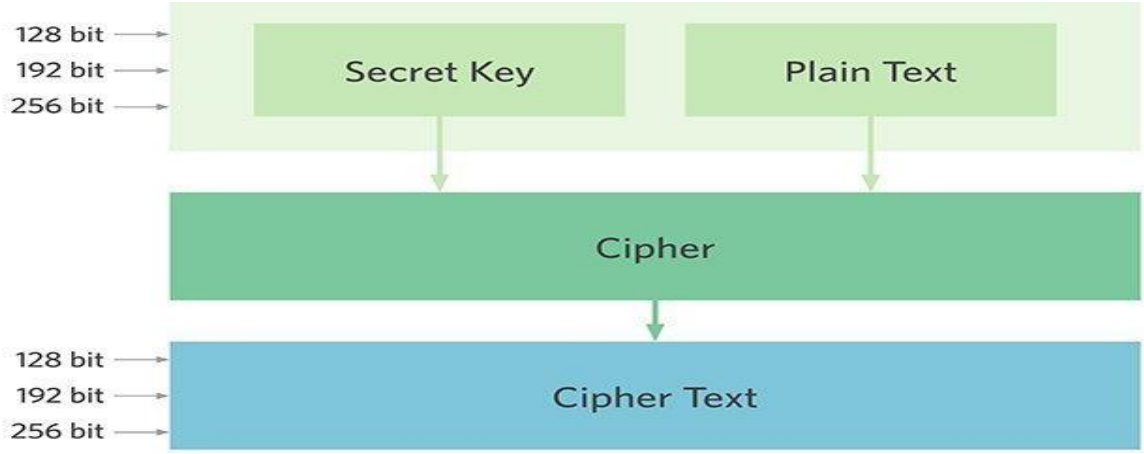
Triple DES Algorithm (3DES):

- Encryption algorithm based on DES that uses DES to encrypt the data three times.
- In 3DES, Data Encryption Standard encryption is applied three times to the plaintext.
- Plaintext is encrypted with key A, decrypted with key B & encrypted again with key C.
- Triple DES (3DES) is also supported encryption protocol for use in IPSec on Cisco products.
- Triple DES (3DES) operates similarly to DES in that data is broken into 64-bit blocks.
- 3DES then processes each block three times, each time with an independent 56-bit key.
- Triple DES effectively doubles encryption strength over 56-bit Data Encryption Standard.
- Triple DES is a variation of DES, which is secure than the usual Data Encryption Standard.



AES (Advanced Encryption Standard):

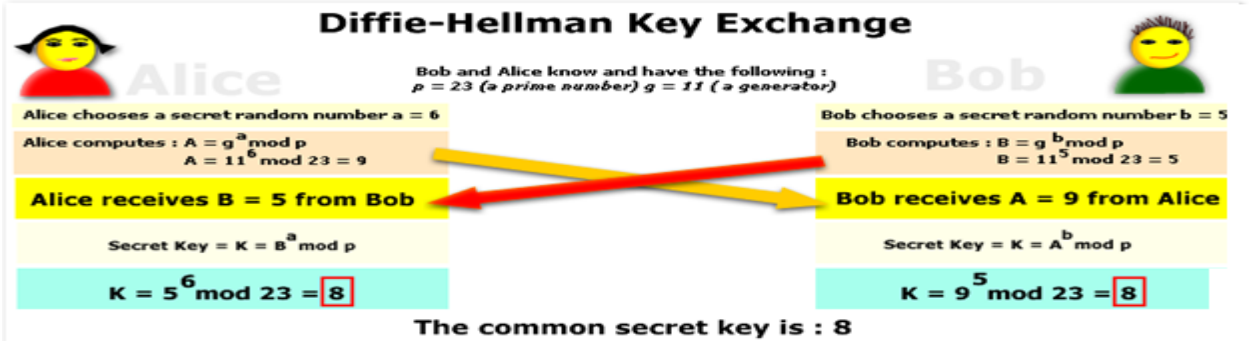
- AES (Advanced Encryption Standard) is strongest encryption algorithm available.
- Advance Encryption Standard (AES) algorithm was developed in the Year 1998.
- Advanced Encryption Standard (AES) is a newer and stronger encryption standard
- Firewalls can use AES encryption keys of these lengths: 128, 192, or 256 bits.
- Algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length.

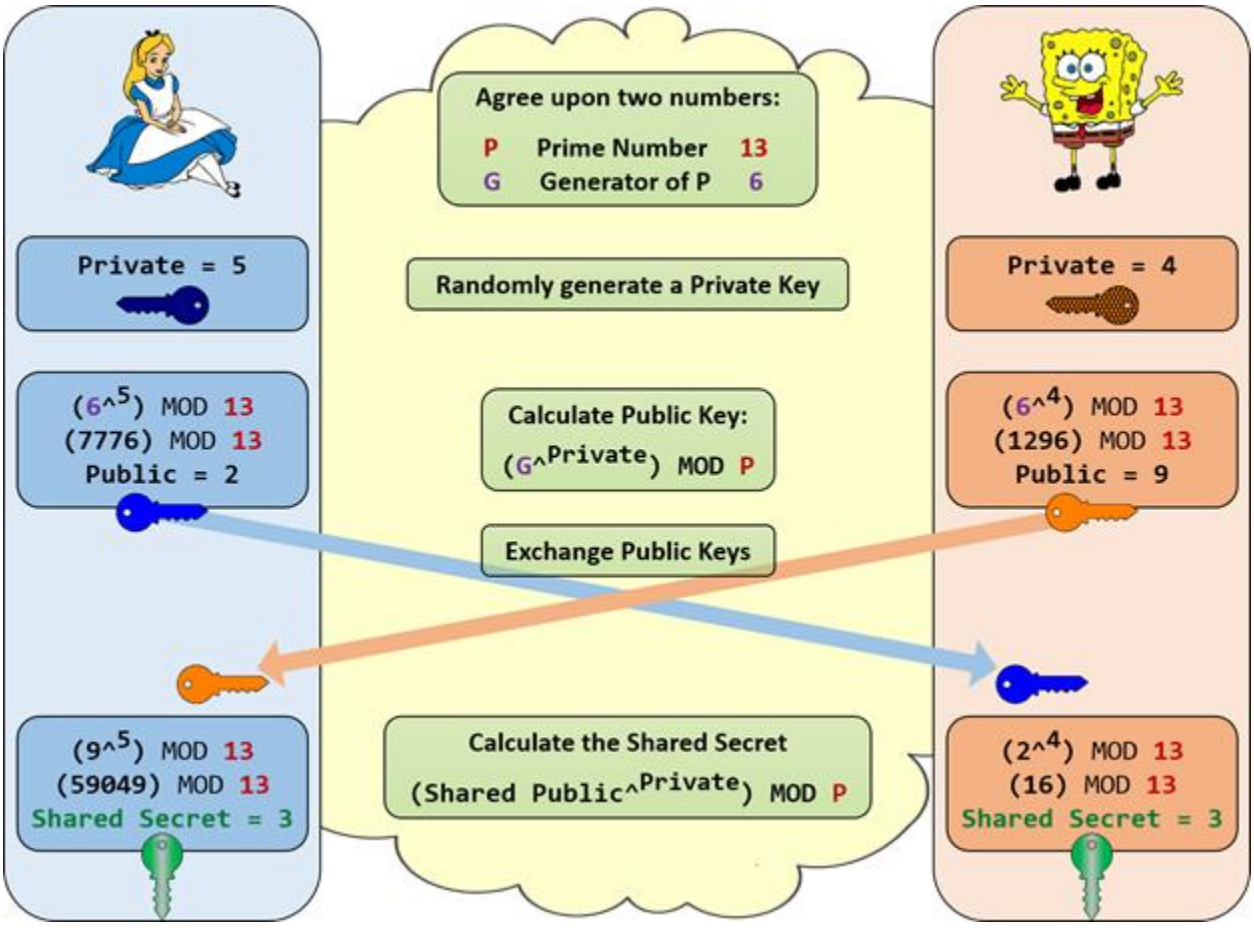


Diffie-Hellman (DH):

- Diffie-Hellman key agreement algorithm was developed in the Year 1976.
- Dr. Whitfield Diffie and Dr. Martin Hellman developed Diffie-Hellman Algorithm.
- Diffie-Hellman (DH) key exchange is a wonderful mathematical algorithm.
- Which allows two parties who have no prior knowledge to generate same secret keys.
- Diffie-Hellman allows two devices to establish a shared secret over an unsecure network.
- The encryption key for the two devices is used as a symmetric key for encrypting data.
- Diffie-Hellman key agreement algorithm is widely used in security protocols like IPSec.
- Diffie-Hellman algorithm is also use in Secure Shell (SSH) & Transport Layer Security (TLS).
- Only two parties involved in the DH key exchange and the key is never sent over the wire.
- Diffie-Hellman key group is a group of integers used for the Diffie-Hellman key exchange.
- Cisco Firewalls and Routers can use Diffie-Hellman (DH) groups 1, 2, 5, 14, 15, 19, and 20.
- Diffie-Hellman groups determine the strength of the key used in the key exchange process.
- Higher group numbers are more secure but require additional time to compute the key.
- Diffie-Hellman groups (DH) is used within IKE to establish session keys.
- 768-bit and 1024-bit D-H groups are supported in the Cisco routers and Firewall.
- The 1024-bit group is more secure because of the larger key size.
- In terms of VPN, it is used in the in IKE or Phase1 part of setting up the VPN tunnel.
- There are multiple, Diffie-Hellman Groups that can be configured in an IKEv2 policy.
- Both peers in VPN exchange must use same DH group, which is negotiated during Phase 1.
- There are multiple Diffie-Hellman Groups 1 to 30 assigned and 31-32767 Unassigned.

DH Group Number	Group Description	Recommendation
Diffie-Hellman group 1	768-bit Modulus	Avoid
Diffie-Hellman group 2	1024-bit Modulus	Avoid
Diffie-Hellman group 5	1536-bit Modulus	Avoid
Diffie-Hellman group 14	2048-bit Modulus	Acceptable
Diffie-Hellman group 15	3072-bit Modulus	Acceptable
Diffie-Hellman group 19	256-bit Elliptic Curve	Elliptic Curve Acceptable
Diffie-Hellman group 20	384-bit Elliptic Curve	Elliptic Curve NGE
Diffie-Hellman group 21	521-bit Elliptic Curve	Elliptic Curve NGE
Diffie-Hellman group 24	2048-bit Modulus	Next Generation Encryption


Diffie-Hellman Key Exchange
Alice
Bob
Bob and Alice know and have the following :
p = 23 (a prime number) g = 11 (a generator)
Alice chooses a secret random number a = 6
Alice computes : A = g^a mod p
A = 11^6 mod 23 = 9
Alice receives B = 5 from Bob
Secret Key = K = B^a mod p
K = 5^6 mod 23 = 8
Bob chooses a secret random number b = 5
Bob computes : B = g^b mod p
B = 11^5 mod 23 = 5
Bob receives A = 9 from Alice
Secret Key = K = A^b mod p
K = 9^5 mod 23 = 8
The common secret key is : 8


Agree upon two numbers:
P Prime Number 13
G Generator of P 6
Private = 5
Randomly generate a Private Key
Private = 4
(6^5) MOD 13
(7776) MOD 13
Public = 2
Calculate Public Key:
(G^Private) MOD P
(6^4) MOD 13
(1296) MOD 13
Public = 9
Exchange Public Keys
(9^5) MOD 13
(59049) MOD 13
Shared Secret = 3
Calculate the Shared Secret
(Shared Public^Private) MOD P
(2^4) MOD 13
(16) MOD 13
Shared Secret = 3