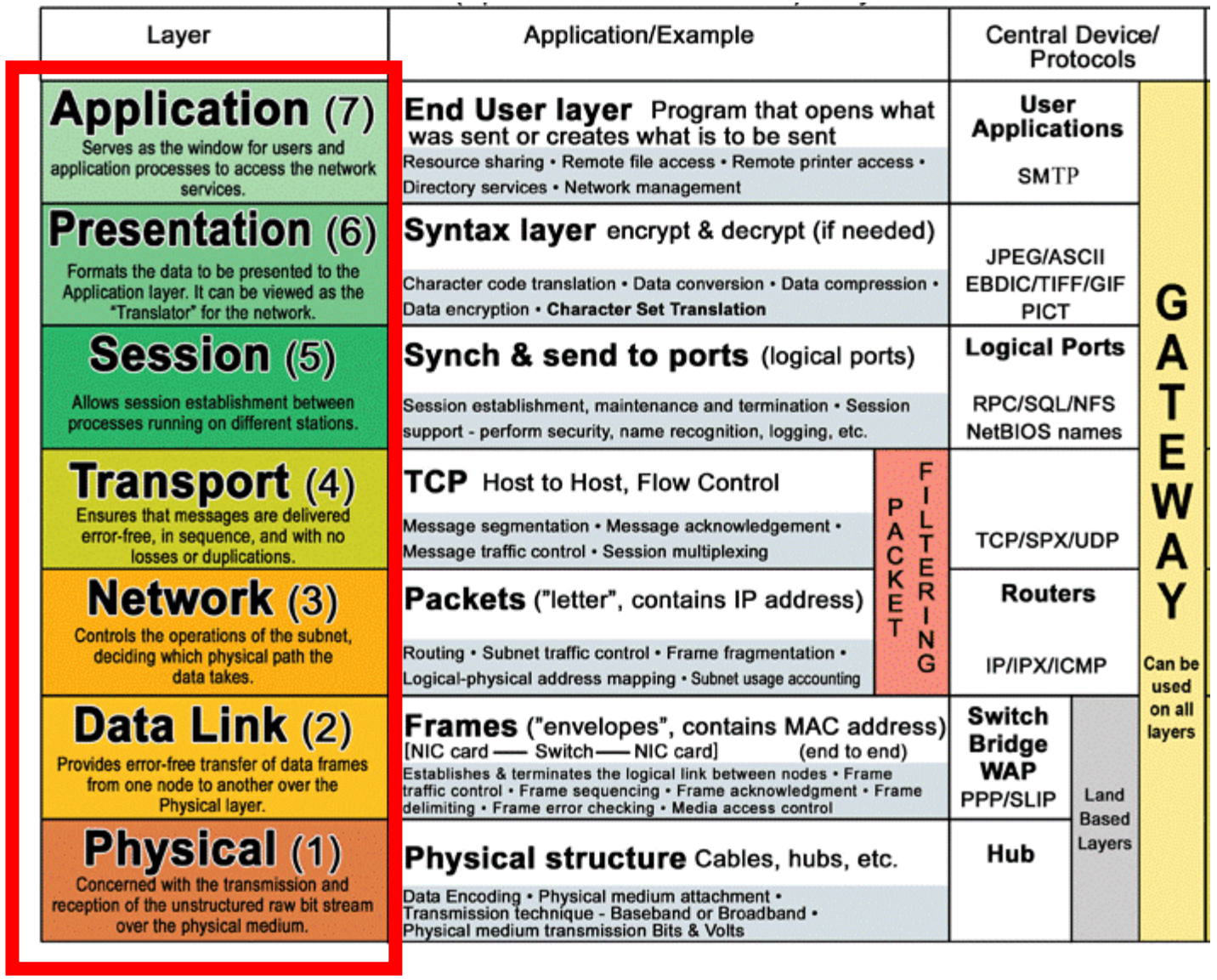
a mini session on

NETWORK SECURITY

NEWORK SECURITY AT ALL LAYERS

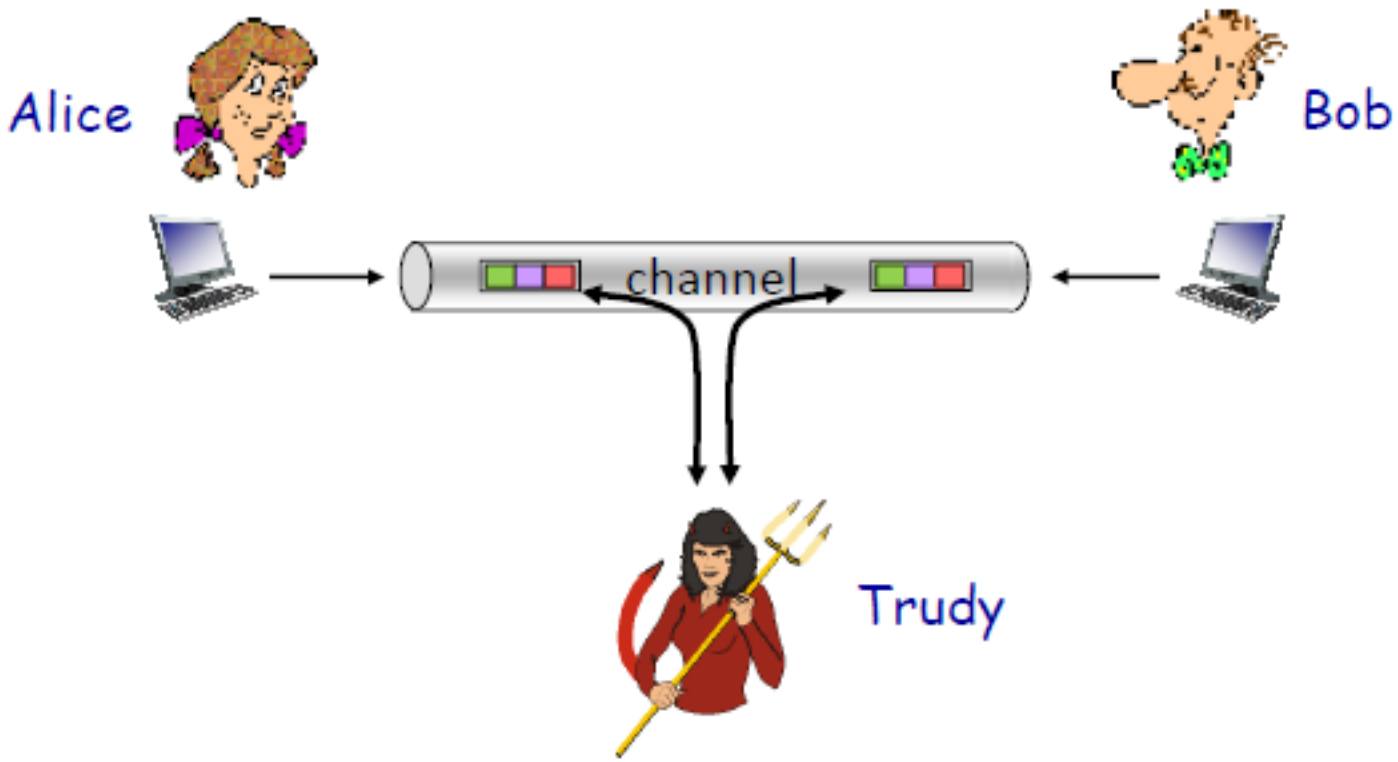


Layer	Application/Example		Central Device/ Protocols		
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers	
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

What is Network Security?

Friends and Enemies: Alice, Bob, Trudy

- Alice and Bob (lovers!) want to communicate "secretly".
- Trudy (intruder) wants to interfere.

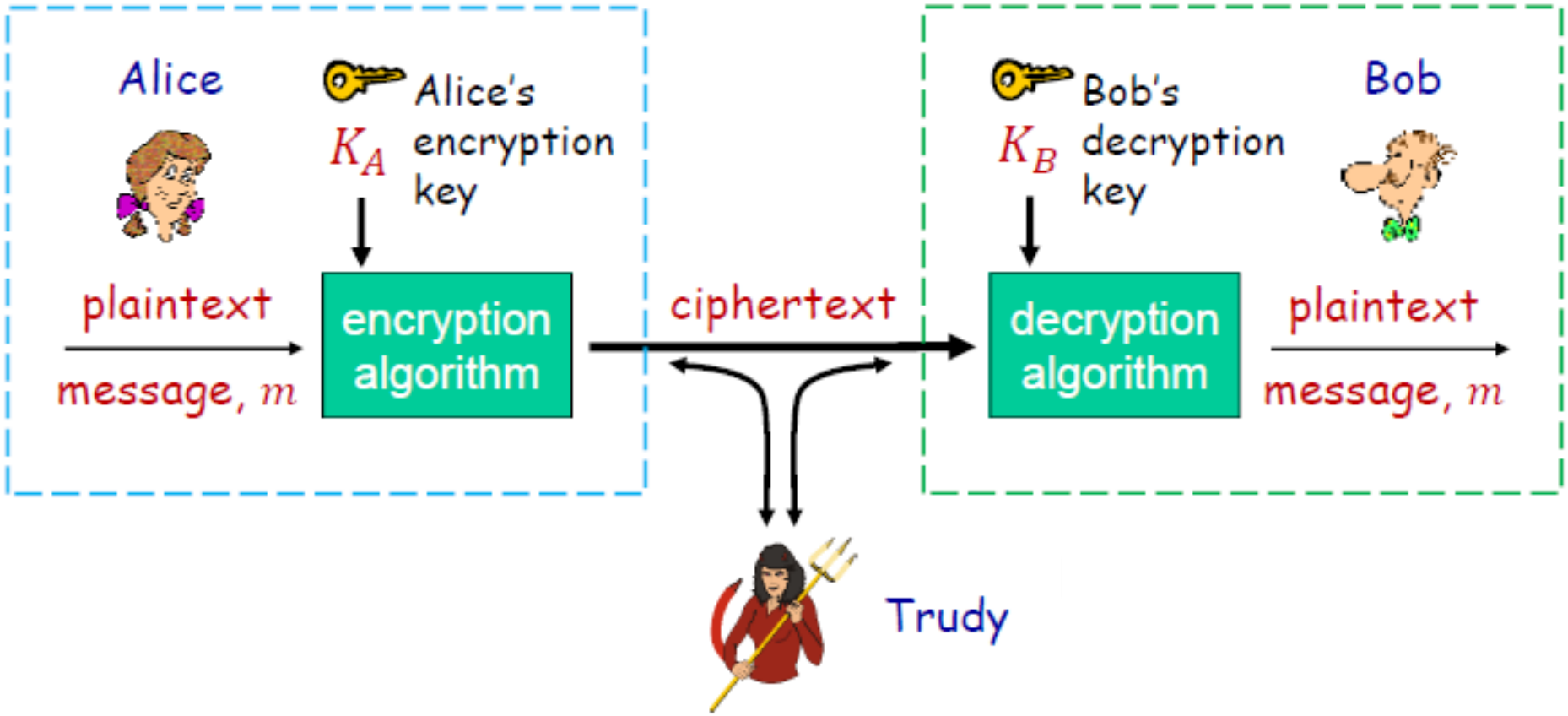


What Can Bad Guy Trudy Do?

Trudy may:

- intercept messages of Alice and Bob.
  - Need to ensure message confidentiality.
- modify messages, or even forge messages and insert into communication between Alice and Bob.
  - Need to ensure message authenticity.
- attack the communication channel between Alice and Bob (e.g. denial-of-service attack).
  - Need to ensure service availability

Cryptography



Types of Cryptography

- The purpose of cryptography is to make it difficult for an unauthorized third party to understand private communication between two parties.

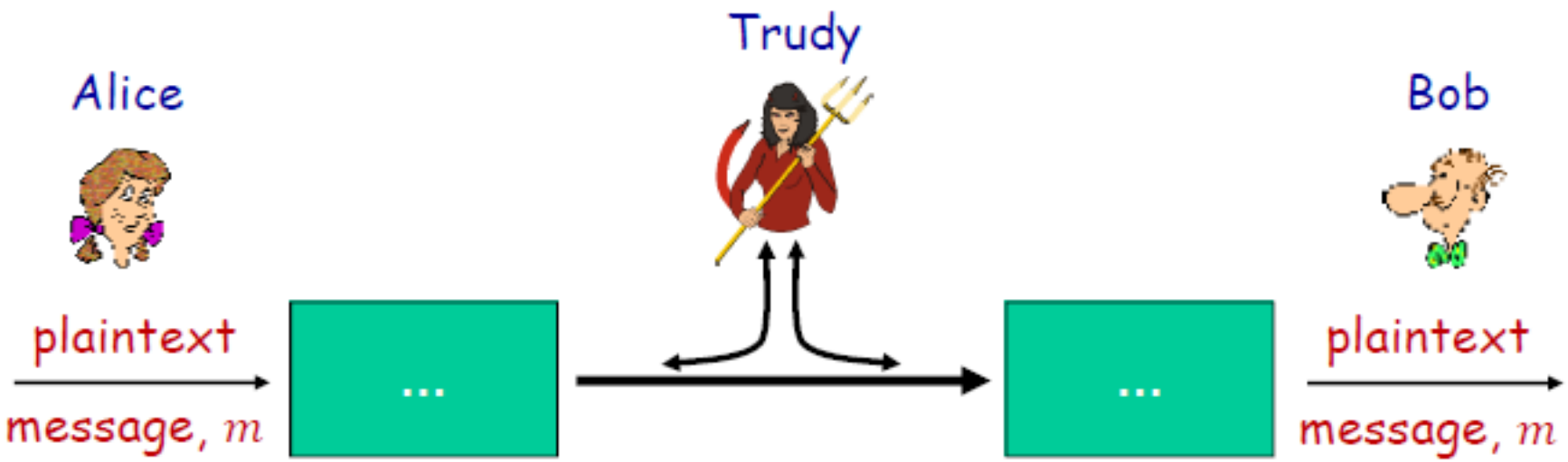
- Cryptography often uses keys:
  - Algorithms are known to everyone
  - Only "keys" are secret

- Symmetric key cryptography
  - Involves the use of one key
- Public key cryptography
  - Involves the use of a pair of keys

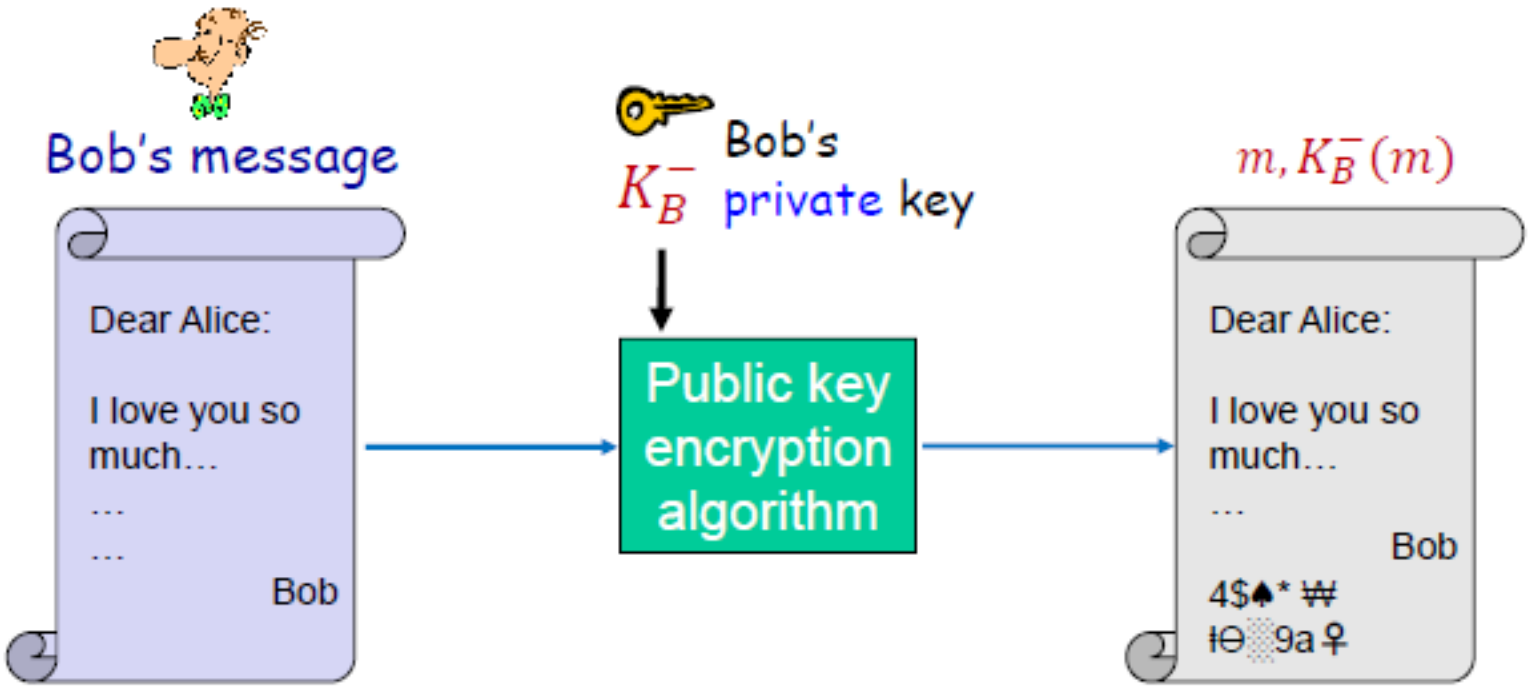
Source: IEEE Spectrum

Message Authenticity

- In addition to encryption, there are other security issues to address.
- For example, suppose Bob receives a message (which may be encrypted or in plaintext). How can Bob know:
  - This message is not tampered with on its way to Bob ?
  - This message is indeed created by Alice ?

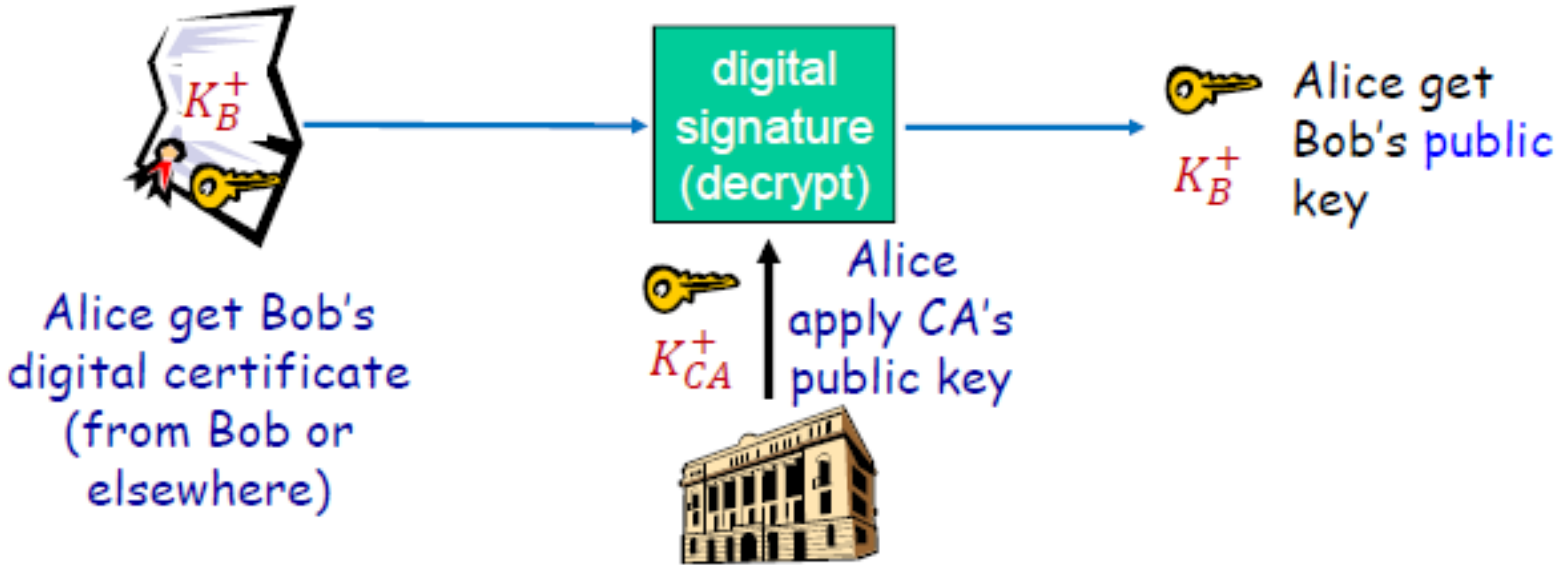


Digital Signature



Digital Certificates

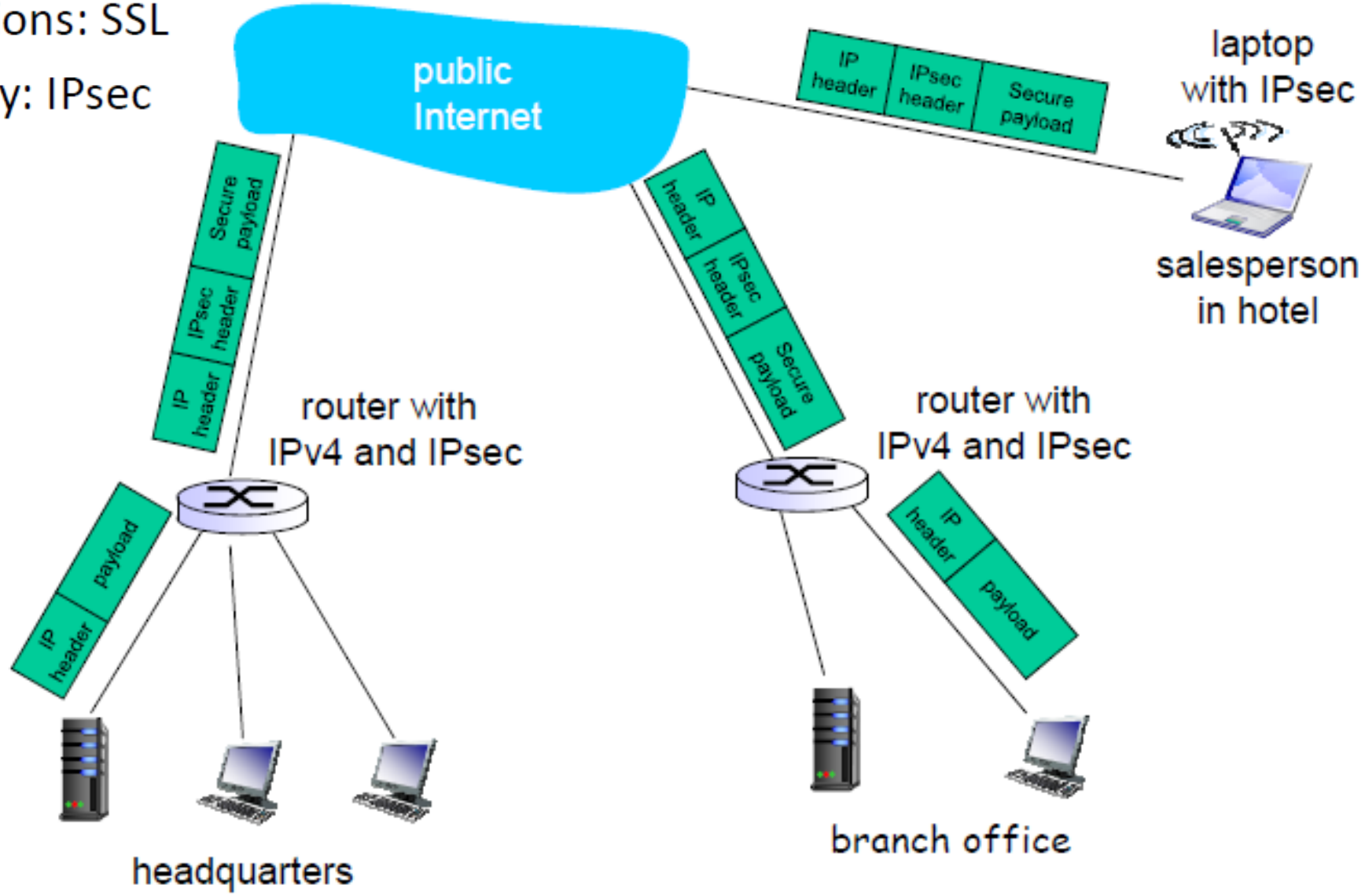
- Alice may wonder if the public key she uses is indeed Bob's.
- Certificate authority (CA) is an entity that issues digital certificates.
  - A digital certificate certifies the ownership of a public key by the named subject of the certificate.



Virtual Private Network (VPN)

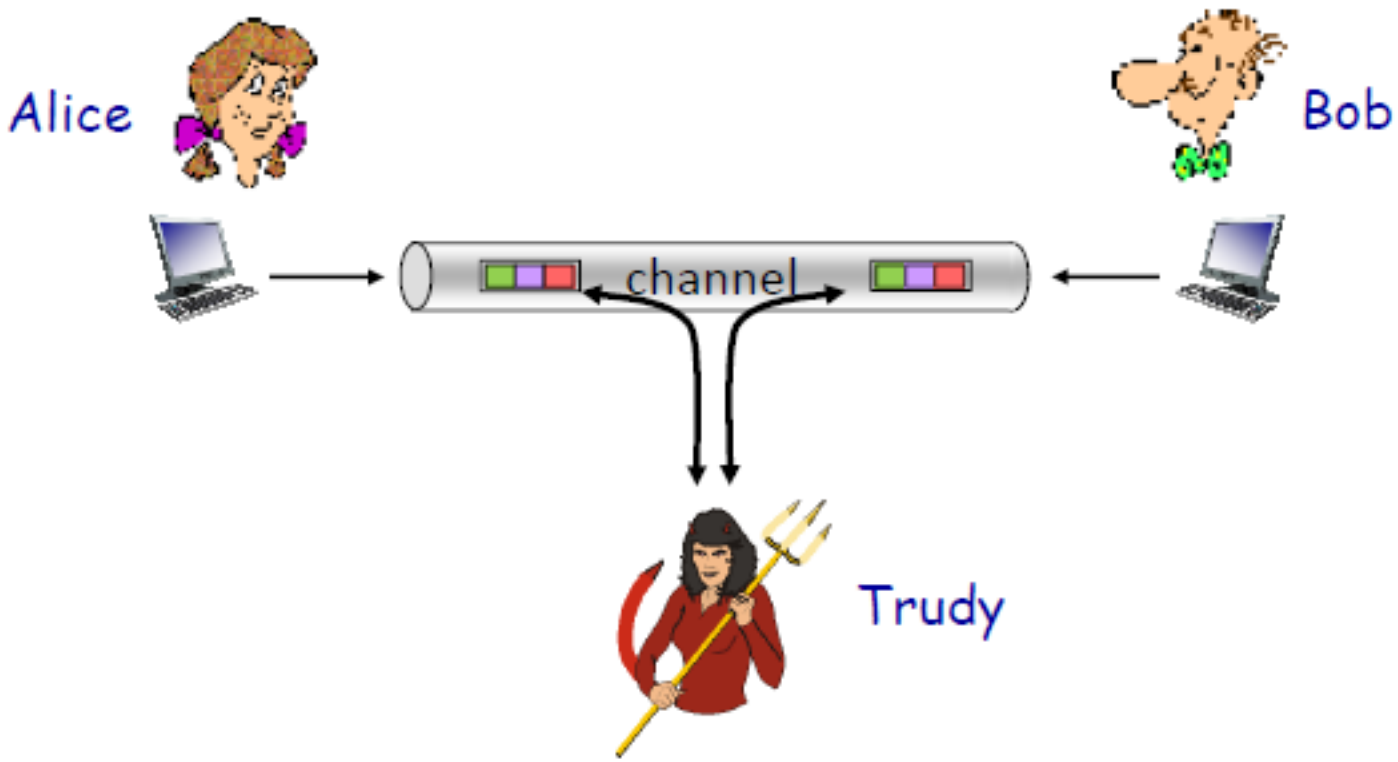
Securing TCP Connections: SSL

Network Layer Security: IPsec



Friends and Enemies: Alice, Bob, Trudy

- Alice and Bob (lovers!) want to communicate "secretly".
- Trudy (intruder) wants to interfere.



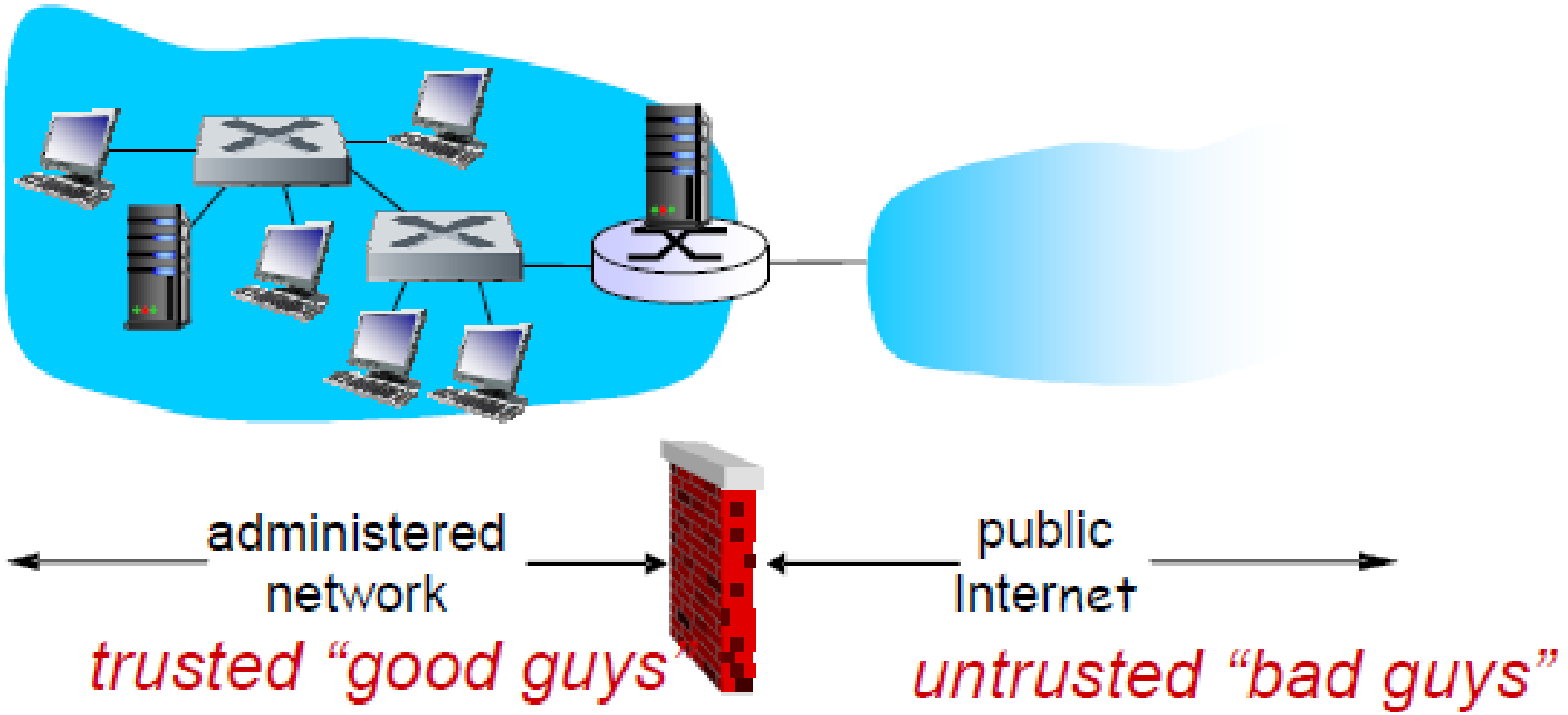
What Can Bad Guy Trudy Do?

Trudy may:

- intercept messages of Alice and Bob.
  - Need to ensure message confidentiality.
- modify messages, or even forge messages and insert into communication between Alice and Bob.
  - Need to ensure message authenticity.
- attack the communication channel between Alice and Bob (e.g. denial-of-service attack).
  - Need to ensure service availability

Firewalls (packet filtering)

isolates organization's LAN from the Internet, allowing some packets to pass, blocking others.



Intrusion Detection Systems

- deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)

- examine correlation among multiple packets
  - port scanning
  - DoS attack