IPv6 : Security Features and Considerations

IPv6 : Security Features and Considerations

IPv4 was not designed with security in mind.

Packet Sniffing: Due to network topology, IP packets sent from a source to a specific destination can also be read by other nodes, which can then get hold of the payload (for example, passwords or other private information).

IP Spoofing: IP addresses can be very easily spoofed both to attack those services whose authentication is based on the sender's address (as the rlogin service or several WWW servers).

Connection Hijacking: Whole IP packets can be forged to appear as legal packets coming from one of the two communicating partners, to insert wrong data in an existing channel.

IPv4 : Security Issues

Shortage of IP Address : Lack of visibility and transparency

Data is open to all : No Confidentiality

Not Designed for any inbuilt Security Feature

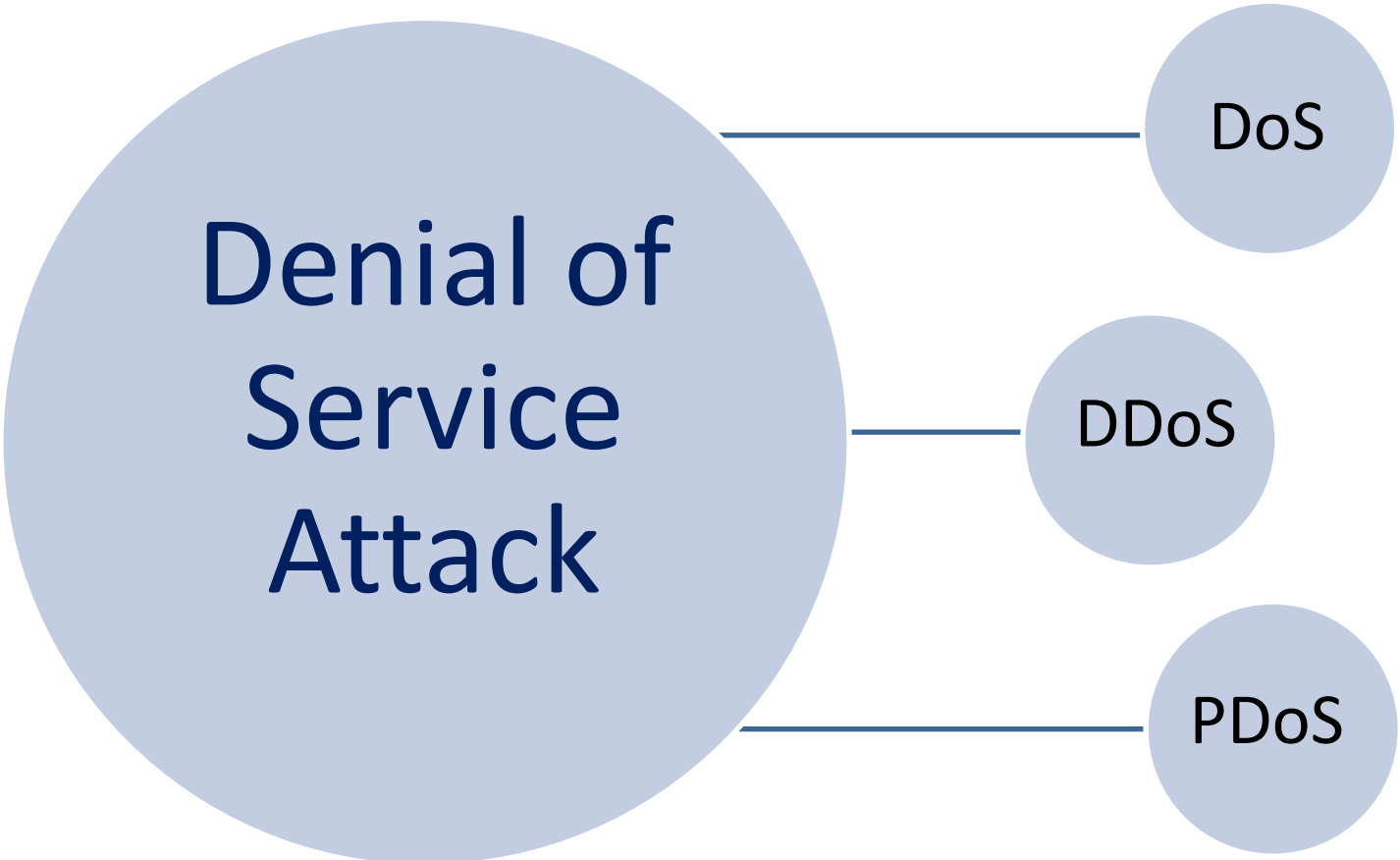
Inherent absence of any tool to ensure integrity of the data

Small Subnet address space helps quick Scanning of Port : Vulnerable to attacks

No provision of Load Balancing helps to achieve Denial of Service (DoS) attack

Broadcast feature actually helps launch of Denial of Service (DoS) attack

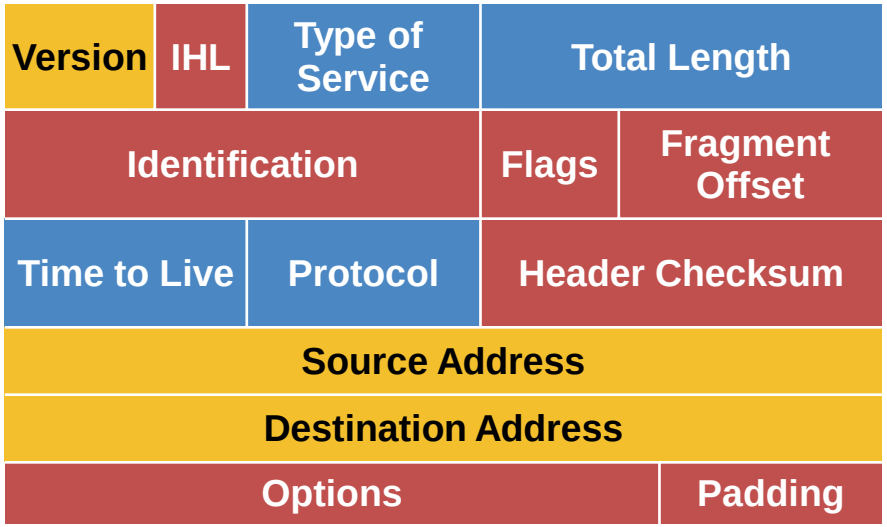
IPv6 : Security Features and Considerations



IPv6 : Security Features and Considerations

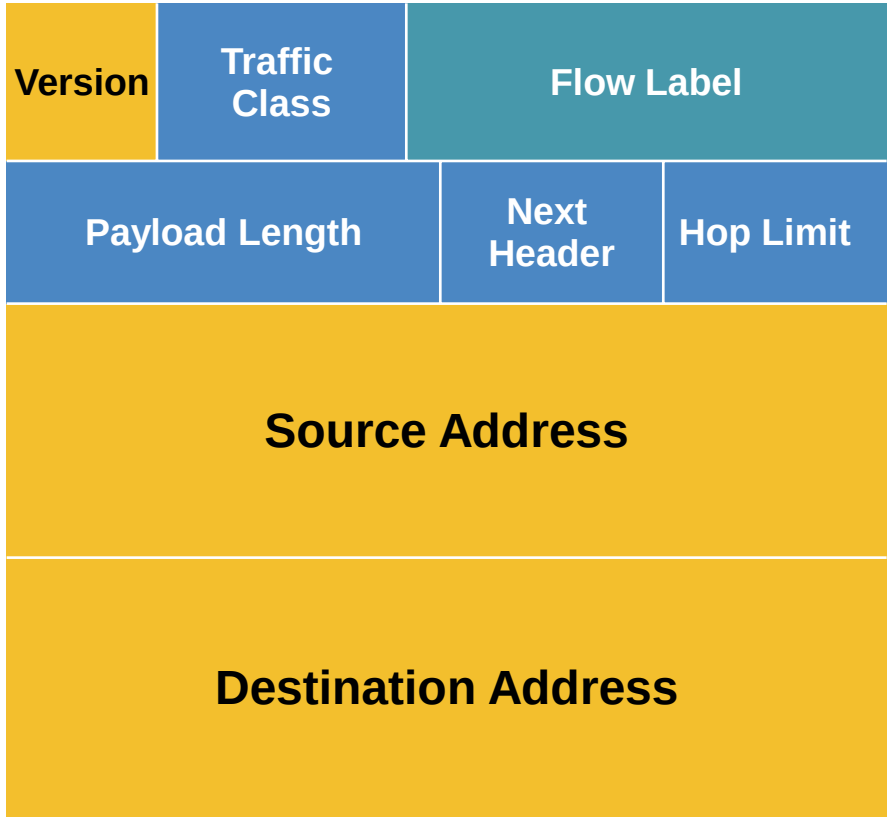
IPv4: 20 Bytes + Options

IPv4 Header

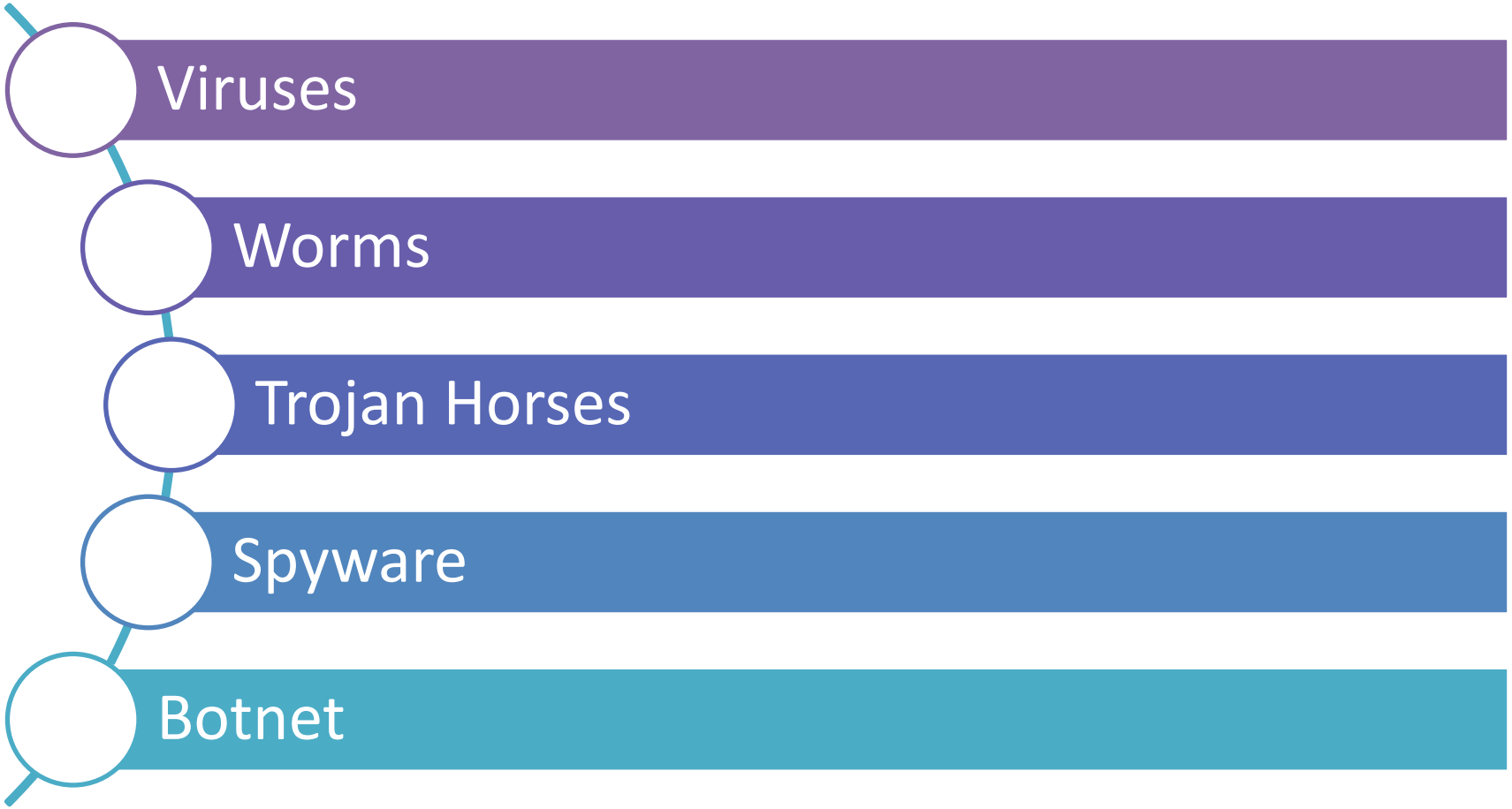


IPv6: 40 Bytes + Extension Header

IPv6 Header



IPv6 : Security Features and Considerations



IPv6 : Security Features and Considerations

Viruses and Worms :

Viruses and Email, IM worms: IPv6 brings in no change.

Other worms:

- **IPv4: reliance on network scanning**
- **IPv6: not so easy**

IPv4 best practices around worm detection and mitigation remain valid.

IPS systems and Anti-viruses will not change.

IPv6 : Security Features and Considerations

IPv4 was not designed with security in mind.

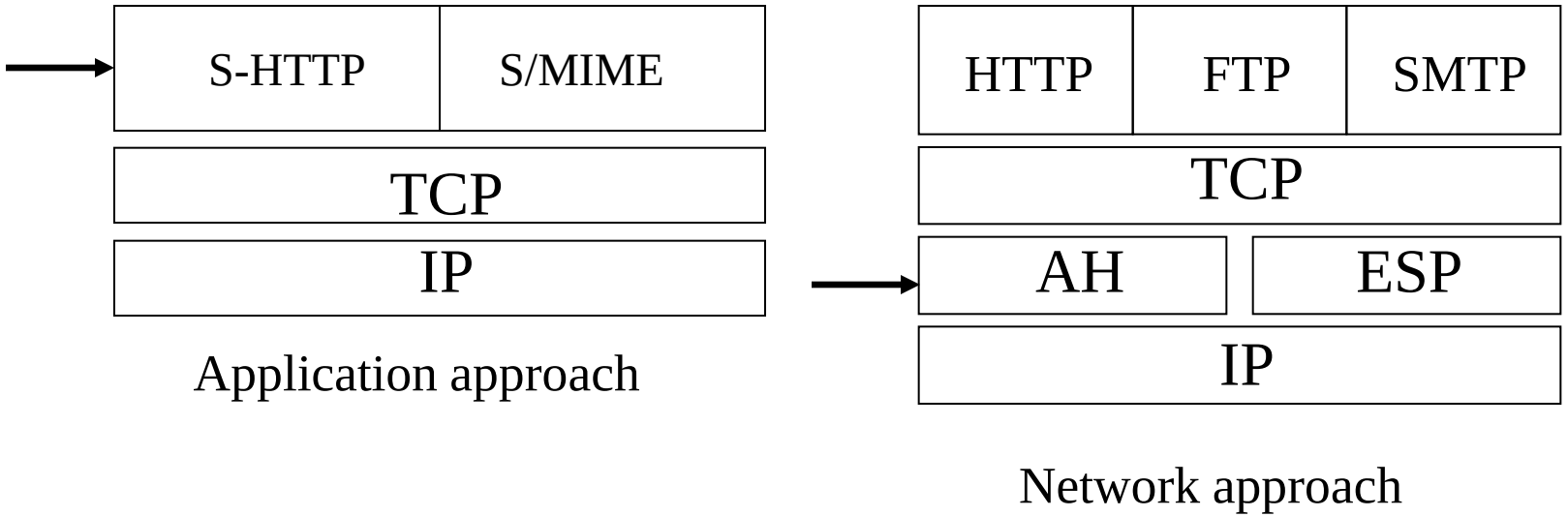
In IPv4, Security is implemented in:

In Applications – HTTPS, IMAPS, SSH etc.

IPsec tunnels

IPv6 : Security Features and Considerations

IPsec Services



IPv6 : Security Features and Considerations

IPv6 IPSec:

Applies to both IPv4 and IPv6:

- **IPSec was retrofitted in IPv4**
- **IPSec is a part of IPv6 base protocol suite.**

Applicable to use over LANs, across public & private WANs, & for the Internet

IPSec is a security framework

- **Provides suit of security protocols**
- **Secures a pair of communicating entities**
- **Two different modes: Transport mode (host-to-host) and Tunnel Mode (Gateway-to-Gateway or Gateway-to-host)**

IPv6 : Security Features and Considerations

Services Provided by IPsec

Authentication – ensure the identity of an entity (integrity) and replay protection

Confidentiality – protection of data from unauthorized disclosure

Key Management – generation, exchange, storage, safeguarding, etc. of keys in a public key cryptosystem

IPv6 : Security Features and Considerations

IPsec Services

Authentication: AH (Authentication Header - RFC 4302)

Confidentiality: ESP (Encapsulating Security Payload - RFC 4303)

Key management: IKEv2 (Internet Key Exchange - RFC4306)

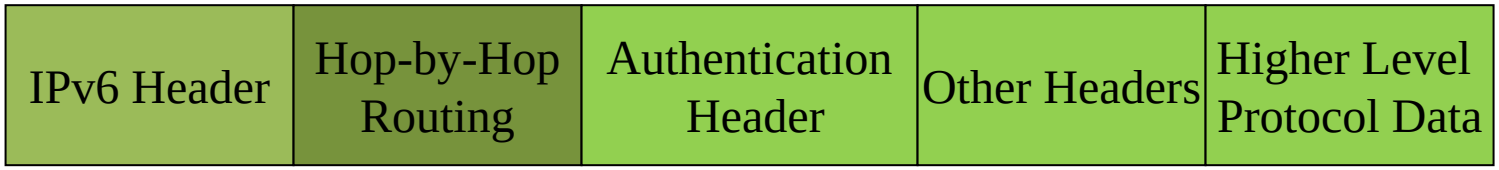
When two computers (peers) want to communicate using IPSec, they mutually authenticate with each other first and then negotiate how to encrypt and digitally sign traffic they exchange. These IPSec communication sessions are called security associations (SAs).

IPv6 : Security Features and Considerations

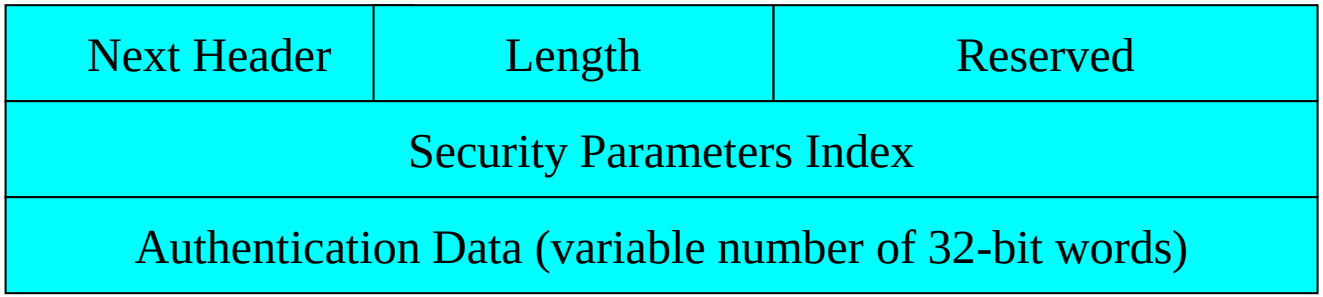
IPv6 IPsec Protocol

IPsec AH

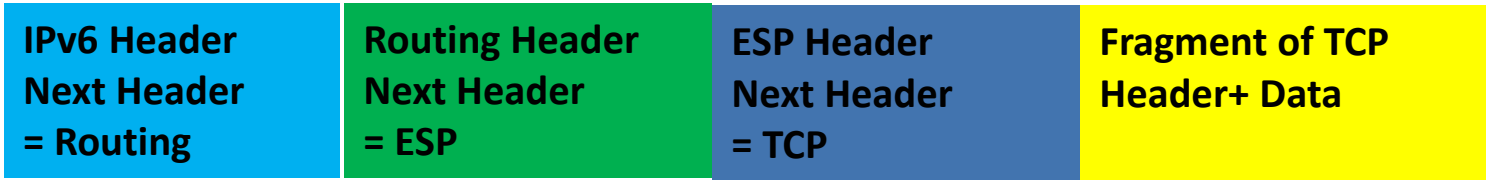
IPv6 AH Packet Format



IPv6 AH Header Format

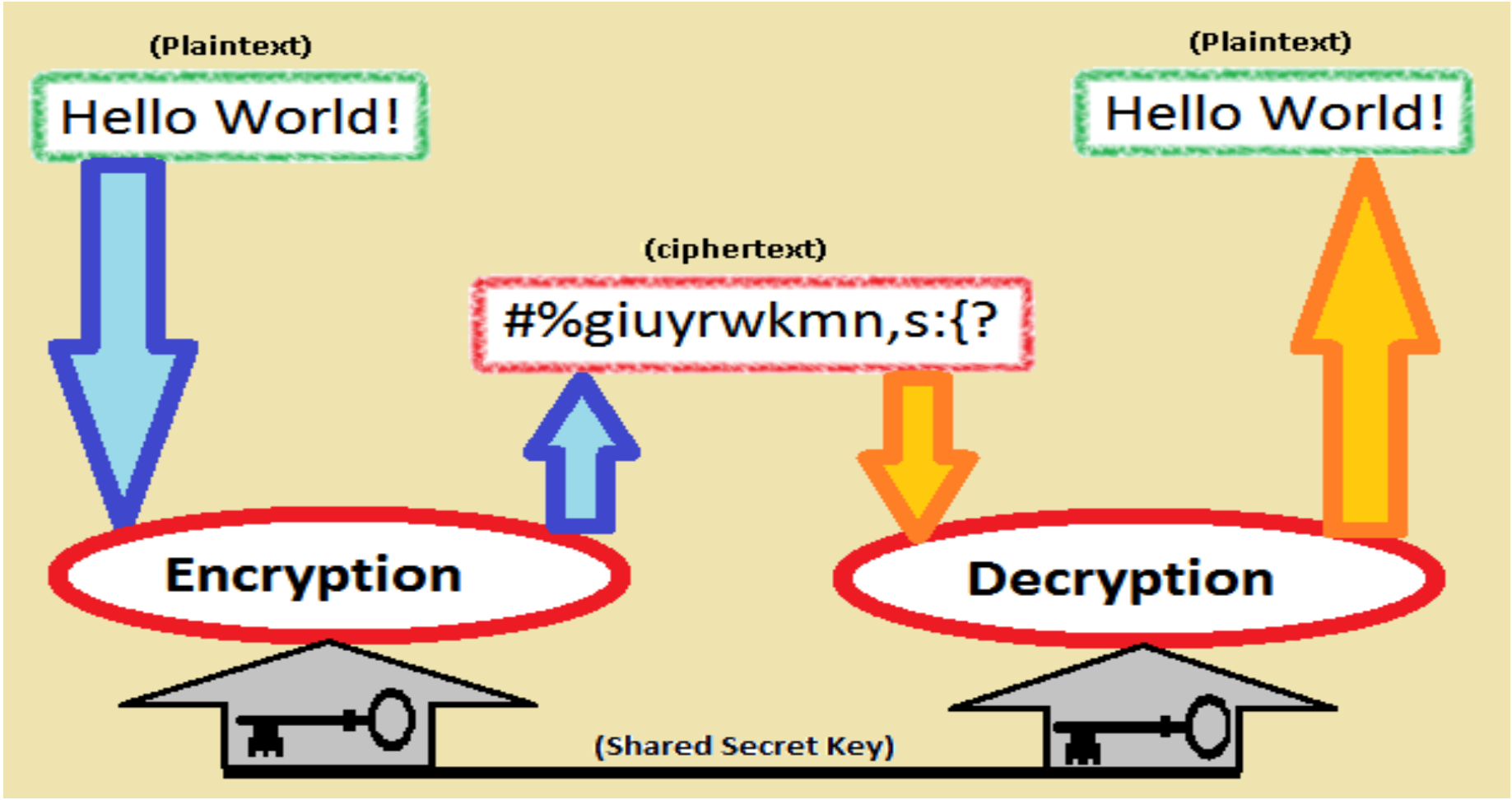


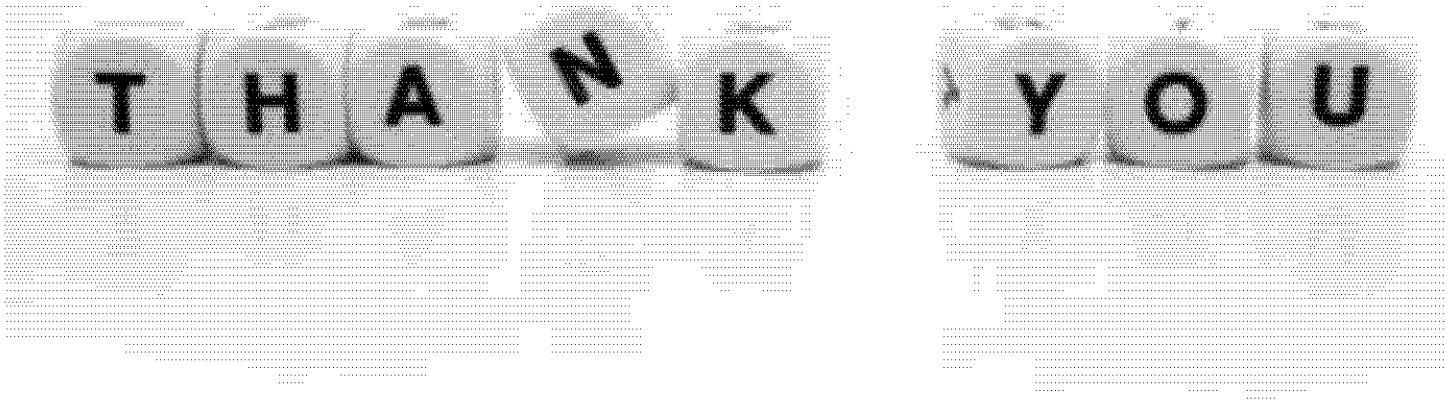
IPv6 : Security Features and Considerations



- IPSec was retrofitted in IPv4
- IPSec is a part of IPv6 base protocol suite.

IPv6 Header Next Header = Routing	Routing Header Next Header = ESP	ESP Header Next Header = TCP	Fragment of TCP Header+ Data




THANK YOU