PARAS . H. DUDHATRA B00728686.

DALHOUSIE UNIVERSITY
Inspiring Minds

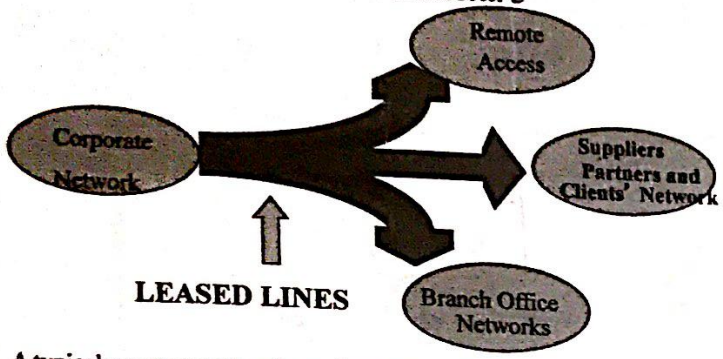
MODULE 6:
Virtual Private Networks (VPNs)

INWK 6119
Network Security
Srini Sampalli
srini@cs.dal.ca

VPN Topics

- Motivation
- Types of VPNs
- Advantages of VPNs
- Tunneling mechanism
- **IPSEC Tunneling Protocol**

Motivation for VPNs → Corporate Network Structure



A typical corporate network requires three main types of secure connections – with remote access users, with suppliers/partners/clients and with branch offices. Traditionally, this was done by leasing lines from a telephone company. The cost of leased lines is directly dependent on the distance and time of usage. Remote users incur long distance charges by dialing in.

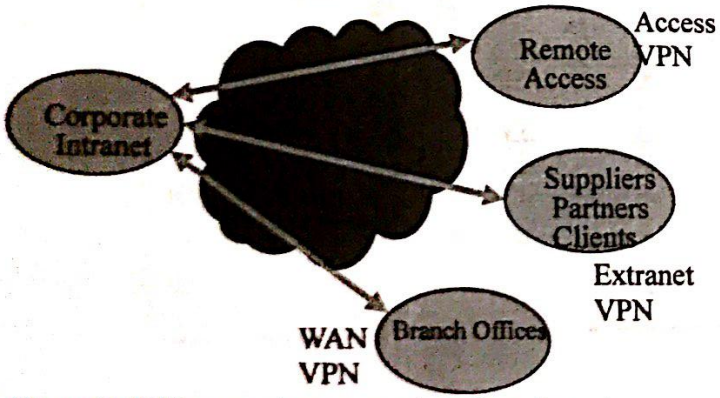
Virtual Private Network - a cost-effective alternative

- A network that enables private communications
  - ***Private Network***
- but still uses a public infrastructure (such as the Internet)
  - ***Virtual***

A **Virtual Private Network (VPN)** *connects the resources and components of one network to another over a public infrastructure (Internet), such that it appears as if the data is being sent over a dedicated link.*

(2)

VPN Types



Thus, with VPNs we can have secure channels on demand.
Three types of VPNs based on the user type:

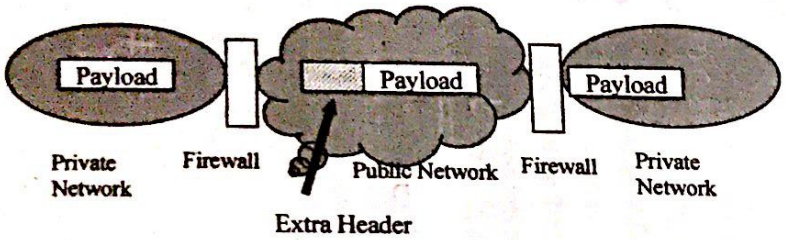
- Access VPN – connection to remote users
- Extranet VPN – connection to suppliers/partners/clients
- Wide Area Network (WAN) VPN – connection to branch offices

Why VPN's?

- ***Cost-effectiveness***: Enterprises can save 20% - 80% of networking costs as compared to leased lines.
- ***Flexibility***: Bandwidths can be utilized as per demand.
- ***Scalability***: More branch offices can be added or existing branch offices can be removed without major changes in infrastructure.

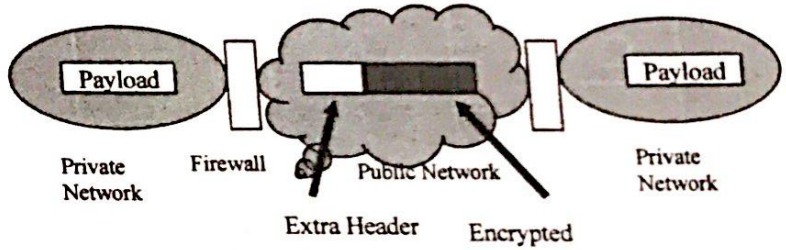
How does a VPN work?

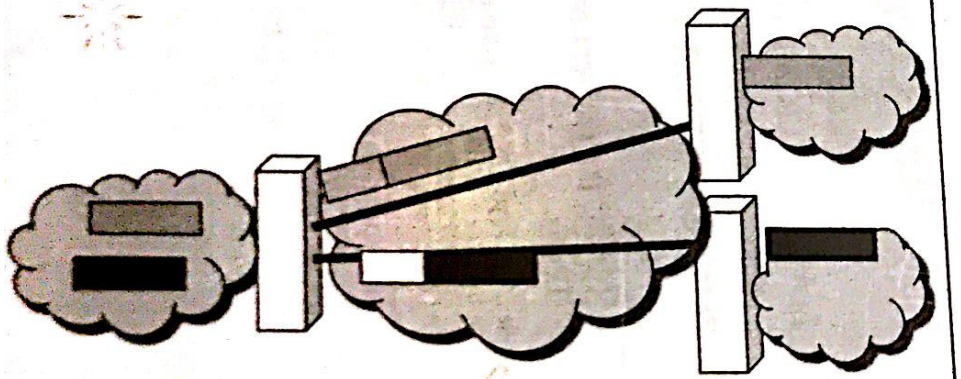
- **A VPN establishes tunnels through the Internet to send packets.**
- **What is a tunnel?**
  Just a logical stream of packets in which each packet is encapsulated with an additional header as it travels through the public network



How does a tunnel provide security?

- ***Simple; with the extra header, the rest of the payload can be encrypted; the packet can also be authenticated and certified***
- ***Firewall provides access control***
- ***Result: Confidentiality, Integrity, Authentication, Non-repudiation, Certification, Access Control, Availability***



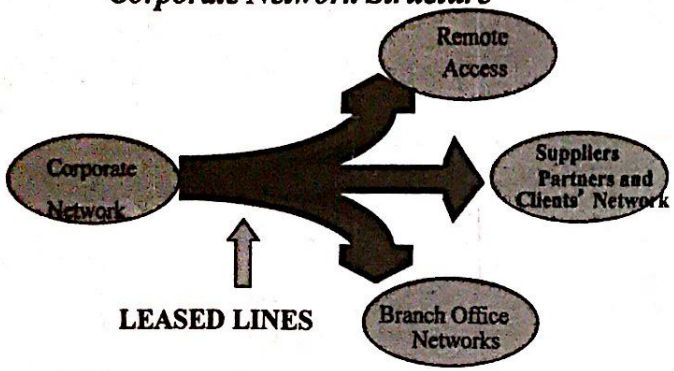


Creation of multiple tunnels

- **So, what do we need to set up a VPN tunnel?**
  A VPN Tunneling Protocol that can establish tunnels with appropriate security mechanisms.
- **What are the tunneling protocols?**
  Many are available –
  PPTP (Point to Point Tunneling Protocol)
  L2F (Layer 2 Forwarding)
  L2TP (Layer 2 Tunneling Protocol)
  The above work at Layer 2 and limited in functionality.

The most popular and the most secure is IPSec

Motivation for VPNs →
Corporate Network Structure



A typical corporate network requires three main types of secure connections – with remote access users, with suppliers/partners/clients and with branch offices.
Traditionally, this was done by leasing lines from a telephone company.
The cost of leased lines is directly dependent on the distance and time of usage.
Remote users incur long distance charges by dialing in.

(2)

Virtual Private Network - a cost-effective alternative

- A network that enables private communications

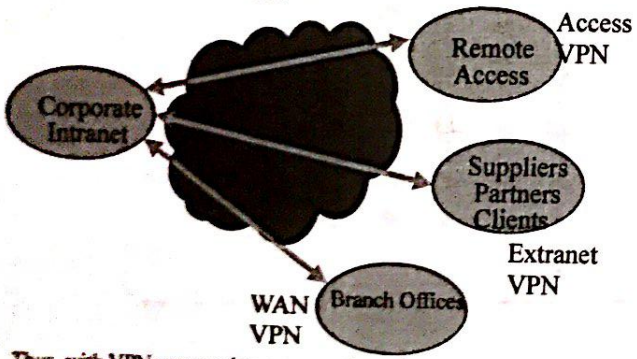
- Private Network

- but still uses a public infrastructure (such as the Internet)

- Virtual

A **Virtual Private Network (VPN)** *connects the resources and components of one network to another over a public infrastructure (Internet), such that it appears as if the data is being sent over a dedicated link.*

VPN Types



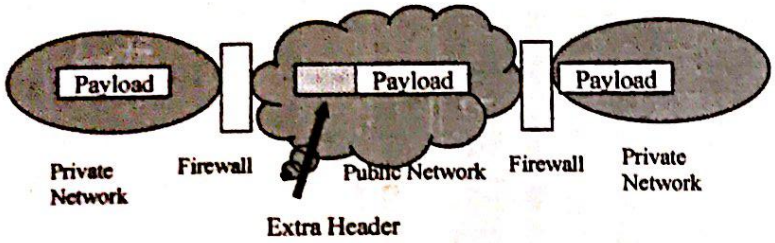
Thus, with VPNs we can have secure channels on demand.
Three types of VPNs based on the user type:
- Access VPN – connection to remote users
- Extranet VPN – connection to suppliers/partners/clients
- Wide Area Network (WAN) VPN – connection to branch offices

Why VPN's?

- ***Cost-effectiveness***: Enterprises can save 20% - 80% of networking costs as compared to leased lines.
- ***Flexibility***: Bandwidths can be utilized as per demand.
- ***Scalability***: More branch offices can be added or existing branch offices can be removed without major changes in infrastructure.

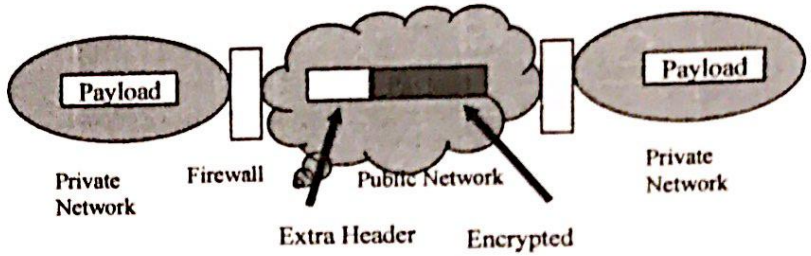
How does a VPN work?

- **A VPN establishes tunnels through the Internet to send packets.**
- **What is a tunnel?**
  Just a logical stream of packets in which each packet is encapsulated with an additional header as it travels through the public network

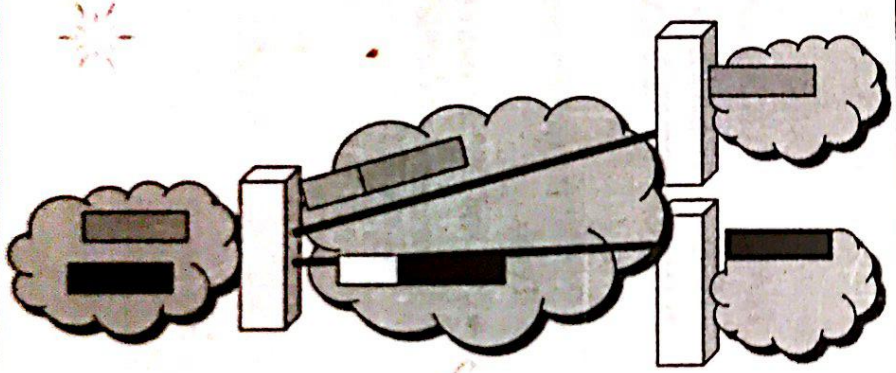


How does a tunnel provide security?

- ***Simple; with the extra header, the rest of the payload can be encrypted; the packet can also be authenticated and certified***
- ***Firewall provides access control***
- ***Result: Confidentiality, Integrity, Authentication, Non-repudiation, Certification, Access Control, Availability***



(3)



Creation of multiple tunnels

- **So, what do we need to set up a VPN tunnel?**
  A VPN Tunneling Protocol that can establish tunnels with appropriate security mechanisms.
- **What are the tunneling protocols?**
  Many are available –
  PPTP (Point to Point Tunneling Protocol)
  L2F (Layer 2 Forwarding)
  L2TP (Layer 2 Tunneling Protocol)
  The above work at Layer 2 and limited in functionality.

The most popular and the most secure is IPSec

IPSEC Tunneling Protocol

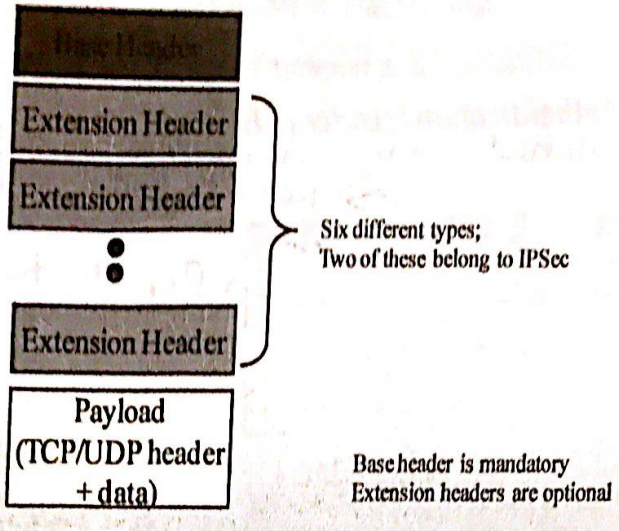
- IPSEC or IP Security is IETF's proposal and is touted as the best security solution for building VPN's.
- It is a network layer tunneling protocol for IP.
- Provides per-packet, end-to-end or segment-by-segment protection.
- Accommodates a wide variety of cryptographic algorithms for confidentiality, integrity and authentication.
- High flexibility- allows nesting or bundling of its component protocols
- Efficient key management and exchange procedure

IPSEC Components

1) AUTHENTICATION HEADER (AH)
2) ENCAPSULATING SECURITY PAYLOAD (ESP)
3) INTERNET KEY EXCHANGE (IKE)

- IPSEC is a resident protocol of IP version 6 (comes with IPv6).
- AH and ESP are two of the six different extension headers that are defined for the IPv6 datagram.

What does an IPv6 packet look like?



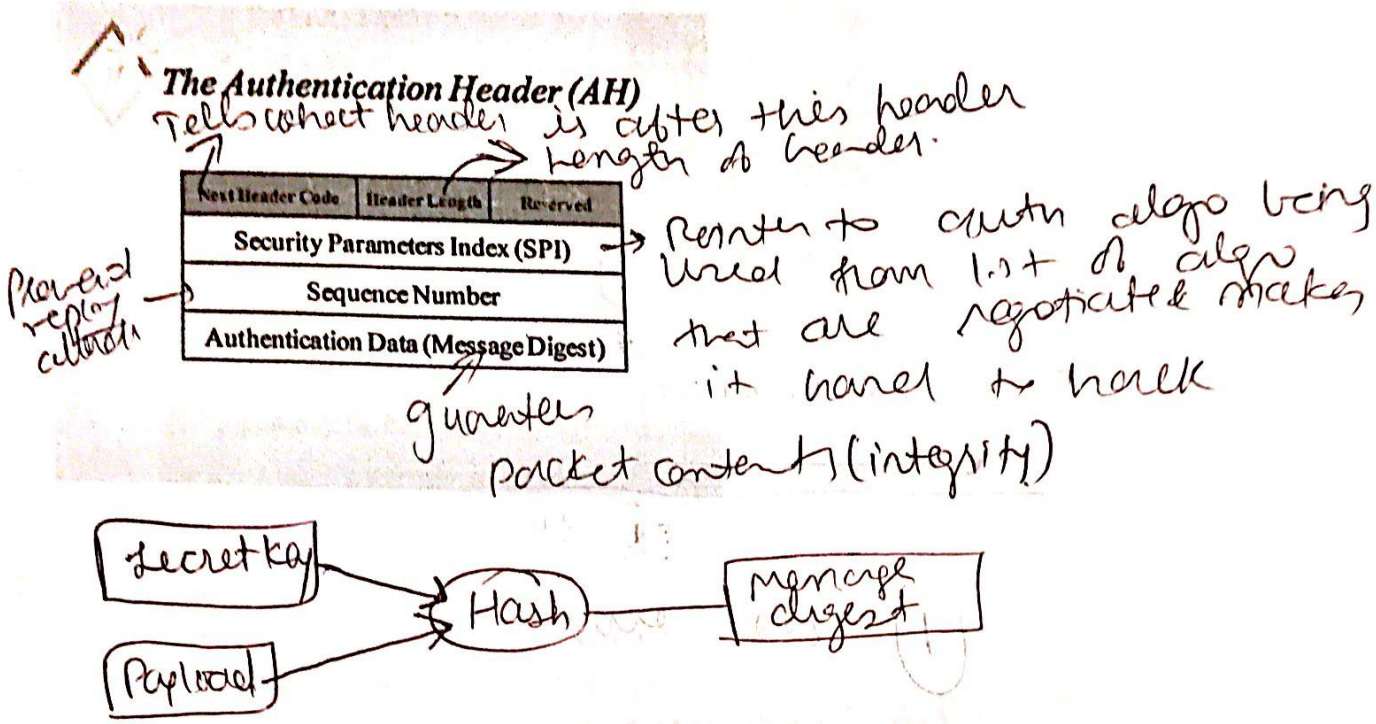
IPv6 Extension Headers

- **Authentication Header (AH)**
- **Encapsulating Security Payload (ESP)**
- Hop by Hop Option Extension Header
- Source Routing Extension Header
- Fragmentation Extension Header
- Destination Option Extension Header

- ***Note: Although AH and ESP are defined for IPv6, they can also be used with IPv4 datagrams. So IPSEC can be deployed on IPv4 and IPv6 networks.***

AUTHENTICATION HEADER (AH)

- Provides integrity and authentication
- Contains a message digest for the contents of the packet
- No encryption is provided by AH



AH MODES

Original packets : | IP Header | Payload |

Transport mode → | original IP header | AH | Payload |

Tunnel mode → | New IP header | AH | original IP Header | Payload |

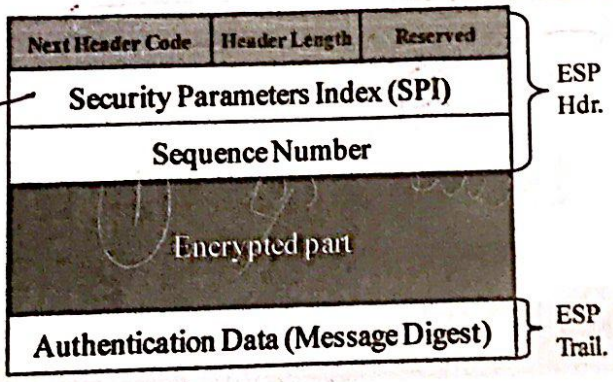
Source & dest = start & end point of tunnel.

ENCAPSULATING SECURITY PAYLOAD (ESP)

- Provides confidentiality, integrity and authentication
- Encryption algorithms: DES, 3DES, RC5, IDEA, CAST128
- Authentication algorithms: HMAC-MD5, HMAC-SHA
- ESP can be used in two modes: Transport and Tunnel

ESP Format

The Encapsulating Security Payload (ESP) Header



Pointer to encryption & authentication algorithms

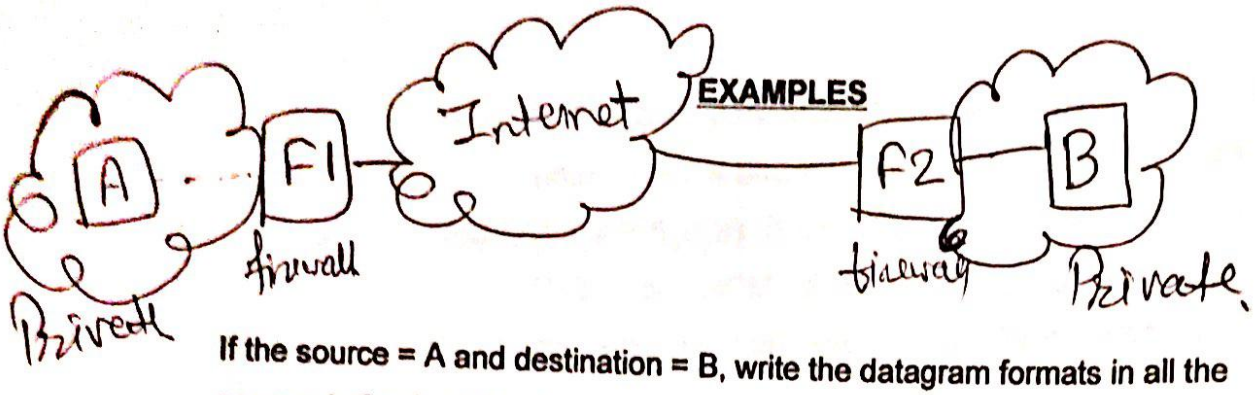
e: encrypted
a: authenticated.

ESP MODES

Original Datagram | original IP Header | Payload.

Transport mode :- | original IP Header | ESP header | Payload | ESP Trailer |

Tunnel mode :- | New IP header | ESP header | original IP encrypted | Payload | ESP trailer |



If the source = A and destination = B, write the datagram formats in all the segments for the following two cases.

a) AH Transport between A and B, ESP Tunnel between F1 and F2

① Original Datagram :- | A, B | Payload |

② A to F1 :- | A,B | AH | Payload |

③ F1 to F2 :- | F1, F2 | ESP-H | A,B | AH | Payload | ESP-T |

④ F2-B same as ②

⑤ A to B → same as ①

b) AH Transport from A to F1, ESP Tunnel from F1 to F2, AH Tunnel from F2 to B

① original Datagram :- | A,B | Payload |

② A-F1 :- | A,B | AH | Payload |

③ F1-F2 :- | F1-F2 | ESP Header | A,B | Payload | ESP Trailer |

④ F2-B :- | F2-B | AH | A,B | Payload |

⑤ At-B :- same as ① (8)

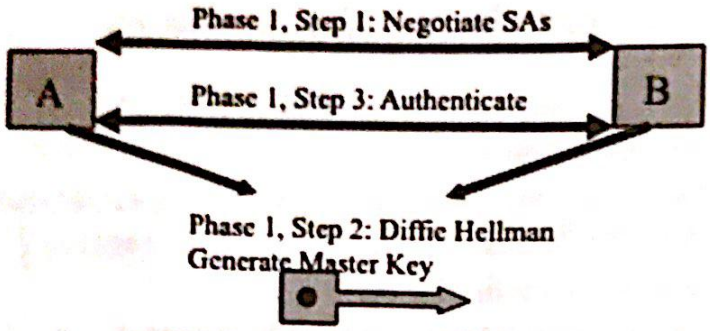
Internet Key Exchange (IKE)

- **Secure exchange of keys is critical to the security of a tunneling protocol.**
- **IPSEC has a highly secure and elaborate key exchange protocol called IKE (Internet Key Exchange).**
- **IKE has two main phases:**
  - **Phase 1: Establishment of a Security Association**
  - **Phase 2: Secure exchange of messages**
- **What is a security association (SA)?**
  - **A security association (SA) between the two tunnel peers defines the encryption and authentication algorithms, the key lengths and their lifetimes.**
  - **SA proposals are negotiated in Phase 1.**

Security Association (SA)

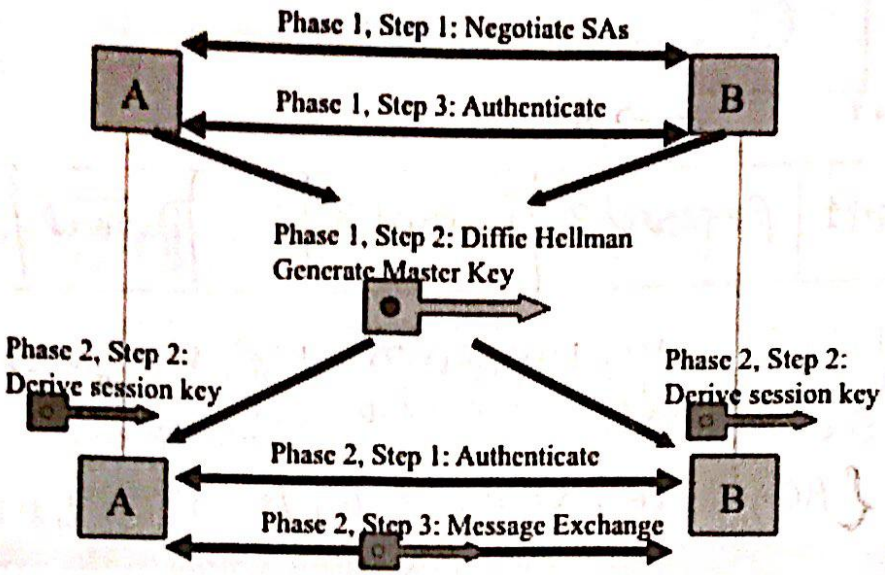
- **The concept of a security association (SA) is central to IKE.**
- **An SA between two tunnel peers defines the following:**
  - **The encryption algorithm and its key length**
  - **The authentication algorithm and its key length**
  - **The lifetime of the keys**
  - **The lifetime of the SA itself**
- **SA proposals are negotiated between the peers in Phase I.**

IKE Overview – Phase I



- PHASE I (6 messages)
  - Security Association (SA) messages are sent and negotiated in messages 1 and 2
  - Diffie Hellman exchanges are done in 3 and 4. A master key SKEYID is established
  - Digital signatures and certificates are exchanged in messages 5 and 6. They are encrypted using SKEYID. The two nodes authenticate each other.

IKE Overview – Phase II



- PHASE II (3 messages)
  - Using encrypted packets and protected by Digital Signatures, they do another Diffie Hellman exchange
  - This generates the secret session key
  - Data is transferred using the secret session key
  - *Keys are refreshed every few minutes in Phase II.*

Note: Data is transferred using a private key encryption algorithm using the secret key generated in Phase II.

IKE DETAILS

PHASE 1, MESSAGES 1 and 2 (Negotiate SAs)

Message 1 $A \rightarrow B$

Proposal 1	Proposal 2	Proposal 3	---	Proposal n	Cookie A

Example

Proposal 1 $\Rightarrow$ {3DES, 112, HMACMD5, 128, 5 mins, 24 hrs}

(3DES: Enc. algo; 112: Key length; HMACMD5: auth. algo; 128: Key length; 5 mins: Key lifetime; 24 hrs: Session lifetime.)

Proposal 2 = {AES, 256, SHA, 256, 10 mins, 48 hrs}

Cookie = Hash(secret of A, IP of A, Timestamp).

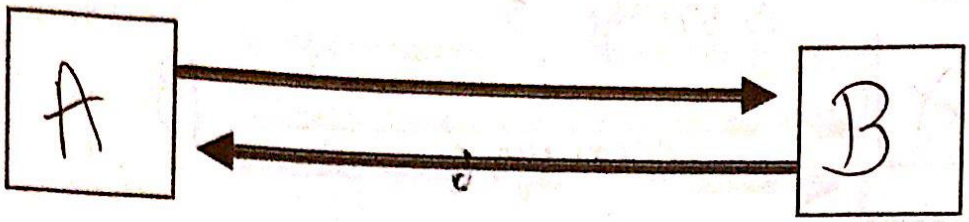
Message 2 $B \rightarrow A$

Proposal 1	Proposal 3	Proposal 6	Cookie A	Cookie B.

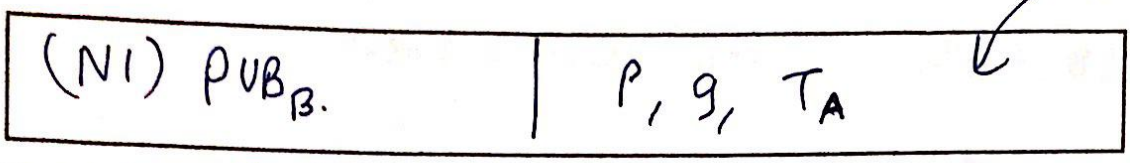
Accepted Proposals.

CookieB = Hash(Secret of B, IP of B, Timestamp).

PHASE 1, MESSAGES 3 and 4 (Protected Diffie Hellman exchange)

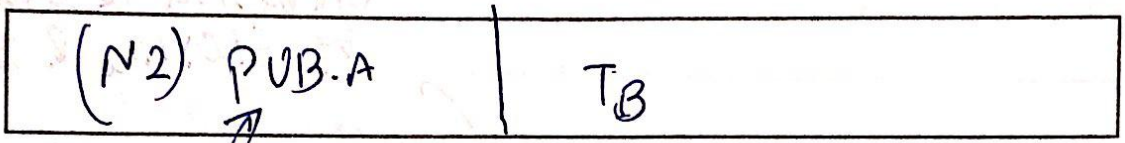


Message 3.



N1 = Encrypted Random number by public key of B.

Message 4



Random number encrypted by Public key of A.

After this exchange, A & B derive a secret number, S from DH.

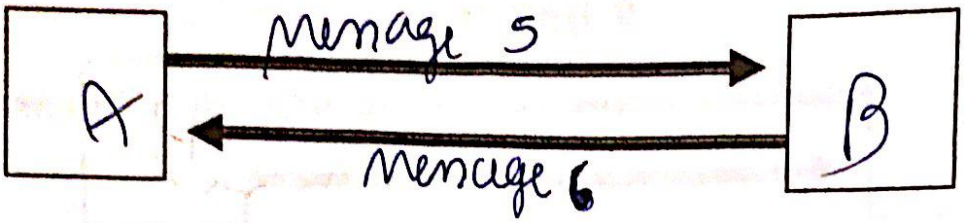
Master key → SKEY ID = Hash (N1, N2, S).
→ from SKEYID 3 keys are derived.

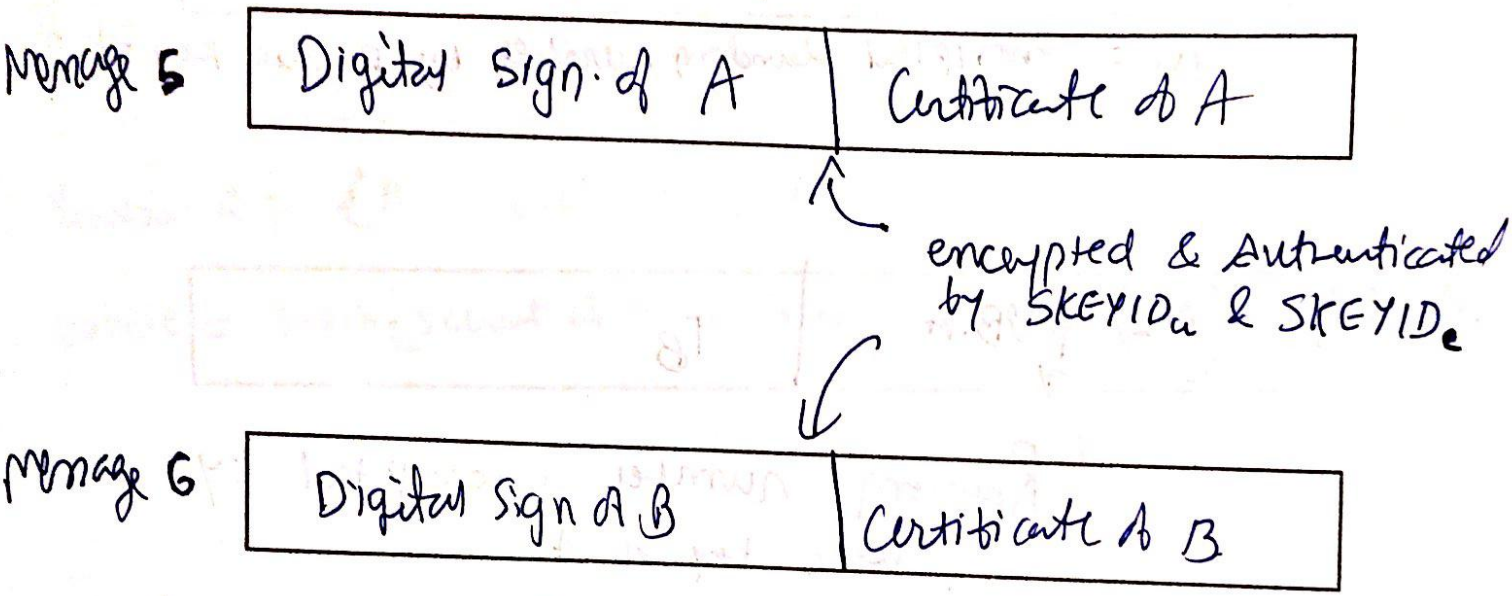
① SKEYIDd = Hash (SKEYID, CookieA, CookieB).
→ for deriving ② & ③

② $SKEYID_e$ = Hash (SKEYID, SKEYID, CookieA, CookieB).
→ for encrypting further IKE messages.

③ $SKEYID_a$ = Hash ($SKEYID_e$, SKEYID, CookieA, CookieB).
→ for authenticating further IKE messages.

PHASE 1, MESSAGES 5 and 6 (Mutual authentication)

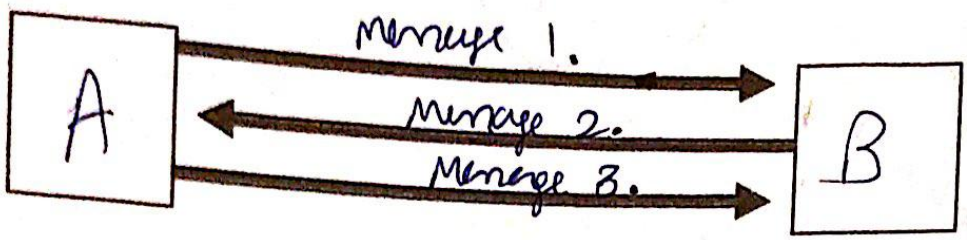




After phase I, 3 things happened

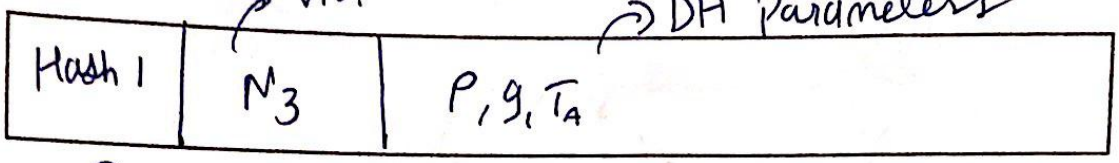
1. negotiation
2. Diffe Hellman exchange
3. Authentication

PHASE II (3 MESSAGES)



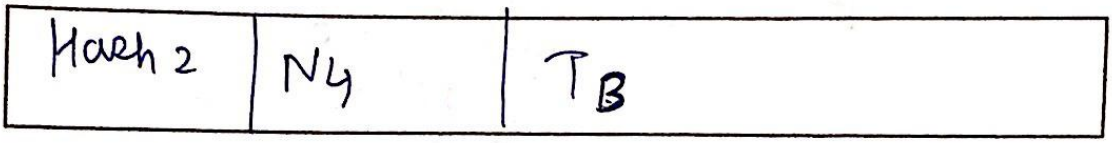
Hash 1 = Hash (SKEYID$_a$, N_3, A, B).

Message 1
A → B



B opens message gets P, g, T_A & Verifies Hash 1

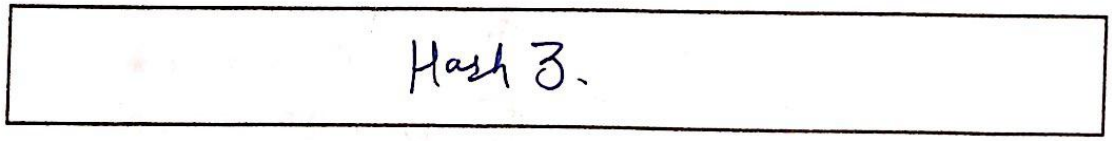
Message 2
B → A



Hash 2 = Hash (SKEYID$_a$, N_4, A, B)

A opens message 2 & gets T_B & verifies Hash 2.

Message 3



Hash 3 = Hash (SKEYID$_a$, N_3, N_4).

SECRET SESSION KEY =
HASH (SKEYID$_d$, DHSecret, N_3, N_4)

Ontario

Driver's Licence
Permis de conduire

ON
CANADA

1,2 NAME/ NOM
JAIN,
AAKASH,PRADEEP

8 1030-5233 DUNDAS ST W
ETOBICOKE, ON, M9B 6M1

4d NUMBER/ NUMÉRO J0183 - 00079 - 30819

4a ISS/ DÉL. 2018/10/15

4b EXP./ EXP. 2023/04/13

5 DD/ RÉF. GG2154202

16 HGT/ HAUT. 170 cm

15 SEX/ SEXE M

9 CLASS/ CATÉG. G2

12 REST./ COND.

3 DOB/DDN 1993/08/19

J0183-00079-30819
1993/08/19