- **Dynamic Host Configuration Protocol (DHCP)**

  Allow host to dynamically obtain its IP address from network server when it joins network.

  1. Host broadcasts "DHCP discover"
     src: 0.0.0.0:68
     dst: 255.255.255.255:67
     yiaddr: 0.0.0.0
  2. DHCP server responds with "DHCP offer"
     src: 165.229.1.10:67
     dst: 255.255.255.255:68
     yiaddr: 165.229.1.4
     Lifetime: 3600 sec
  3. Host requests IP address with "DHCP request"
     src: 0.0.0.0:68
     dst: 255.255.255.255:67
     yiaddr: 165.229.1.4
     Lifetime: 3600 sec
  4. DCHP server sends address with "DHCP ACK"
     src: 165.229.1.10:67
     dst: 255.255.255.255:68
     yiaddr: 165.229.1.4
     Lifetime: 3600 sec

- **Link State Routing** (Global, Static)

  In link state routing, if each node in the domain has the entire topology of the domain, the node can use Dijkstra's algorithm to build a routing table.

- **Distance Vector Routing** (Decentralized, Dynamic)

  Each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route.

- **Autonomous System (AS)** is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators on behalf of a single administrative entity or domain that presents a common, clearly defined routing policy to the Internet.

- **Subnet** is a set of interfaces that can be connected to each other without going through a router

- **Intra-AS Routing aka Inter Gateway Protocols (IGP)**

  Most common Intra-AS routing protocols:
  Routing Information Protocol (RIP) (Decentralized)
  Open Shortest Path First (OSPF) (Global)
  Interior Gateway Routing Protocol (IFRP)

- **Inter-AS Routing**

  Border Gateway Protocol (BGP) is the de facto standard. BGP provides each AS a means to: Obtain subnet reachability information from neighboring AS. / Propagate reachability information to all AS-internal routers. / Determine "good" routes to subnets based on reachability information and policy.

  Allows subnet to advertise its existence to rest of Internet: "I am here".

  Admin wants control over how its traffic routed, who routes through its net. Policy may dominate over performance.

- **OSI/IP Model, TCP/IP Model**

  Application RIP / BGP / FTP / HTTP / NFS / DHCP
  +Presentation MIME / TLS / SSL
  +Session

  Transport TCP / UDP / SCTP / DCCP
  Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing.

  Network ARP / IP / IPsec / ICMP
  Structuring and managing a multi-node network, including addressing, routing and traffic control.

  Data link Ethernet / PPP
  Reliable transmission of data frames between two nodes connected by a physical layer.

  Physical Ethernet / USB / Bluetooth
  Transmission and reception of raw bit streams over a physical medium.

- **User Datagram Protocol (UDP)**

  Best effort service, UDP segment may be lost or delivered out of order to app.

  Connectionless: No handshaking between UDP sender, receiver. Each UDP segment handled independently of others.

  UDP has no congestion control, so can blast away as fast as desired. Loss tolerant, Rate Sensitive.

- **Transmission Control Protocol (TCP)**

  Reliable, In-order Byte Stream / Pipelined / Full Duplex Data / Connection-oriented / Flow controlled

  TCP uses cumulative acks and uses single retransmission timer. Retransmissions are triggered by timeout events or duplicate acks.

- **TCP** provides "**Fast Retransmission**", that is, TCP retransmit last segment when 3 duplicated ACK even though the timer is not expired.

- **TCP** provides "**Flow Control**", that is, sender won't overflow receiver's buffer by transmitting too much, too fast.

  Receiver advertise spare room by including value of `RcvWindow` in segments.

- **TCP Opening a Connection**

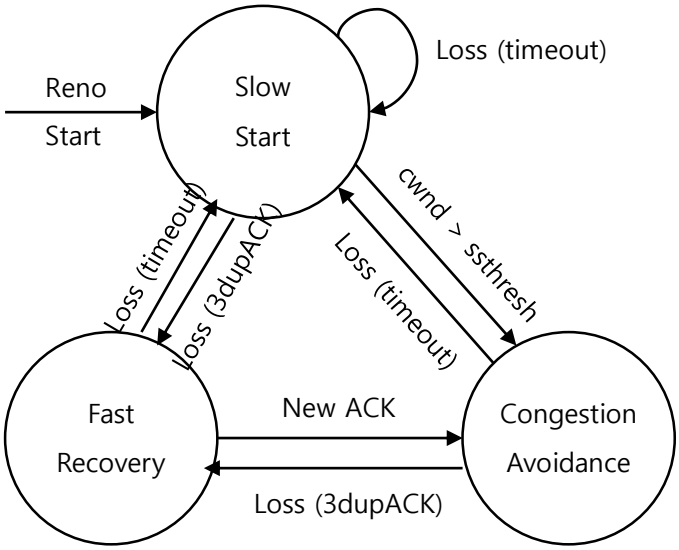
  TCP sender, receiver establish connection before exchanging data segments, that called three-way hand shaking.

  1. Client host sends SYN segment to server with specifies initial seq and without data.
  2. Server host receives SYN, replies with SYNACK segment with specifies server initial seq, then, allocates buffers.
  3. Client receives SYNACK, replies with ACK segment, which may contain data.

- **TCP Closing a Connection**

  1. Client sends FIN control segment to server.
  2. Server receives FIN, replies with ACK, then, closes connection, sends FIN.
  3. Client receives FIN, replies ACK, then, enter "TIME WAIT" because it can receive late arriving packets.
  4. Server receives ACK. Connection closed.

- **TCP** provides "**Congestion Control**" to avoid network's congestive collapse.

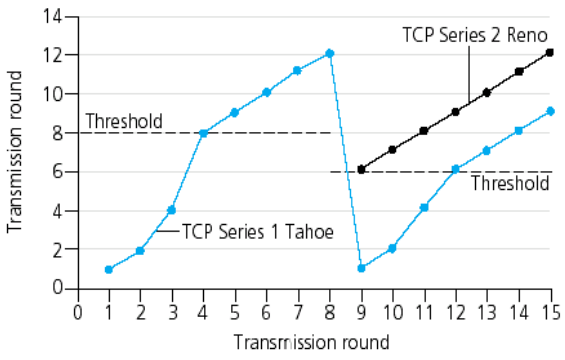


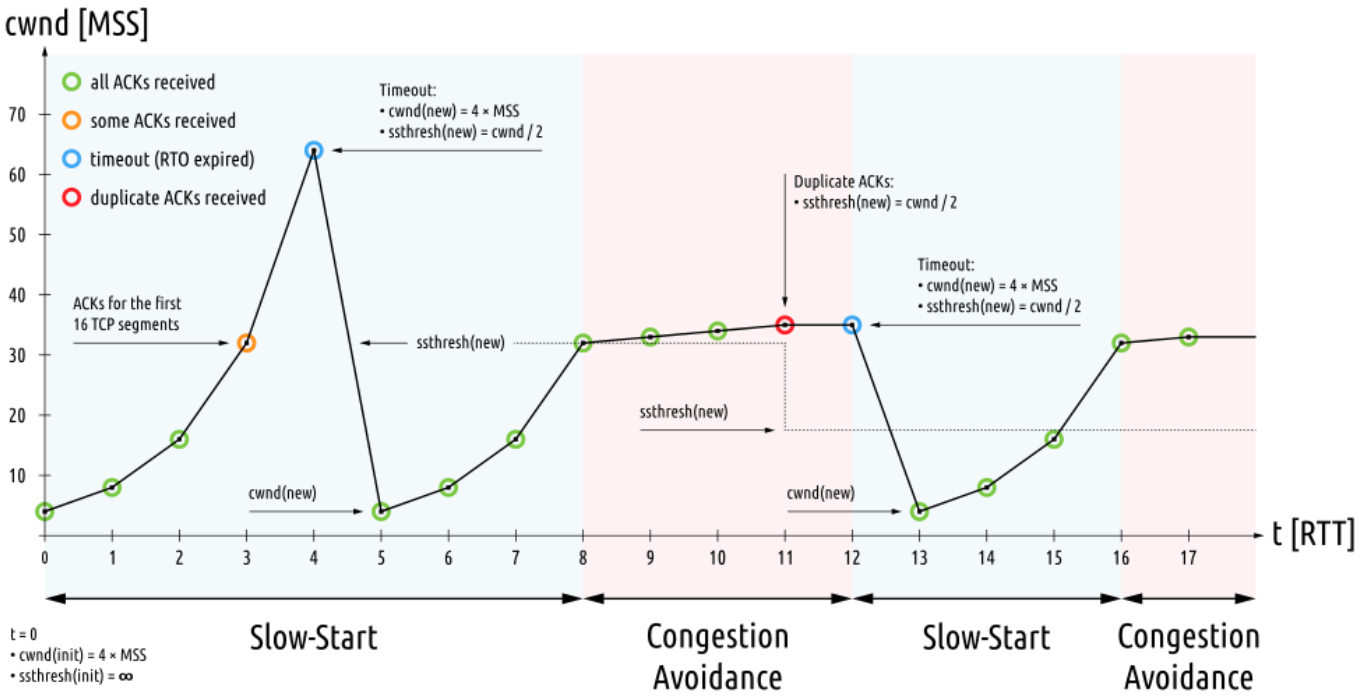
Additive Increase: increase `CongWin` by `1MSS` every RTT until loss detected.

Multiplicative decrease: cut `CongWin` in half after loss.

When connection begins, `CongWin = 1MSS`, then, increase rate exponentially fast until first loss evet. It called Slow Start.

$$\text{Source Rate} = \frac{\text{W} \cdot \text{MSS}}{\text{RTT}} \text{bps}$$





- **Elements of a Wireless Network: Hosts**

  May be stationary (non-mobile) or mobile such as Laptop, PDA, IP Phone.

- **Elements of a Wireless Network: Base Station**

  Typically connected to wired network. Responsible for sending packets between wired network and wireless host(s) in its area such as Cell Towers, AP.

- **Elements of a Wireless Network: Wireless Link**

  Typically used to connect mobile(s) to base station. Multiple Access Protocol coordinates link access.

- **Wireless Network: Infrastructure mode**

  Base station connects mobiles into wired network. Change of base station with connection into wired network called Handoff.

- **Wireless Network: Ad-Hoc mode**

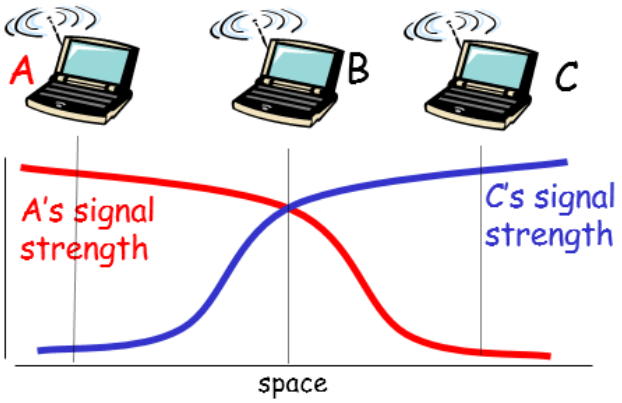
  No base stations. Nodes can only transmit to other nodes within link coverage, that is, nodes organize themselves into a network.

- **Wireless Link Characteristics**

  Decreased Signal Strength
  Radio signal attenuates as it propagates through matter.

  Interference from Other Sources
  Standardized wireless network frequencies shared by other devices; devices interfere as well.

  Multipath Propagation
  Radio signal reflects off objects ground, arriving at destination at slightly different times.



Terminal Problem: B, A and B, C hear each other but A, C cannot hear each other, so interfering at B.

- **802.11** divide spectrum into 11 channels at different frequencies. Channel can be same as that chosen by neighboring AP, so *host must associate* with an AP. Scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address.

- **802.11 Passive Scanning**

  1. Beacon frames sent from APs.
  2. Association Request frame sent from host to AP.
  3. Association Response frame sent from selected AP to host.

- **802.11 Active Scanning**

  1. Probe Request frame broadcast from host.
  2. Probes response from sent from APs.
  3. Association Request frame send from host to selected AP.
  4. Association Response fame sent from selected AP to host.

- **Carrier Sense Multiple Access (CSMA)**

  Listen before transmit. If channel sensed idle, transmit entire frame, if not, defer transmission. But collision can still occur since propagation delay.

- **CSMA/CD (Collision Detection)**

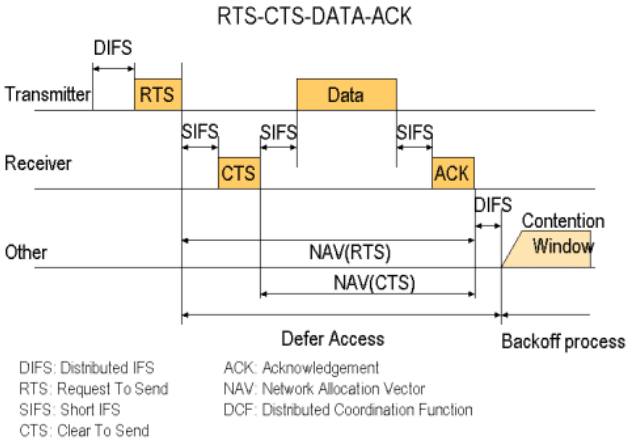
  If collision detected, transmission abort and random back-off. This is pretty good in wired LANs but difficult in wireless LANs because received signal strength overwhelmed by local transmission strength.

- **Beacon Frame** contains all the information about the network and contains list of mobiles with AP-to-Mobile frames waiting to be sent.

- **802.11 Power Management**

  Node-to-AP, I will sleep until next beacon fame. AP knows not to transmit frames to this node.

- **CSMA/CA (Collision Avoidance)**



If sense channel idle, sender wait DIFS because another host may be transmitting, then send RTS, wait CTS. If sense channel busy or CTS is not for itself, start or continue random back-off timer.

When receiver before receiving, broad cast CTS. If the receiver received frame, return ACK after SIFS since Terminal Problem.

- **802.11 Frame**

ADDR1 is MAC address of wireless host or AP to receive this frame.

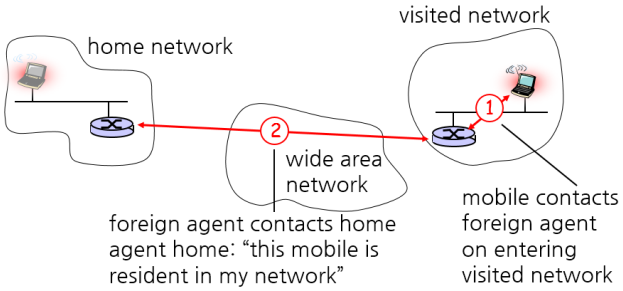
ADDR2 is MAC address of wireless host or AP transmitting this frame.

ADDR3 is MAC address of router interface to which AP is attached.

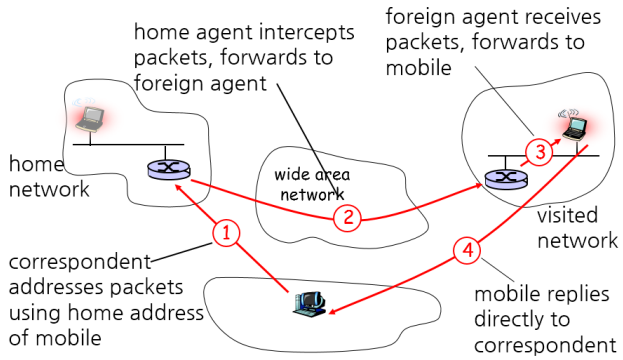
ADDR4 is used only in Ad-Hoc mode.

Duration of reserved transmission time.

- **Mobility Registration**



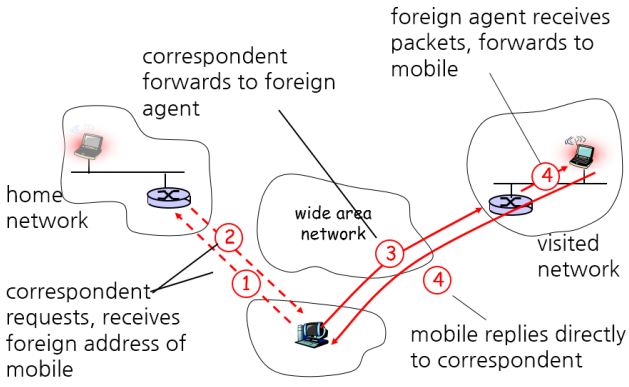
- **Mobility vid Indirect Routing**



Mobile uses two addresses:
Permanent Address used by correspondent (hence mobile location is transparent to correspondent)
Care-of-Address used by home agent to forward datagrams to mobile.

Triangle Routing Problem: It is very inefficient when correspondent, mobile are in same network.

- **Mobility via Direct Routing**



Overcome triangle routing problem but non-transparent to correspondent. Correspondent must get care-of-address from home agent.

- **Confidentiality (기밀성)**

Only sender, intended receiver should "understand" message contents.

- **Authentication (인증)**

Both sender and receiver want to confirm identity of each other.

- **Message Integrity (무결성)**

Both sender and receiver want to ensure message not altered (in transit, or afterwards) without detection.

- **Access and Availability (접근 가능성)**

Service must be accessible and available to users.

- **Hacker can**

Intercept message (Eavesdrop) / Actively insert messages into connection / Fake (spoof) source addr in packet (Impersonation) / "Take Over" ongoing connection by removing sender or receiver, inserting himself in place (Hijacking) / Prevent service from being used by others (Denial of Service) / ...

- **Breaking an Encryption Scheme**

Chipher-text only Attack: Hacker has cipher text who can analyze. / *Known-plaintext Attack*: Hacker has plaintext corresponding to cipher text. / *Chosen-plaintext Attack:* Hacker can get cipher text for chosen plaintext.

- **Symmetric Key Cryptography**

$$m = K_{A-B}(K_{A-B}(m))$$

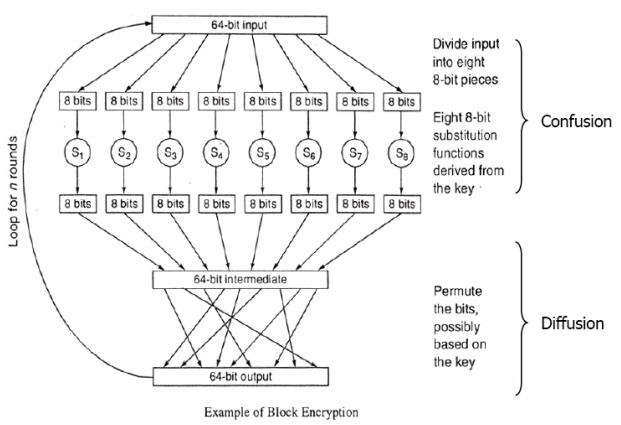
Both A and B share the same key K_{A-B}.

- **Public Key Cryptography**

$$m = K_B^-\left(K_B^+(m)\right)$$

Given public key K_B^+, it should be impossible to compute via private key K_B^-.

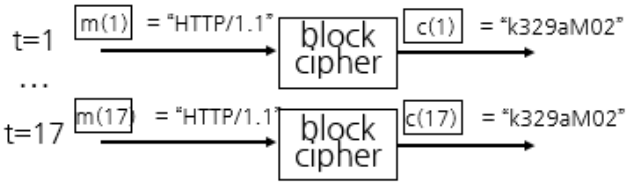
- **Block Cipher**



Example of Block Encryption

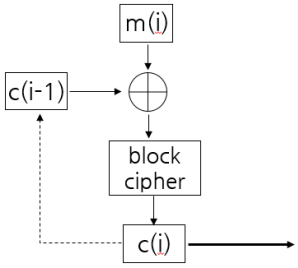
One pass through, one input bit affects eight output bits but in multiple pass through, each input bit affects all output bits. DES, AES… using Block Cipher.

- **Cipher Block Chaining**



If input block repeated, cipher block will produce same cipher text.

XOR i[th] input block. m(i), with previous block of cipher text, c(i-1).



- **Modular Arithmetic**

$$[(a \bmod n)(b \bmod n)] \bmod n = ab \bmod n$$

$$\therefore (a \bmod n)^d \bmod n = a^d \bmod n$$

- **Fermat's Little Theorem**

Prime number p, integer a s.t. $a < p$.

$$a^{p-1} \bmod p = 1$$

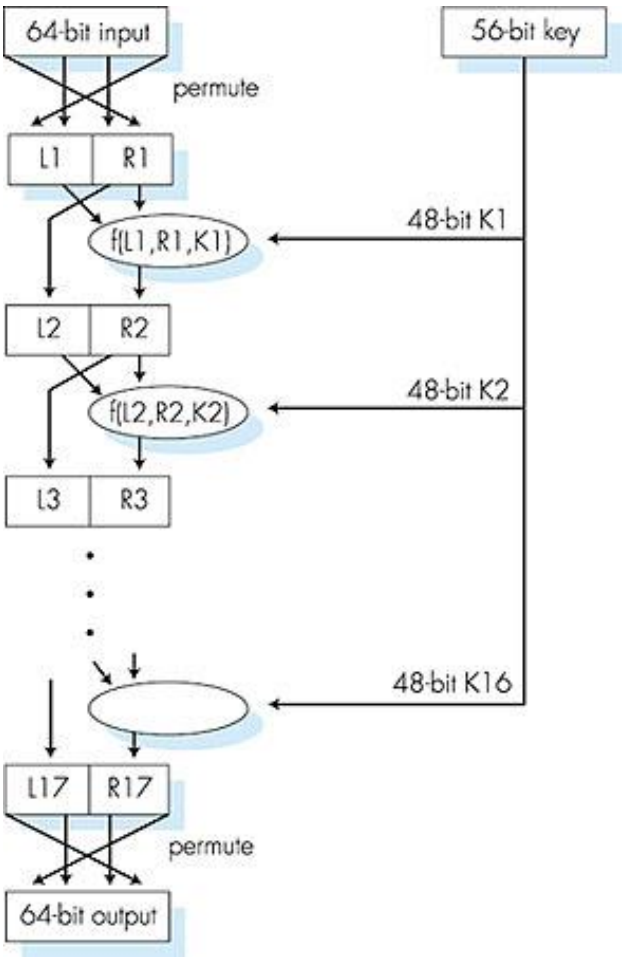
- **Euler's Totient Function**

$\varphi(n)$는 1부터 n까지 양의 정수 중 n과 서로소인 수의 개수.

$$\varphi(mn) = \varphi(m)\varphi(n)$$

$$\varphi(p) = p - 1 \text{ where } p \text{ is prime}$$

- **Data Encryption Standard (DES)**



- **Rivest, Shamir, Adleman Algorithm (RSA)**

1. Choose two large prime numbers p, q.
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e with $e < n$ that has no common factors with z. (e, z are "relatively prime")
4. Choose d such that $ed - 1$ is exactly divisible by z. In other words, $ed \bmod z = 1$.
5. Public key is $K_B^+(n, e)$, Private key is $K_B^-(n, d)$.

To encrypt message $m(< n)$, compute $c = m^e \bmod n$
To decrypt message c, compute $m = c^d \bmod n$

$$m = (m^e \bmod n)^d \bmod n$$

- **Euler's Theorem**

Euler's totient function $\varphi(n)$, integer a s.t. $a < n$

$$a^{\varphi(n)} \bmod n = 1$$

- **Proof of RSA**

$$
\begin{aligned}
&(m^e \bmod n)^d \bmod n \\
&= m^{ed} \bmod n \because (a \bmod n)^d \bmod n = a^d \bmod n \\
&= m^{ed-1+1} \bmod n \\
&= m^{kz+1} \bmod n \quad \text{where} \quad k \in \mathbb{Z} \\
&= m^{k(p-1)(q-1)} m \bmod pq \\
&= \left[\left(m^{k(p-1)(q-1)} \bmod pq\right)(m \bmod pq)\right] \bmod pq \\
&= \left[\left(m^{k\varphi(p)\varphi(q)} \bmod pq\right)(m \bmod pq)\right] \bmod pq \\
&= \left[\left(m^{k\varphi(pq)} \bmod pq\right)(m \bmod pq)\right] \bmod pq \\
&= \left[\left(\left(m^{\varphi(pq)} \bmod pq\right)^k \bmod pq\right)(m \bmod pq)\right] \bmod pq \\
&= [(1^k \bmod pq)(m \bmod pq)] \bmod pq \\
&= (m \bmod pq) \bmod pq \\
&= m \because m < pq
\end{aligned}
$$

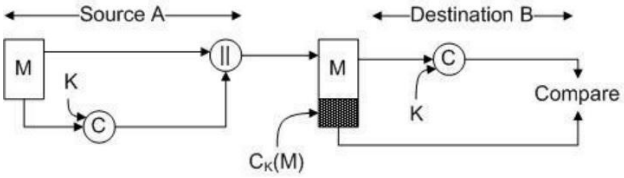
- **Proof of $\boldsymbol{m = K^-(K^+(m)) = K^+(K^-(m))}$**

$$
\begin{aligned}
(m^e \bmod n)^d \bmod n &= m^{ed} \bmod n = m^{de} \bmod n \\
&= (m^d \bmod n)^e \bmod n
\end{aligned}
$$

- **Cryptographic Hash**

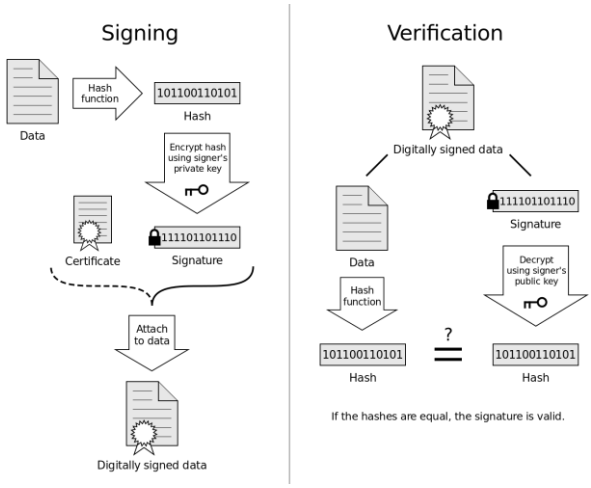
Takes input m, produces fixed length value, $H(m)$. Computationally infeasible (실행불가능한) to find two different message, x, y such that $H(x) = H(y)$.

- **Message Authentication Code (MAC)**



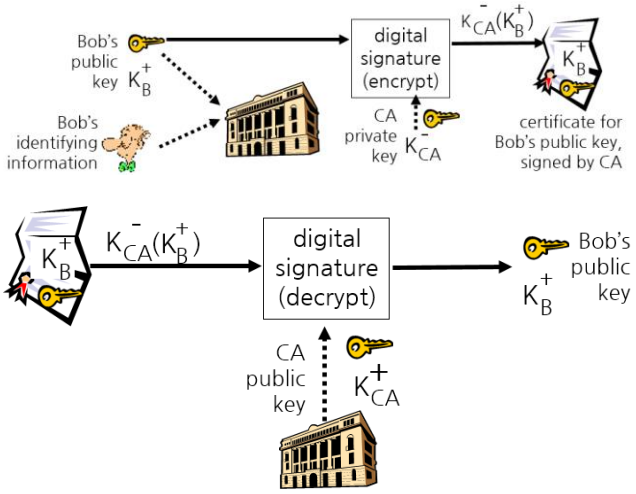
MD5 or SHA-1 hash functions are widely used.

- **Digital Signatures**



Cryptographic technique analogous to hand-written signatures. The reason why encrypt after hash is to reduce the transmitted size.

- **Certification Authorities (CA)**



Binds public key to particular entity, E. E provides proof of identity to CA. CA creates certificate binding E to its public key. Certificate containing E's public key digitally signed by CA.

1. Bob create public key and private key.
2. Bob register public key to CA.
3. CA create certificate including Bob's public key and signature using CA's private key.
4. Alice request certificate that included Bob's public key.
5. Alice decrypt certificate using CA's public key.
6. Alice check the key is Bob's.

- **Playback Attack**

Hacker records sender's packet and later plays it back to receiver.

- **Man in the Middle Attack**
- **Network-layer Confidentiality**
- **Virtual Private Networks (VPN)**
- **IPsec** provides Data integrity / Origin authentication / Replay attack prevention / Confidentiality.

IPsec datagram emitted and received by end-system. Protects upper level protocols. No protection or encryption on the original IP header.

- **Authentication Header (AH) Protocol**

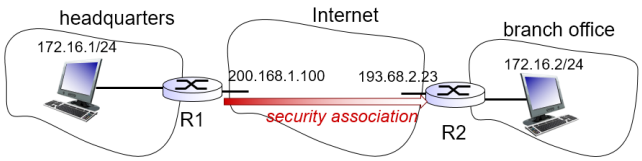
  Provides source authentication & data integrity but not confidentiality.

- **Encapsulation Security Protocol (ESP)**

  Provides source authentication, data integrity, and confidentiality.

- **Security Associations (SA)**

  Before sending data, SA established from sending to receiving entity. SAs are simplex. Ending, receiving entities maintain state information about SA, that is, IPsec is connection-oriented.



  State info at R1 for this SA:
  32-bit SA identifier: Security Parameter Index (SPI) / Origin SA interface / Destination SA interface / Type of encryption SA interface / Type of encryption used / Encryption key / Type of integrity check used / Authentication key

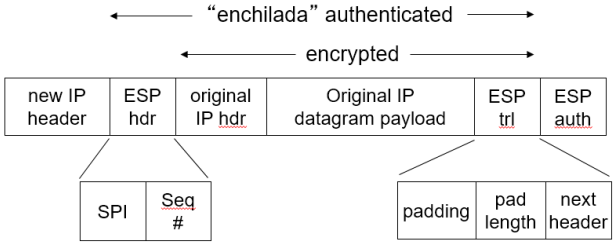
- **Security Association Database (SAD)**

  Endpoint holds SA state in SAD, where it can locate them during processing. With n salespersons, 2+2n SAs in R1's SAD.

  When sending IPsec datagram, R1 accesses SAD to determine how to process datagram.

  When IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, and processes datagram accordingly.

- **IPsec Datagram**



- **Convert Original Datagram to IPsec Datagram**

  1. Appends to back of original datagram (which includes original header fields) an "ESP trailer" field.
  2. Encrypts result using algorithm & key specified by SA.
  3. Appends to front of this encrypted quantity the "ESP header", creating "Enchilada".
  4. Creates authentication MAC over the whole enchilada, using algorithm and key specified in SA.
  5. Appends MAC to back of enchilada, forming payload.
  6. Creates brand new IP header, with all the classic IPv4 header fields, which it appends before payload.

- **Security Policy Database (SPD)**

  For a given datagram, sending entity needs to know if it should use IPsec and needs also to know which SA to use.

  Info in SPD indicates "what" to do with arriving datagram, info in SAD indicates "how" to do it.

- **Internet Key Exchange (IKE)**

  Authentication (prove who you are) with either pre-shared secret (PSK) or with public/private keys and certificates (PKI). IKE message exchange for algorithms, secret keys, SPI numbers.

  PSK is both sides start with secret. Run IKE to authenticate each other and to generate IPsec SAs (one in each direction), including encryption, authentication keys.

  PKI is both sides start with public/private key pair, certificate. Run IKE to authenticate each other, obtain IPsec SAs (one in each direction).

- **Firewalls**

  Isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.

  Prevent denial of service attacks. / Prevent illegal modification/access of internal data. / Allow only authorized access to inside network.

- **Intrusion Detection Systems (IDS)**

  Packet filtering operates on TCP/IP headers only. IDS includes *Depp Packet Inspection* (DPI) which is look at packet contents and includes *Examine Correlation* among multiple packets.

- **ARP Spoofing**

  Registration of a fake IP-MAC address mapping in the ARP cache of a remote machine.

- **AKD Diagram**

- **Defense against ARP Spoofing**

  Use static ARP entries. It cannot be updated, spoofed ARP relies are ignored, and ARP table needs a static entry for each machine on the network.

- **S-ARP** is cryptography-based approach. Normal ARP request but ARP replies are signed by the sender's private key. It needs Authoritative Key Distributor (AKD) for management of mapping between an IP address and the corresponding public key.

  Limitations of S-ARP: Single-point-of-failure problem / Computation cost / Infrastructure upgrade overhead (Upgrade of DHCP server required) / Incremental deployment is not easy (S-ARP node does not accept replies from non-S-ARP nodes)