



EEC-484/584 Computer Networks

Lecture 22

Wenbing Zhao
wenbing@ieee.org

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



Outline

- Review of last lecture
 - Multimedia
- Today's topics
 - Introduction to network security
 - Symmetric-key algorithms



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 RFC 822 MIME-like response
- HTTP
 - Connection (HTTP 1.0/1.1/2.0)
 - Methods: had some provision for object-oriented programming. Method names are case sensitive!
 - Message header



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

Multimedia

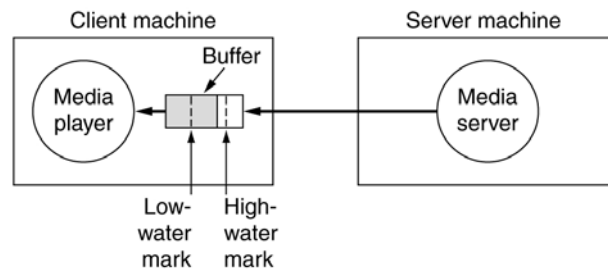
- Introduction to Audio
- Audio Compression
- Streaming Audio
- Internet Radio
- Voice over IP
- Introduction to Video
- Video Compression
- Video on Demand
- The MBone – The Multicast Backbone

Audio Compression

- Two ways to do audio compression
 - **Waveform coding:** the signal is transformed mathematically by a Fourier transform into its frequency components.
 - **Perceptual coding:** based on the science of **psychoacoustics** (how people perceive sound)
 - **Frequency masking** and **temporal masking**
 - MP3 (MPEG audio layer 3) is based on perceptual coding

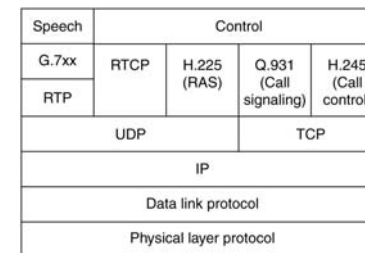
Streaming Audio

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



Voice over IP

The H323 protocol stack.



Video Compression

- Requirements on encoding and decoding
 - Decoding happens a lot and it must be fast
 - For most of video documents, it is OK if the encoding algorithm is complex and time consuming
 - For real-time multimedia, encoding must also be fast and efficient
 - Encode/decode process need not be invertible
- A video is just a sequence of images plus sound
 - A good algorithm for encoding a single image is a good starting point. When the decoded output is not exactly the same as original input, the system is said to be **lossy**
 - **JPEG** – Joint Photographic Experts Group

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

Network Security

- Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone
- Network security problems can be divided roughly into four closely intertwined areas
 - Secrecy (confidentiality)
 - Authentication
 - Nonrepudiation
 - Integrity control

Need for Security

- Some people who cause security problems and why

Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by e-mail
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

Cryptography

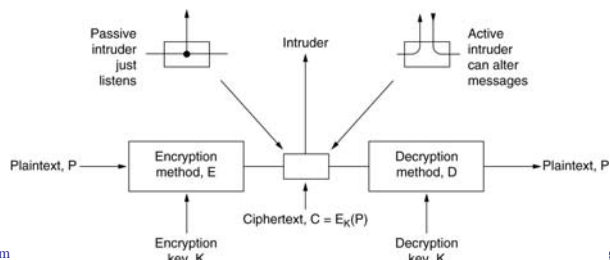
- Introduction to Cryptography
- Substitution Ciphers
- Transposition Ciphers
- One-Time Pads
- Two Fundamental Cryptographic Principles

Cryptography

- **Cryptography**: comes from Greek words for “secret writing”
- **Cipher**: a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message
- **Code**: a code replaces one word with another word or symbol. Codes are not used any more
- **Cryptology**
 - **Cryptography** – art of devising ciphers
 - **Cryptanalysis** – art of breaking ciphers

An Introduction to Cryptography

- **Plaintext**: message to be encrypted
- **Key**: string of characters used to encrypt the message
- **Ciphertext**: encrypted message
- $D_K(E_K(P)) = P$



Introduction to Cryptography

- **Kerckhoff's principle**: all algorithms must be public; only the keys are secret
 - Security by obscurity: keep the algorithm secret
- Since the real secrecy is in the key, its length is a major design issue
 - The longer the key, the higher the work factor the cryptanalyst has to deal with
 - The work factor for breaking the system by exhaustive search of the key space is exponential in the key length

Introduction to Cryptography

- Cryptanalysis problems
 - **Ciphertext-only**: cryptanalyst has a quantity of ciphertext and no plaintext
 - **Known plaintext**: cryptanalyst has some matched ciphertext and plaintext
 - **Chosen plaintext**: cryptanalyst has the ability to encrypt pieces of plaintext of his own choosing
- Encryption methods
 - **Substitution** ciphers
 - **Transposition** ciphers

Substitution Ciphers

- Idea: each letter or group of letters is replaced by another letter or group of letters
- Caesar cipher – circularly shift by 3 letters
 - a -> D, b -> E, ... z -> C
 - More generally, shift by k letters, k is the key
- Monoalphabetic cipher – map each letter to some other letter
 - A b c d e f ... w x y z
 - Q W E R T Y ... V B N M <= the key

Substitution Ciphers

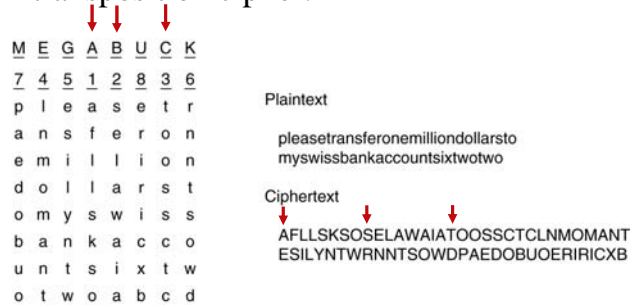
- Not difficult to determine the key using frequencies of letters, pairs of letter etc., or by guessing a probable word or phrase
- Most frequently occurred
 - Letters: e, t, o, a, n, ...
 - Digrams: th, in, er, re, an, ...
 - Trigrams: the, ing, and, ion, ent
 - Words: the, of, and, to, a, in, that, ...

Transposition Ciphers

- Substitution cipher – preserves order of plaintext symbols but disguises them
- Transposition cipher – reorders symbols but does not disguise them
- Columnar transposition
 - Plaintext written in rows, number of columns = key length
 - Key is used to number the columns
 - Column 1 corresponds to key letter
 - Closest to start of alphabet
 - Ciphertext read out by columns, starting with column whose key letter is lowest

Transposition Ciphers

- A transposition cipher.



One-Time Pads

- One-time pad: way to construct an unbreakable cipher
 - > Choose a random bit string as the key
 - > Convert the plaintext into a bit string
 - > Compute the XOR of these two strings, bit by bit
 - > The resulting ciphertext cannot be broken, because in a sufficiently large sample of ciphertext, each letter will occur equally often, as will every digram, every trigram, and so on,
 - > => there is simply no information in the message because all possible plaintexts of the given length are equally likely

One-Time Pads

I love you

Message 1: 1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
 Pad 1: 1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
 Ciphertext: 0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101

Pad 2: 1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
 Plaintext 2: 1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011
 Elvis lives

The use of a one-time pad for encryption and the possibility of getting any possible plaintext from the ciphertext by the use of some other pad

One-Time Pads

- Disadvantages
 - > The key cannot be memorized, both sender and receiver must carry a written copy with them
 - > Total amount of data can be transmitted is limited by the amount of key available
 - > Sensitive to lost or inserted characters

Quantum Cryptography

- Background knowledge
 - Light comes in **photons**
 - Light can be **polarized**. If a beam of light is passed through a polarizing filter, all photons emerging from it will be polarized in the direction of the filter's axis
 - **Rectilinear basis**: one vertical filter and horizontal filter
 - **Diagonal basis**: rectilinear basis rotated by 45 degree
 - If a photon hits a filter polarized at 45 degrees to its own polarization, it randomly jumps to the polarization of the filter or to a polarization perpendicular to the filter with equal probability
 - Bits sent one photon at a time are called **qubits**

Quantum Cryptography

- Alice want to establish a one-time pad with Bob
 - Alice and Bob are called principals
- Alice picks a one-time pad and transfers it bit by bit to Bob, choosing one of her two bases at random for each bit
 - To send a bit, her photon gun emits one photon polarized appropriately for the basis she is using for that bit
 - Given the one-time pad and the sequence of bases, the polarization to use for each bit is uniquely determined

Quantum Cryptography

- Bob picks a basis at random for each arriving photon and just uses it
 - If he picks the correct basis, he gets the correct bit
 - If he picks the incorrect basis, he gets a random bit
- Bob tells Alice which basis he used for each bit in plaintext and she tells him which are right and which are wrong in plaintext
 - Both can build a bit string from the correct guesses
 - On average, this bit string will be half the length of the original bit string

Quantum Cryptography

Bit number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Data	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1	0
(a) What Alice sends	↘	↑	↑	↘	↘	↘	↘	↘	↑	↘	↘	↘	↘	↘	↘	↑
(b) Bob's bases	+	+	×	×	×	+	+	×	+	+	×	×	×	×	+	×
(c) What Bob gets	↑	↑	↘	↘	↘	↑	↘	↘	↘	↘	↘	↘	↘	↘	↘	↘
(d) Correct basis?	No	Yes	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	No	Yes	No
(e) One-time pad	0		1					0	1		1	0	0		1	
(f) Trudy's bases	×	+	+	×	+	+	+	×	+	+	×	×	+	×	×	×
(g) Trudy's pad	x	0	x	1	x	x	x	?	1	x	?	?	0	x	?	x

Quantum Cryptography

- Trudy – intruder overhearing Alice and Bob’s conversion
 - She has to randomly pick one basis for each bit
 - She may find out which bit forms the actual one-time pad
 - She may know some of her guess is right
 - But on average, half of the bits she guessed wrong and there is no way for her to find out the correct bit values

Quantum Cryptography

- Privacy amplification
 - Alice and Bob can perform a transformation on the agreed-upon one-time pad, for example, square every 1024 bit block to form a 2048-bit number
 - With partial knowledge, Trudy has no way to generate its square

Two Fundamental Cryptographic Principles

- Principle 1: messages must contain some redundancy
 - Consider an example, an order message consists of a customer name and 1-byte on quantity, and 2-bytes on product id
 - If only the last 3 bytes are encrypted, a disgruntled ex-employ could steal the customer list and fabricate order messages, without knowing the key => any 3 bytes are legal
 - Need redundant info in the encrypted message, e.g., a few extra bytes for CRC or even a few bytes of 0
- Principle 2: some method is needed to foil replay attacks