

EEC-682/782 Computer Networks I

Lecture 26

Wenbing Zhao

wenbingz@gmail.com

http://academic.csuohio.edu/zhao_w/teaching/eec682.htm

(Lecture notes are based on materials supplied by
Dr. Louise Moser at UCSB and Prentice-Hall)



Outline

- # Today's topics
 - Web Security
 - Social issues
 - Review for final exam
- # All deferred assignments due by mid-night next Thursday (May 12, 2005)
 - Use my google mail account to turn in: **wenbingz@gmail.com**
- # **Final Exam:** May 12 Th, 6:00-8:00pm
 - One sheet of Letter-sized notes allowed
 - Primarily on chapters 7 and 8; other important topics include IP and TCP protocols, and routing protocols (potentially)
- # **Grading** will be posted to the class Web site by mid-night Monday, May 16, 2005

Web Security

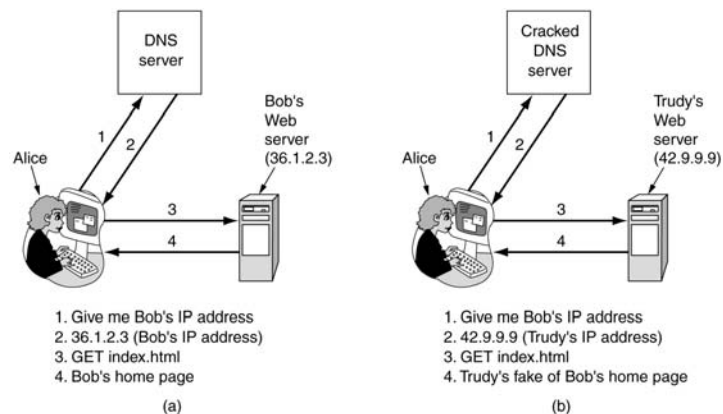
- # Threats
- # Secure Naming
- # SSL - The Secure Sockets Layer
- # Mobile Code Security

Threats

- # Web server is compromised and Web page is replaced
- # Denial of Service attack
- # Steal confidential data such as credit card info
- # Propagation of false information over Internet

Secure Naming

- # (a) Normal situation. (b) An attack based on breaking into DNS and modifying Bob's record



Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

5

Secure Naming

- # **DNS spoofing:** tricking a DNS server into installing a false IP address
- # **Poisoned cache:** a cache that holds an intentionally false IP address
- # DNS has some preliminary barrier for DNS spoofing
 - First, DNS server checks to see that the reply bears the correct IP source address of the top-level server
 - But since Trudy can put anything she wants in that IP field, she can defeat that test easily since the IP addresses of the top-level servers have to be public
 - Second, to allow DNS servers to tell which reply goes with which request, all requests carry a sequence number
 - To spoof Alice's ISP, Trudy has to know its current sequence number

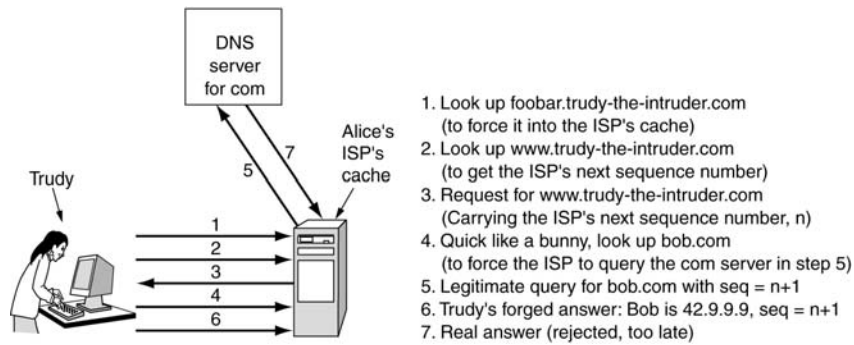
Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

6

Secure Naming

How Trudy spoofs Alice's ISP.



Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

7

Secure Naming

- # **DNSsec (DNS security):** based on public-key cryptography. Every DNS zone has a public/private key pair
 - All information sent by a DNS server is signed with the originating zone's private key, so the receiver can verify its authenticity
- # DNSsec offers three fundamental services:
 - Proof of where the data originated: verifies that the data being returned has been approved by the zone's owner
 - Public key distribution: storing and retrieving public keys securely
 - Transaction and request authentication: guards against playback and spoofing attacks
- # Secrecy is not an offered service since all the information in DNS is considered public

Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

8

Secure Naming

- # DNS records are grouped into sets called **RRSets (Resource Record Sets)**, with all the records having the same name, class and type being lumped together in a set.
- # An RRSet may contain multiple *A* records, for example, if a DNS name resolves to a primary IP address and a secondary IP address
- # Each RRSet is cryptographically hashed (e.g., using MD5 or SHA-1). The hash is signed by the zone's private key (e.g., using RSA).
- # The unit of transmission to clients is the signed RRSet.

Secure Naming

- # Upon receipt of a signed **RRSet**, the client can verify whether it was signed by the private key of the originating zone. If the signature agrees, the data are accepted.
- # Since each **RRSet** contains its own signature, RRsets can be cached anywhere, even at untrustworthy servers, without endangering the security

Secure DNS

- # The **RRSets** are extended with several new record types
 - **KEY record**: holds the public key and other info
 - **SIG record**: holds the signed hash according to the algorithm specified in the *KEY* record
 - **CERT record**: can be used for storing (e.g., X.509) certificates

Domain name	Time to live	Class	Type	Value
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7B73F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A8B848F5272E53930C...

Secure DNS

- # **KEY record**:
 - The public key of a zone, user, host, or other principal
 - The public key is stored as plaintext
 - The cryptographic algorithm used for signing
 - The protocol used for transmission, and a few other bits
 - The algorithm field holds a 1 for MD5/RSA signatures (the preferred choice), and other values for other combinations
 - The protocol field can indicate the use of IPsec or other security protocols, if any

Secure DNS

- # **SIG record**: holds the signed hash according to the algorithm specified in the *KEY* record
 - The signature applies to all the records in the RRSet, including any *KEY* records present, but excluding itself
 - It also holds the times when the signature begins its period of validity and when it expires, as well as the signer's name and a few other items
- # In practice, it is expected that **clients will be preconfigured with the public keys of all the top-level domains**

Self-Certifying Names

- # **Self-certifying URL**: The essence of the idea is that each URL contains a cryptographic hash of the server's name and public key as part of the URL
 - The hash is computed by concatenating the DNS name of the server with the server's public key and running the result through the SHA-1 function to get a 160-bit hash
 - A string of 32 characters can hold the 160-bit SHA-1 hash

Server SHA-1 (Server, Server's Public key) File name

http://www.bob.com:2g5hd8bfjkc7mf6hg8dgany23xds4pe6/photos/bob.jpg

SSL—The Secure Sockets Layer

- # **SSL (Secure Sockets Layer):** a security package for secure communication over Internet. It is widely used
 - Introduced in 1995, Netscape Communications Corp
- # SSL builds a secure connection between two sockets, including
 - Parameter negotiation between client and server.
 - Mutual authentication of client and server.
 - Secret communication.
 - Data integrity protection.

SSL—The Secure Sockets Layer

- # **HTTPS (Secure HTTP):** HTTP over SSL
 - Sometimes it is available at a new port (443) instead of the standard port (80)
- # Layers (and protocols) for home user using HTTPS

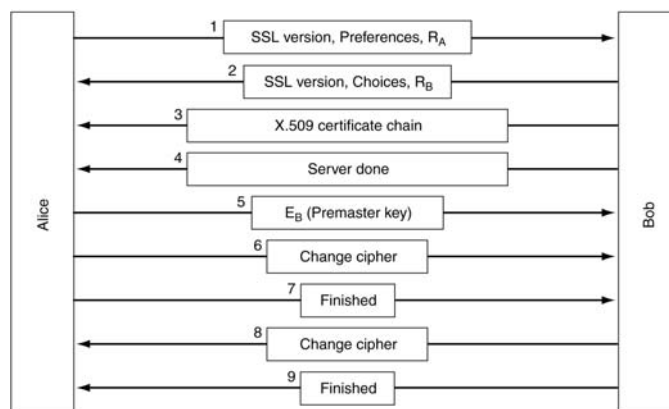
Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

SSL—The Secure Sockets Layer

- # SSL consists of two subprotocols, one for establishing a secure connection and one for using it
- # SSL supports multiple cryptographic algorithms
 - The strongest one uses triple DES with three separate keys for encryption and SHA-1 for message integrity
 - This combination is mostly used for banking and other applications in which the highest security is required
 - For ordinary e-commerce applications, RC4 is used with a 128-bit key for encryption and MD5 is used for message authentication

SSL

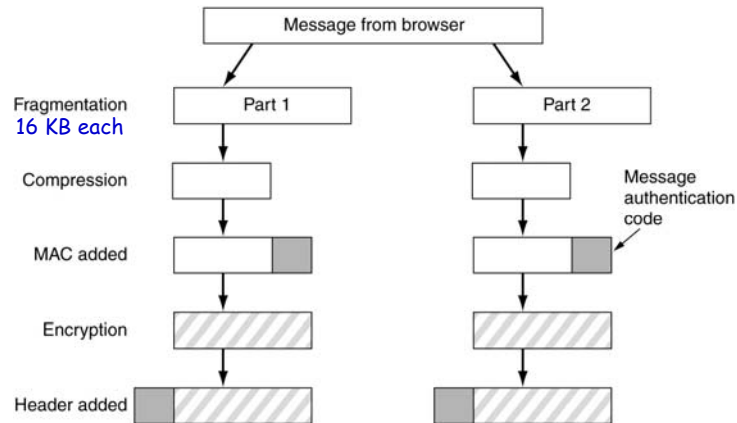
- # SSL **connection establishment subprotocol**
 - key used for encrypting data is derived from the **premaster** key combined with **both nonces** in a complex way



SSL

Data transmission using SSL

- MAC: a secret key derived from the two nonces and premaster key is concatenated with the compressed text and the result hashed with the agreed-on hashing algorithm



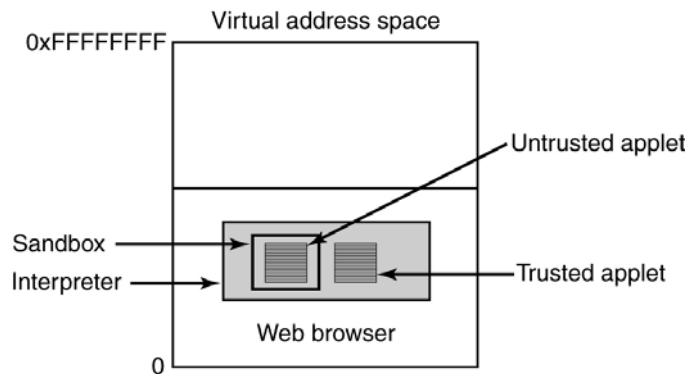
SSL and TLS

In 1996, Netscape Communications Corp. turned SSL over to IETF for standardization. The result was **TLS (Transport Layer Security)**

- It is described in RFC 2246.
- The changes made to SSL were relatively small, but just enough that SSL version 3 and TLS cannot interoperate
- The TLS version is also known as SSL version 3.1

Java Applet Security

- # Applets inserted into a Java Virtual Machine interpreter inside the browser



ActiveX Security

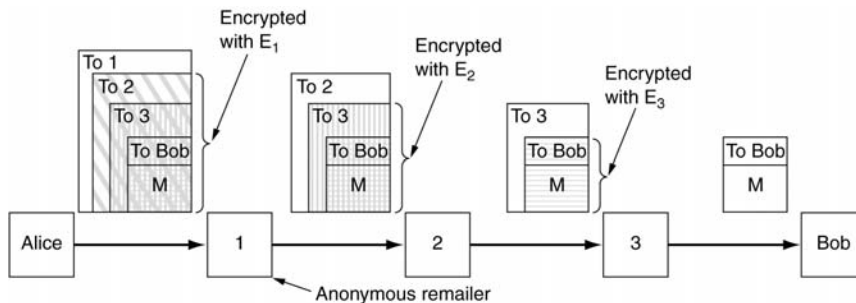
- # **ActiveX**: Win32 programs that can be embedded into Web pages. Its security is based on code signing
 - **Code signing**: Each ActiveX control is accompanied by a digital signature—a hash of the code that is signed by its creator using public key cryptography.
 - When an ActiveX control shows up, the browser first verifies the signature to make sure it has not been tampered with in transit.
 - If the signature is correct, the browser then checks its internal tables to see if the program's creator is trusted or there is a chain of trust back to a trusted creator
 - Users got to choose whether to enable trusted ActiveX or not
 - Once an ActiveX program is enabled, it can do anything it wants

Social Issues

- # Privacy
- # Freedom of Speech
- # Copyright

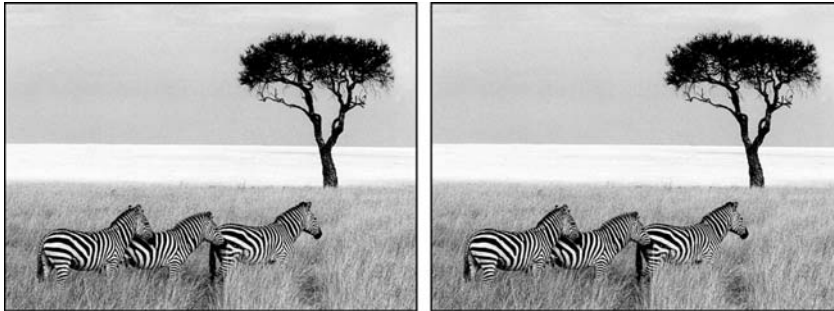
Anonymous Remailers

- # Users who wish anonymity chain requests through multiple anonymous remailers



Steganography

- # The science of hiding messages is called **steganography**
 - From the Greek words for "covered writing"
 - (a) Three zebras and a tree. (b) Three zebras, a tree, and the complete text of five plays by William Shakespeare



Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

25

Steganography

- # How does this **steganographic** channel work?
 - The original color image is 1024 x 768 pixels. Each pixel consists of three 8-bit numbers, one each for the red, green, and blue intensity of that pixel.
 - The pixel's color is formed by the linear superposition of the three colors.
 - The steganographic encoding method uses the low-order bit of each RGB color value as a covert channel.
 - Thus, each pixel has room for 3 bits of secret information, one in the red value, one in the green value, and one in the blue value.
 - With an image of this size, up to 1024 x 768 x 3 bits or 294,912 bytes of secret information can be stored in it

Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

26

Review of Chapters 7 & 8

Application layer

- DNS, Email, HTTP, Multimedia

Network security

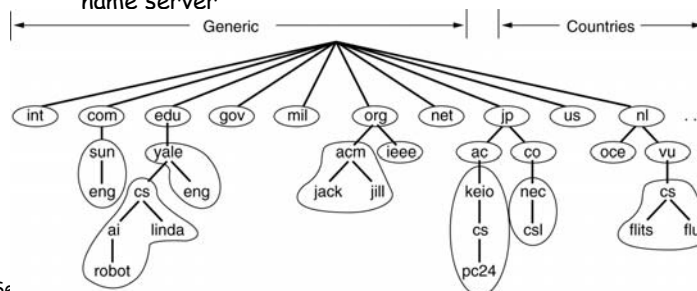
- Symmetric-key algorithms, cipher modes
- Public-key algorithms, digital signatures, message digest, public key management
- Communications security (IPsec, firewall, VPN, 802.11 security)
- Authentication protocols, PGP, SSL

DNS - The Domain Name System

- # Hierarchical domain-based naming scheme and distributed database system for implementing it
- # Maps ASCII strings to network addresses, i.e., maps hostnames and email addresses to IP addresses
- # Application program calls library procedure
 - Resolver whose input is name, output is IP address
 - Resolver sends UDP packet to local DNS server
 - Local DNS server looks up name, returns IP address to resolver
 - Resolver returns IP address to caller

Name Servers

- # DNS name space divided into non-overlapping zones
- # Each zone contains
 - Part of tree and
 - Name server holding info about zone
 - One primary name server gets its info off disk
 - One or more non-primary name servers get info from primary name server

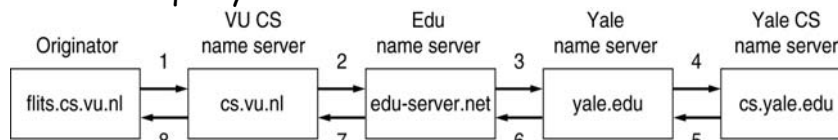


Spring Se

29

Name Servers

- # When resolver has query about domain names, it passes query to one of local name servers
- # If domain is in jurisdiction of name server, it returns resource record
- # If domain is remote, name server sends query message to top-level name server for domain requested using recursive query



Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

30

HyperText Transfer Protocol

- # HTTP - HyperText Transfer Protocol
 - It specifies what messages clients may send to servers and what responses they get back in return.
 - Each interaction consists of one ASCII request, followed by one EFC 822 MIME-like response
 - Defined in RFC 2616
- # HTTP
 - Connection
 - In HTTP 1.0: make connection, sends a request, gets a response, tears down connection
 - In HTTP 2.0: connection can be reused
 - Methods: had some provision for object-oriented programming
 - Message header

HTTP Methods

- # The built-in HTTP request methods

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

HTTP Message Headers

Header	Type	Contents
User-Agent	Request	Information about the browser and its platform
Accept	Request	The type of pages the client can handle
Accept-Charset	Request	The character sets that are acceptable to the client
Accept-Encoding	Request	The page encodings the client can handle
Accept-Language	Request	The natural languages the client can handle
Host	Request	The server's DNS name
Authorization	Request	A list of the client's credentials
Cookie	Request	Sends a previously set cookie back to the server
Date	Both	Date and time the message was sent
Upgrade	Both	The protocol the sender wants to switch to
Server	Response	Information about the server
Content-Encoding	Response	How the content is encoded (e.g., gzip)
Content-Language	Response	The natural language used in the page
Content-Length	Response	The page's length in bytes
Content-Type	Response	The page's MIME type
Last-Modified	Response	Time and date the page was last changed
Location	Response	A command to the client to send its request elsewhere
Accept-Ranges	Response	The server will accept byte range requests
Set-Cookie	Response	The server wants the client to save a cookie

Performance Enhancement

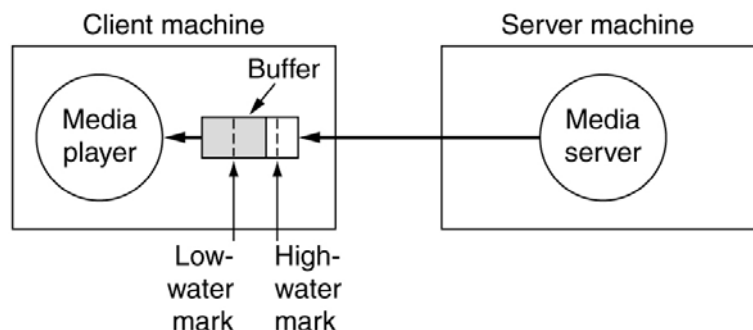
- # Caching
 - Save pages that have been requested in case they are used again
 - Client-side technique
- # Server replication
 - Replicate server's contents at multiple locations
 - Sometimes called mirroring
- # Content delivery networks
 - Deliver contents for their providers to end users efficiently for a fee
 - Whole process starts with URL replacement so all contents point to a CDN server
 - On receiving client's request, the request is redirected to the closest proxy server

Audio Compression

- # Two ways to do audio compression
 - **Waveform coding:** the signal is transformed mathematically by a Fourier transform into its frequency components.
 - The amplitude of each component is then encoded in a minimal way.
 - The goal is to reproduce the waveform accurately at the other end in as few bits as possible
 - **Perceptual coding:** exploits certain flaws in the human auditory system to encode a signal in such a way that it sounds the same to a human listener, even if it looks quite different on an oscilloscope
 - Some sounds can mask other sounds
 - **Frequency masking:** a loud sound in one frequency band can hide a softer sound in another frequency band
 - **Temporal masking:** it takes the human ear a brief period of time to hear the masked signal even after the masking signal goes away
 - MP3 (MPEG audio layer 3) is based on perceptual coding

Streaming Audio

- # The media player buffers input from the media server and plays from the buffer rather than directly from the network.



The MPEG Standard

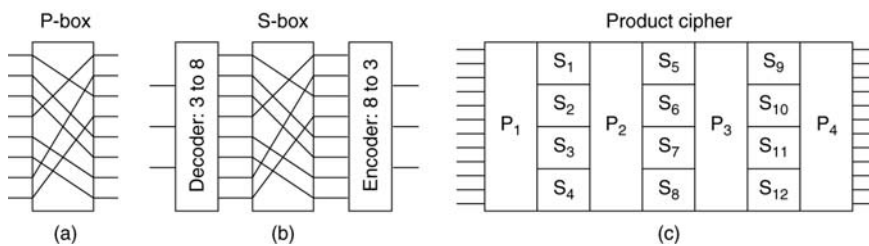
- # MPEG - Motion Picture Experts Group
- # MPEG-1: to produce video-recorder-quality output
 - 352x240 for NTSC, bit rate of 1.2 Mbps
 - 352x240 image with 24 bits/pixel and 25 frames/sec requires 50.7 Mbps. We need a factor of 40 compression
- # MPEG-2: designed for compressing broadcast-quality video into 4 to 6 Mbps. Later, MPEG-2 was expanded to support higher resolution, including HDTV
 - It forms the basis for DVD and digital satellite television

The MPEG Standard

- # MPEG-1 output consists of four kinds of frames
 - I (Intracoded) frames: self-contained JPEG-encoded still pictures
 - P (Predictive) frames: block-by-block difference with the last frame
 - B (Bidirectional) frames: differences between the last and next frame
 - D (DC-coded) frames: block averages used for fast forward

Data Encryption Standard

- # Developed by IBM. US standard for unclassified info (1977)
- # P-box (permutation box) used to implement transposition in hardware
- # S-box (substitution box) used to implement substitution in hardware



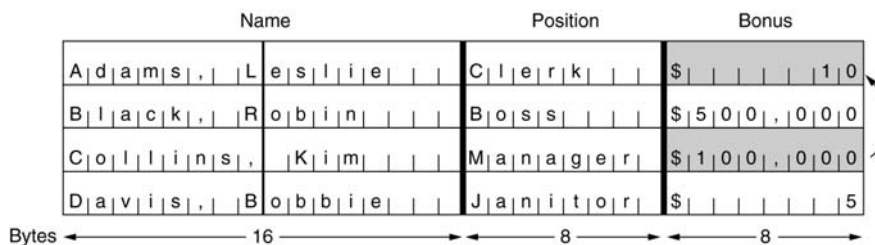
Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

39

Electronic Code Book Mode

- # The plaintext of a file encrypted as 16 DES blocks
 - One can make a copy of a block that contains a bigger bonus and replace the block that contains a smaller bonus



Spring Semester 2005

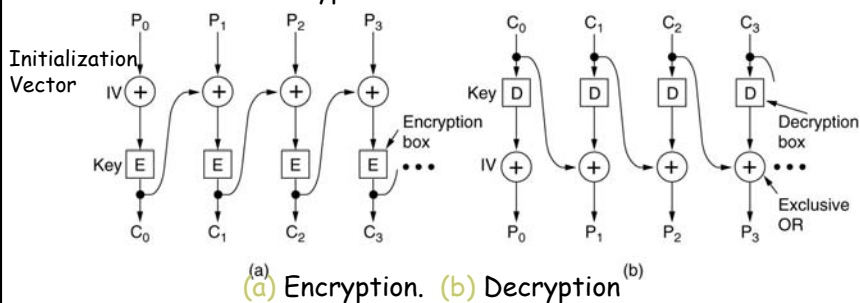
EEC-682: Computer Networks I
- Wenbing Zhao

40

Cipher Block Chaining Mode

To avoid the ECB mode problem: replacing a block will cause the plaintext decrypted starting at the replaced to be garbage

- Exclusive OR the encrypted text with the next block of plaintext before encryption: $C_0 = E(P_0 \text{ XOR } IV)$, $C_1 = E(P_1 \text{ XOR } C_0)$, etc.
- **Drawback:** must wait until full 64-bit (128-bit) block to arrive to decrypt

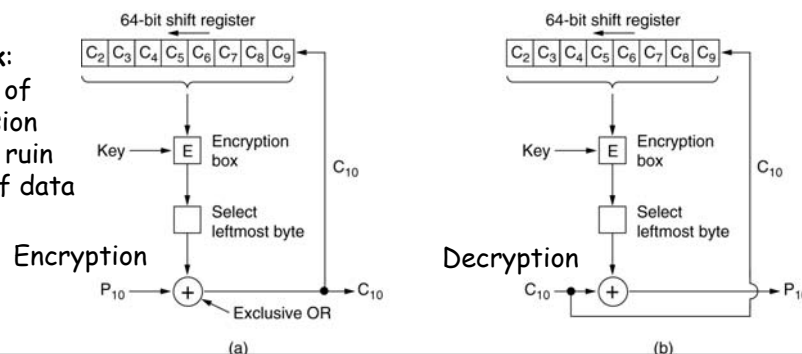


Cipher Feedback Mode

To enable byte-by-byte encryption

- When plaintext byte 10 (P_{10}) arrives, DES algo. operates a 64-bit register to generate a 64-bit ciphertext (128-bit register needed for AES)
- Leftmost byte of that ciphertext is extracted and XORed with P_{10}
- That byte is transmitted on the transmission line
- The shift register is shifted left 8 bits, causing C_2 to fall off the left end, and C_{10} is inserted in the position just vacated at the right end by C_9

Drawback:
One byte of transmission error will ruin 8 bytes of data

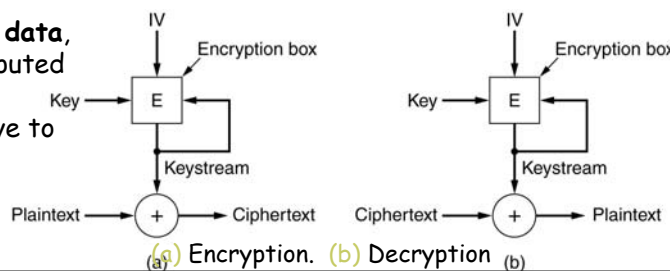


Stream Cipher Mode

To be insensitive to transmission error, an arbitrarily large sequence of output blocks, called the **keystream**, is treated like a one-time pad and XORed with the plaintext to get the ciphertext

- It works by encrypting an IV, using a key to get an output block.
- The output block is then encrypted, using the key to get a second output block.
- This block is then encrypted to get a third block, and so on.

The keystream is independent of the data, so (1) It can be computed in advance (2) It is completely insensitive to transmission errors

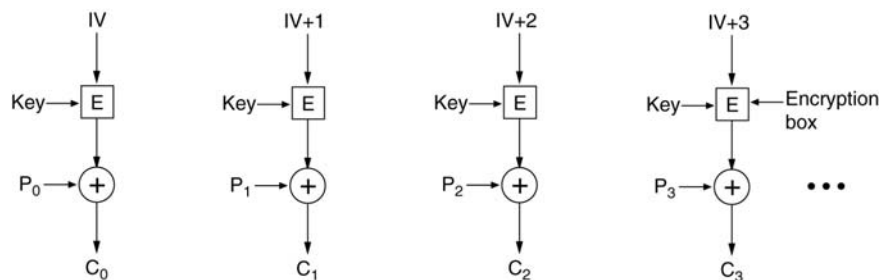


Stream Cipher Mode

- # It is essential never to use the same (key, IV) pair twice with a stream cipher because doing so will generate the same keystream each time.
- # Using the same keystream twice exposes the ciphertext to a **keystream reuse attack**.
 - Plaintext block, P_0 , is encrypted with the keystream to get $P_0 \text{ XOR } K_0$.
 - Later, a second plaintext block, Q_0 , is encrypted with the same keystream to get $Q_0 \text{ XOR } K_0$.
 - An intruder who captures both ciphertext blocks can simply XOR them together to get $P_0 \text{ XOR } Q_0$, which eliminates the key.
 - The intruder now has the XOR of the two plaintext blocks.
 - If one of them is known or can be guessed, the other can also be found.
 - In any event, the XOR of two plaintext streams can be attacked by using statistical properties of the message.
 - For example, for English text, the most common character in the stream will probably be the XOR of two spaces, followed by the XOR of space and the letter 'e', etc.

Counter Mode

- # To allow random access to encrypted data
 - The IV plus a constant is encrypted, and the resulting ciphertext XORed with the plaintext
 - By stepping the IV by 1 for each new block, it is easy to decrypt a block anywhere in the file without first having to decrypt all of its predecessors



Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

45

RSA

- # **Rivest, Shamir, Adleman**, 1978: a good method for public-key cryptography
- # RSA method:
 - Choose two large primes, p and q (typically 1024 bits)
 - Compute $n = p \times q$ and $z = (p-1) \times (q-1)$
 - Choose a number relatively prime to z and call it d
 - Find e such that $e \times d = 1 \pmod{z}$
- # To encrypt a message, P , Compute $C = P^e \pmod{n}$
- # To decrypt C , compute $P = C^d \pmod{n}$
- # The public key consists of the pair (e, n)
- # The private key consists of the pair (d, n)

Spring Semester 2005

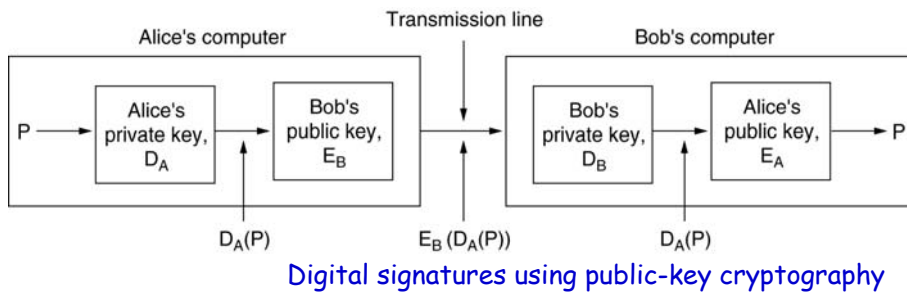
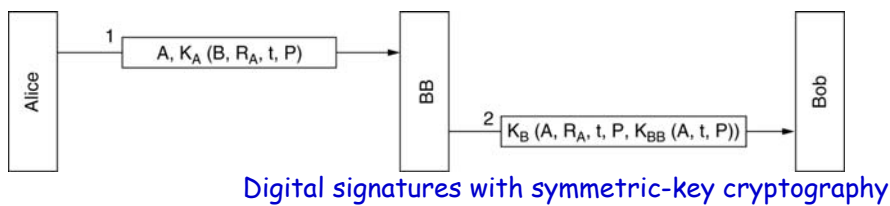
EEC-682: Computer Networks I
- Wenbing Zhao

46

Digital Signatures

- # Requirement on **digital signatures**: one party can send a signed message to another party in such a way that the following conditions hold:
- The receiver can verify the claimed identity of the sender.
 - The sender cannot later repudiate the contents of the message
 - The receiver cannot possibly have concocted the message himself

Digital Signatures

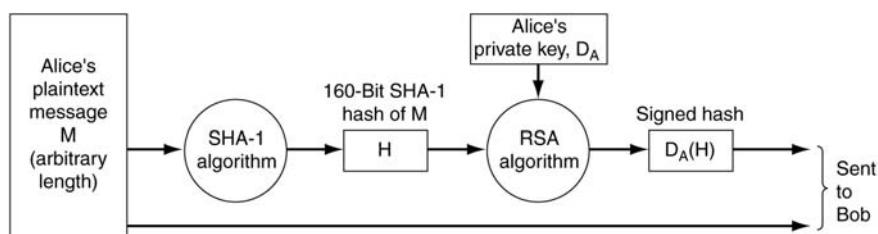


Message Digests

- # Often, authentication is needed but secrecy is not
- # **Message digest (MD)**: using a one-way hash function that takes an arbitrarily long piece of plaintext and from it computes a fixed-length bit string
 - Given P , it is easy to compute $MD(P)$
 - Given $MD(P)$, it is effectively impossible to find P
 - Given P no one can find P' such that $MD(P') = MD(P)$
 - A change to the input of even 1 bit produces a very different output

Message Digests

- # **MD5** is the fifth in a series of message digests designed by Ronald Rivest (1992). MD5 generates a 128-bit fixed value
- # **SHA-1: Secure Hash Algorithm 1**, developed by National Security Agency (NSA) and blessed by NIST. It generates 160-bit message digest

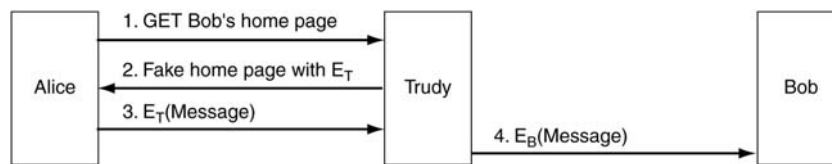


Problems with Public-Key Management

If Alice and Bob do not know each other, how do they get each other's public keys to start the communication process ?

- It is essential Alice gets Bob's public key, not someone else's

A way for Trudy to subvert public-key encryption



Certificates

Certification Authority (CA): an organization that certifies public keys

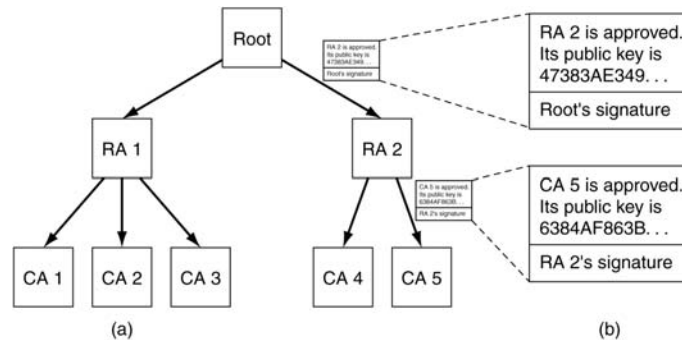
- It certifies the public keys belonging to people, companies, or even attributes
- CA does not need to be on-line all the time

A possible certificate and its signed hash

<p>I hereby certify that the public key 19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A belongs to Robert John Smith 12345 University Avenue Berkeley, CA 94702 Birthday: July 4, 1958 Email: bob@superdupernet.com</p>
<p>SHA-1 hash of the above certificate signed with the CA's private key</p>

Public-Key Infrastructures

- # Hierarchical PKI
- # A **chain of trust/certification path**:
A chain of certificates going back to the root



Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

53

Public-Key Infrastructures

- # **Revocation**: sometimes certificates can be revoked, due to a number of reasons
 - Person or organization holding it has abused it in some way
 - The subject's private key has been exposed
 - The CA's private key has been compromised
- # **Reinstatement**: a revoked certificate could conceivably be reinstated
 - E.g., if it was revoked for nonpayment of some fee that has since been paid
- # Each CA periodically issue a **CRL (Certificate Revocation List)** giving the serial numbers of all certificates that it has revoked
 - A user who is about to use a certificate must now acquire the CRL to see if the certificate has been revoked

Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

54

IPsec

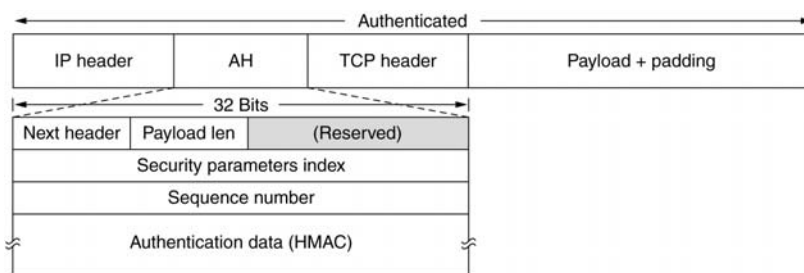
- # **IPsec (IP security):** a solution for Internet security
- # The complete IPsec design is a framework for multiple services, algorithms and granularities.
 - The major services are **secrecy, data integrity, and protection from replay attacks** (intruder replays a conversation).
 - All of these are based on **symmetric-key cryptography** because high performance is crucial.

IPsec

- # **Security Association (SA):** A simplex connection between two end points and has a security identifier associated with it.
 - If secure traffic is needed in both directions, two security associations are required.
 - **Security identifiers** are carried in packets traveling on these secure connections and are used to look up keys and other relevant
- # IPsec can be used in either of two modes
 - Transport mode
 - Tunnel mode

IPsec

- # **AH (Authentication Header)**: It provides integrity checking and anti-replay security, but not secrecy (i.e., no data encryption)

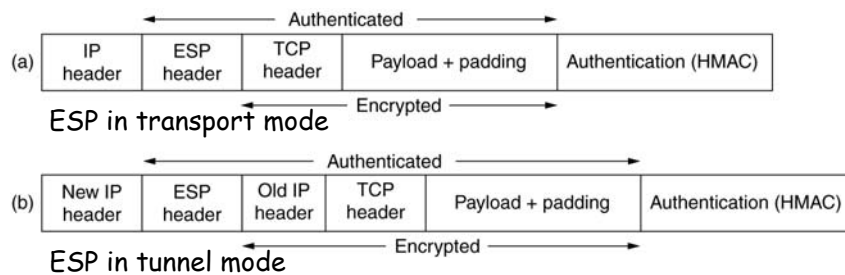


IPsec - AH header

- # The **Sequence number** field is used to number all the packets sent on an SA. **Every packet gets a unique number, even retransmissions.**
 - The purpose of this field is to detect **replay attacks**.
 - These sequence numbers may not wrap around. If all 2^{32} are exhausted, a new SA must be established to continue communication.
- # The **Authentication data**, which is a variable-length field that contains the payload's digital signature
 - When the SA is established, the two sides negotiate which signature algorithm they are going to use and the shared key to use
 - **HMAC (Hashed Message Authentication Code)**: Compute the hash over the packet plus the shared key. The shared key is not transmitted.
 - The integrity check covers some of the fields in the IP header, namely, those that do not change as the packet moves from router to router

IPsec - ESP Header

- # **ESP (Encapsulating Security Payload):** provides both authentication and confidentiality guarantee for packets. Can be used for both transport mode and tunnel mode



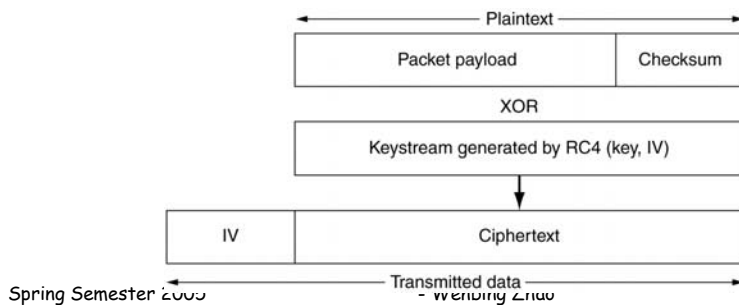
802.11 Security

- # **WEP (Wired Equivalent Privacy):** a data link-level security protocol prescribed by 802.11 standard
 - It is designed to make the security of a wireless LAN as good as that of a wired LAN
- # When 802.11 security is enabled, each station has a secret key shared with the base station
 - WEP encryption uses a stream cipher based on the **RC4** algorithm
 - In WEP, RC4 generates a keystream that is XORed with the plaintext to form the ciphertext

802.11 Security

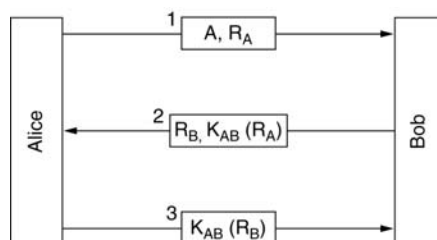
Packet encryption using WEP

- Payload is checksummed using CRC-32 polynomial
- Checksum is appended to the payload to form the plaintext
- This plaintext is XORed with a chunk of keystream its own size. The result is the ciphertext
- The IV used to start RC4 is sent along with the ciphertext



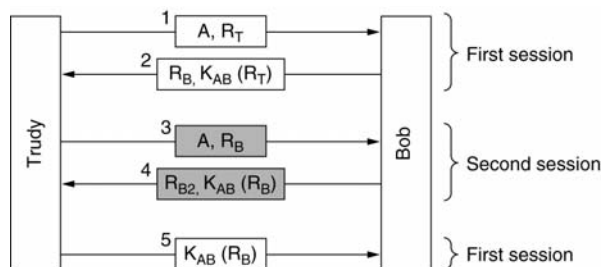
Authentication Based on a Shared Secret Key

- # A shortened two-way authentication protocol. Is this new protocol an improvement over the original one?
 - In one sense it is: it is shorter.
 - Unfortunately, it is also wrong. Under certain circumstances, Trudy can defeat this protocol by using what is known as a **reflection attack**



Authentication Based on a Shared Secret Key

- # **The reflection attack:** Trudy can break it if it is possible to open multiple sessions with Bob at once
 - This attack can be defeated by encrypting R_B with K_{AB} in message 2



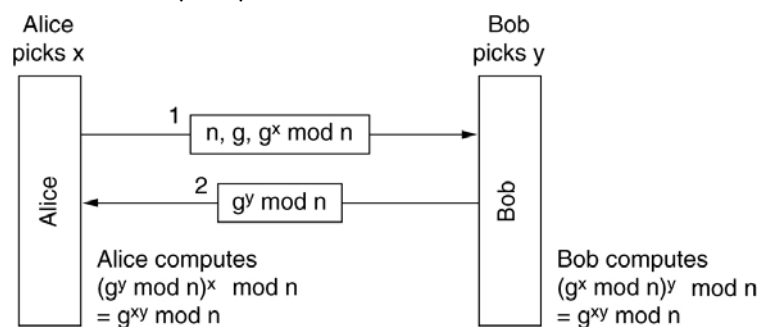
Spring Semester 2005

EEC-682: Computer Networks I
- Wenbing Zhao

63

Establishing a Shared Key: The Diffie-Hellman Key Exchange

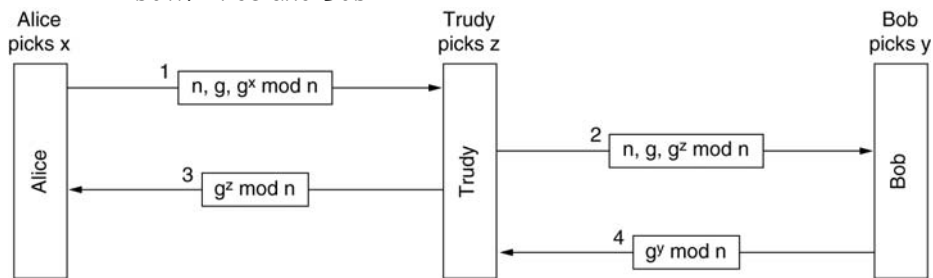
- # **Diffie-Hellman key exchange:** protocol that allows strangers to establish a shared secret key
 - Two large numbers, n and g , where n is a prime, $(n-1)/2$ is also a prime and certain conditions apply to g . These numbers may be public



Establishing a Shared Key: The Diffie-Hellman Key Exchange

The **bucket brigade** or **man-in-the-middle attack**

- When Bob gets the triple (47, 3, 28), how does he know it is from Alice and not from Trudy? There is no way he can know. Unfortunately, Trudy can exploit this fact to deceive both Alice and Bob



Spring Semester 2005

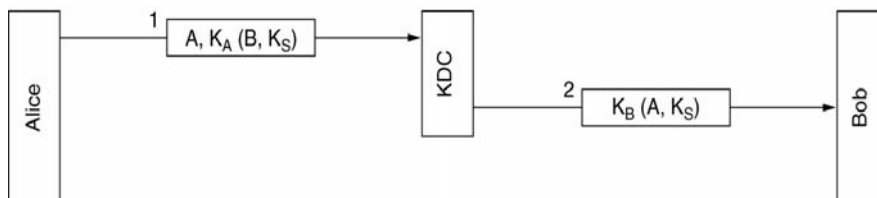
EEC-682: Computer Networks I
- Wenbing Zhao

65

Authentication Using a Key Distribution Center

- # Each user has a single key shared with the KDC. Authentication and session key management now goes through the KDC

- # The following protocol is subject to **replay attack**



Spring Semester 2005

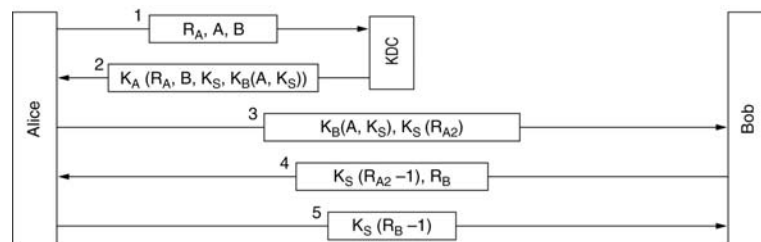
EEC-682: Computer Networks I
- Wenbing Zhao

66

Authentication Using a Key Distribution Center

Needham-Schroeder authentication protocol: a multiway challenge-response protocol

- By having each party both generate a challenge and respond to one, the possibility of any kind of replay attack is eliminated

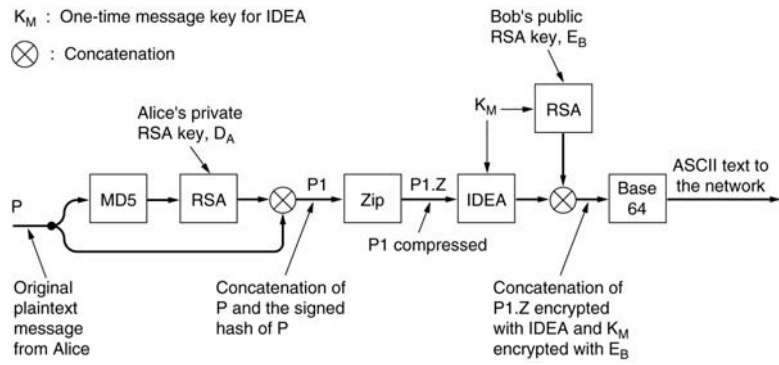


General Rules for Authentication Protocols Design

- # Have the initiator prove who she is before the responder has to. In this case, Bob gives away valuable information before Trudy has to give any evidence of who she is
- # Have the initiator and responder use different keys for proof, even if this means having two shared keys, K_{AB} and K'_{AB}
- # Have the initiator and responder draw their challenges from different sets. For example, the initiator must use even numbers and the responder must use odd numbers
- # Make the protocol resistant to attacks involving a second parallel session in which information obtained in one session is used in a different one

PGP - Pretty Good Privacy

PGP in operation for sending a message



Spring Semester 2005

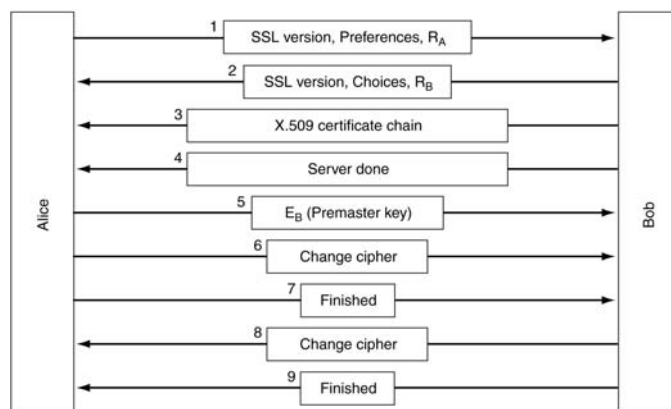
EEC-682: Computer Networks I
- Wenbing Zhao

69

SSL

SSL connection establishment subprotocol

- key used for encrypting data is derived from the **premaster** key combined with **both nonces** in a complex way



SSL

Data transmission using SSL

- MAC: a secret key derived from the two nonces and premaster key is concatenated with the compressed text and the result hashed with the agreed-on hashing algorithm

