Communication Security

Protocols For Secure Communications

What is network security?

confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Protocols for Secure Communications

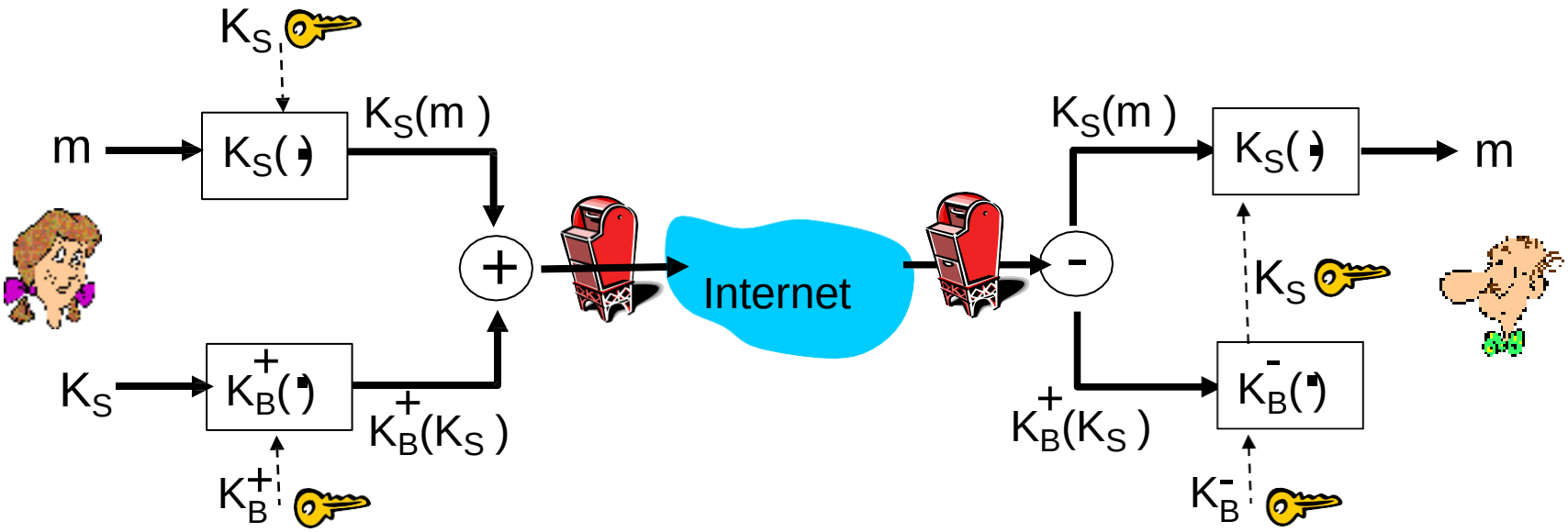
- Much of the software currently used to protect the confidentiality of information are not true cryptosystems
- They are applications to which cryptographic protocols have been added
- Particularly true of Internet protocols
- As the number of threats to the Internet grew, so did the need for additional security measures

Securing Internet Communication with S-HTTP and SSL

- Secure Socket Layer (SSL) protocol:
  - uses public key encryption to secure channel over public Internet
- Secure Hypertext Transfer Protocol (S-HTTP):
  - extended version of Hypertext Transfer Protocol; provides for **encryption of individual messages** between client and server across Internet.
  - It is an encrypted solution to the unsecured version of HTTP.
- S-HTTP is the application of SSL over HTTP(https-Microsoft)
  - Allows encryption of information passing between computers through protected and secure virtual connection

Secure e-mail

Alice wants to send confidential e-mail, m, to Bob.

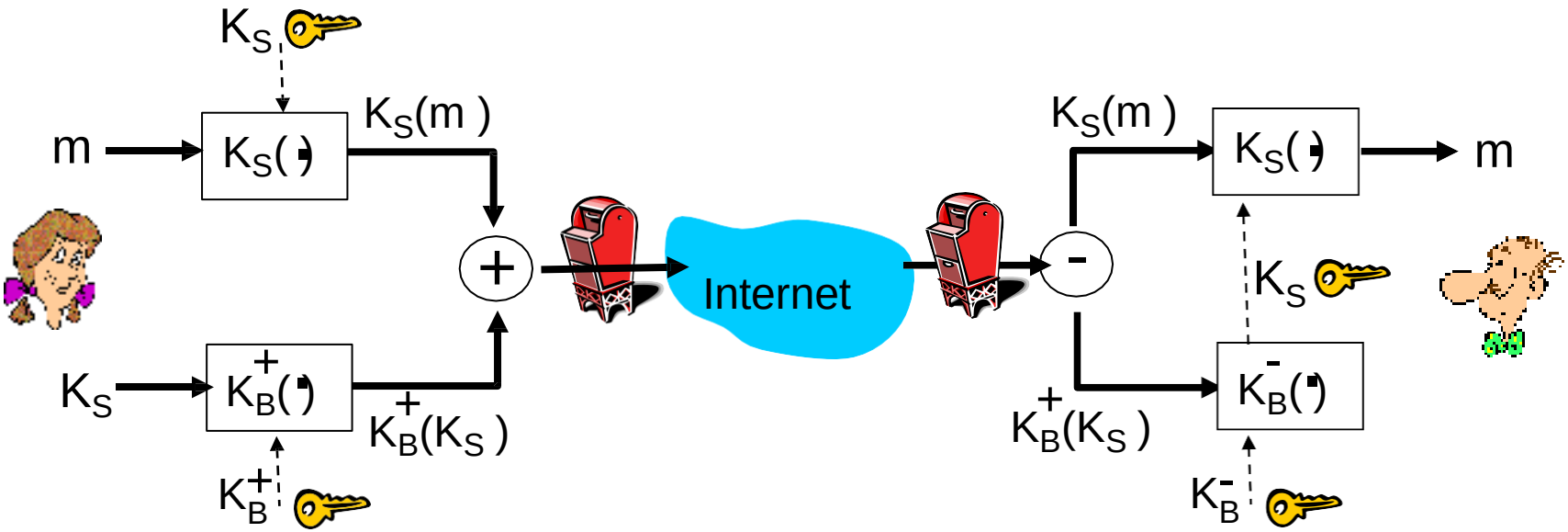


Alice:

- generates random *symmetric* private key, K_S
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob

Secure e-mail

Alice wants to send confidential e-mail, m, to Bob.

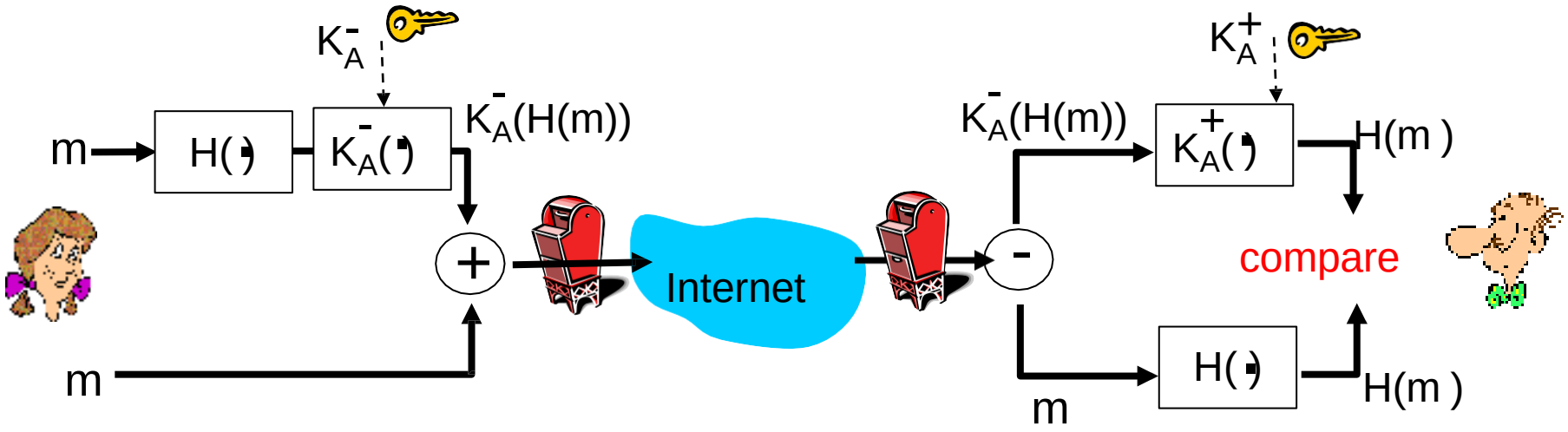


Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure e-mail (continued)

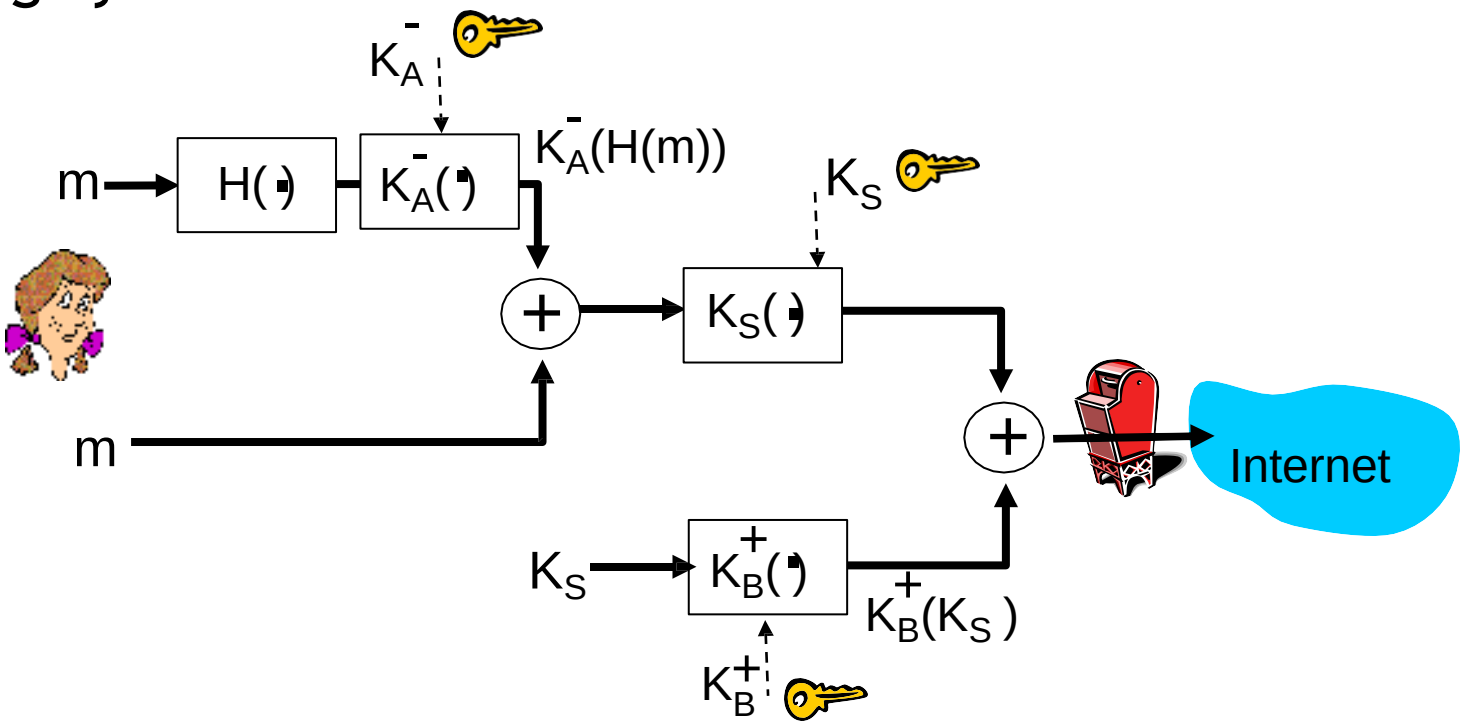
Alice wants to provide sender authentication message integrity



- Alice digitally signs message
- sends both message (in the clear) and digital signature

Secure e-mail (continued)

Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

Securing e-mail with S/MIME, PEM, and PGP

- Secure Multipurpose Internet Mail Extensions (S/MIME):
  - builds on Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication **through digital signatures** based on public key cryptosystems**.**
- Privacy Enhanced Mail (PEM):
  - proposed as standard to function with public-key cryptosystems;
  - uses 3DES symmetric key encryption
- Pretty Good Privacy (PGP):
  - uses IDEA Cipher for message encoding
  - 128-bit symmetric key block encryption algorithm with 64-bit blocks for message encoding.
  - uses RSA for symmetric key exchange and for digital signatures.

- PGP, PEM, and S/MIME **work to secure e-mail operations.**

Securing Web transactions with SET, SSL, and S-HTTP

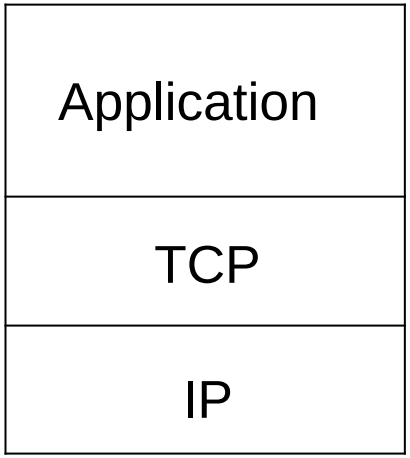
- Secure Electronic Transactions (SET):
  - developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
  - **Uses DES to encrypt credit card information transfers and RSA for key exchange.**
  - Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores.

- SET, SSL, S-HTTP, Secure Shell (SSH-2), and IP Security (IPSec) work to secure Web browsers, especially at electronic commerce sites.

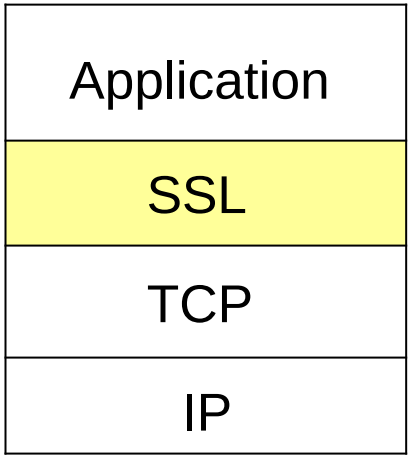
SSL: Secure Sockets Layer

- widely deployed security protocol
  - supported by almost all browsers, web servers
  - https
  - billions $/year over SSL
- variation -TLS: transport layer security, RFC 2246
- provides
  - *confidentiality*
  - *integrity*
  - *authentication*
- original goals:
  - Web e-commerce transactions
  - encryption (especially credit-card numbers)
  - Web-server authentication
  - optional client authentication
- available to all TCP applications
  - secure socket interface

SSL and TCP/IP



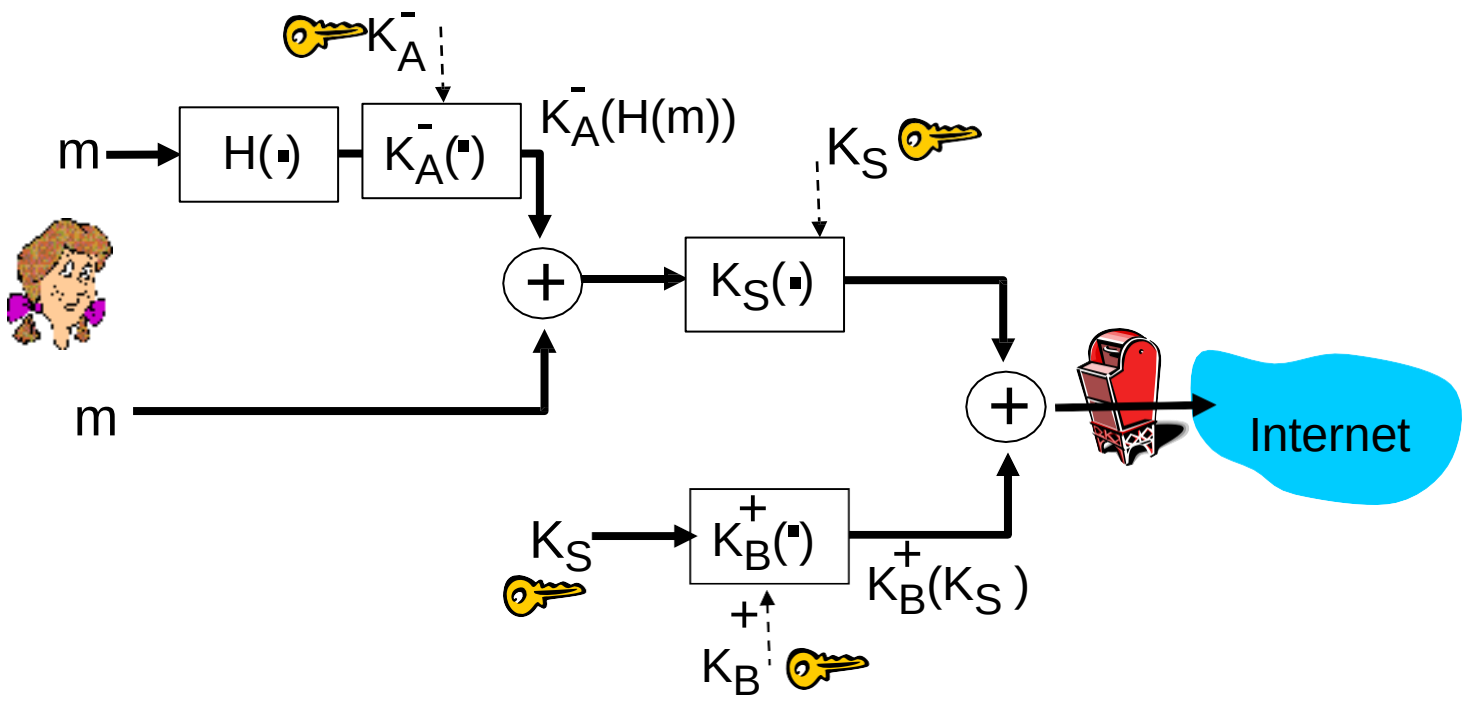
normal application



application with SSL

- SSL provides application programming interface (API) to applications
- C and Java SSL libraries/classes readily available

Could do something like PGP:



- but want to send byte streams & interactive data
- want set of secret keys for entire connection
- want certificate exchange as part of protocol: handshake phase

Toy SSL: a simple secure channel

- *handshake:* Alice and Bob use their certificates, private keys to authenticate each other and exchange shared secret
- *key derivation:* Alice and Bob use shared secret to derive set of keys
- *data transfer:* data to be transferred is broken up into series of records
- *connection closure:* special messages to securely close connection

Securing Wireless Networks with WEP and WPA

- Wired Equivalent Privacy (WEP):
  - early attempt to provide security with the 802.11 network protocol
- Wi-Fi Protected Access (WPA and WPA2):
  - created to resolve issues with WEP
- Next Generation Wireless Protocols:
  - Robust Secure Networks (RSN), AES – Counter Mode Encapsulation, AES – Offset Codebook Encapsulation
- Bluetooth:
  - can be exploited by anyone within approximately 30 foot range, unless suitable security controls are implemented

Protocols for Secure Communications

Securing TCP/IP with IPSec

- Internet Protocol Security (IPSec):
  - open source protocol to secure communications across any IP-based network
- IPSec designed to protect **data integrity**, **user confidentiality**, and **authenticity** at IP packet level
- IPSec combines several different cryptosystems:
  - **Diffie-Hellman key exchange, Public-key cryptography**, Bulk **encryption algorithms**, **Digital certificates.**
- In IPSec, IP layer security obtained by use of application header (AH) protocol or encapsulating security payload (ESP) protocol
    - **defines the information to add to an IP packet, as well as how to encrypt packet data**

Securing TCP/IP with IPSec and PGP

- Internet Protocol Security (IPSec):
  - an open-source protocol framework for security development within the TCP/IP family of protocol standards

- IPSec uses several different cryptosystems
  - Diffie-Hellman key exchange for deriving key material between peers on a public network
  - Public key cryptography for signing the Diffie-Hellman exchanges to guarantees identity
  - Bulk encryption algorithms for encrypting the data
  - Digital certificates signed by a certificate authority to act as digital ID cards

Securing TCP/IP with IPSec and PGP

- Pretty Good Privacy (PGP): hybrid cryptosystem designed in 1991 by Phil Zimmermann
  - Combined best available cryptographic algorithms to become open source de facto standard for encryption and authentication of e-mail and file storage applications
  - Freeware and low-cost commercial PGP versions are available for many platforms
  - PGP security solution provides six services: authentication by digital signatures; message encryption; compression; e-mail compatibility; segmentation; key management

Function	Algorithm	Application
Public key encryption	RSA/SHA-1 or DSS/SHA-1	Digital signatures
Conventional encryption	3DES, RSA, IDEA or CAST	Message encryption
File management	ZIP	Compression

Table 8-12 PGP Functions[24]