CompSci 314 S2 C
Modern Data Communications

Revision of lectures #2 to #11

Clark Thomborson

12 August 2010

Three Layers of Understanding

1. Terms, such as digital, analog, bit, signal, code; SI prefixes.
   - All terms used in the lecture slides are examinable.
   - You must be able to understand questions that are expressed in these terms.
   - You must be able to use these terms, accurately, in your responses.
   - You may be asked to define a term.
2. Concepts, such as information, bandwidth, compression.
   - All concepts discussed in the lecture slides are examinable.
   - You must have a "working understanding" of these concepts to get a B in this class.
3. Analyses, such as Fourier analysis, Shannon capacity.
   - All analyses illustrated in the lecture slides are examinable.
   - You will get an A on my portion of the exam if you are able to perform analyses under examination conditions, and if you are able to express your results in the appropriate terms.

Important Concepts

- Bits (information), signals (analog encodings of information), and symbols (digital encodings of information).
- Coding and decoding.
- Latency (s) and bandwidth (b/s, Baud).
- Variable-length and fixed-length codes.
  - Morse, Baudot, ASCII, UTF-8, UTF-32 (examinable for concepts e.g. escape codes, but not for specific codings)
- NRZ, NRZI, and Manchester signalling.
- Modulation and demodulation; modems.
- Period, frequency, amplitude, phase.

Important Concepts (2)

- Fourier transformation, DCT.
- SNR, dB.
- ASK, FSK, PSK (digital encodings).
- AM, FM, PM (analog encodings).
- Data compression techniques:
  - variable-length encoding (short codes for frequent symbols)
  - run-length encoding
  - encoding repeated strings by references/pointers
  - differential encoding.
- Data compression algorithms, at conceptual level only (detailed designs are not examinable):
  - Huffman, Lempel-Ziv, JPEG, MP3, MPEG4.

Important Concepts (3)

- Error detection, error correction.
- Single bit errors, burst errors.
- Parity: odd, even.
- Checksum, CRC, BCH, Reed-Solomon: conceptual level only (details will not be examined)
- Two-dimensional parity, Hamming code: you may be required to work an example on the exam, if you are provided important details (e.g. r1 is even parity on bits 1, 3, 5; r2 is even parity on bits 2, 3; r4 is even parity on bits 4, 5).

Important Concepts (4)

- Basic security goals: CIA, source authentication.
- Basic attacks: Interception, interruption, fabrication, modification.
- Darkside goals: interception, modification, interruption, fabrication, stegocommunication.
  - Note: basic security goals are attacks on darkside goals; basic attacks are darkside goals.
- Security functions: the gold standard, identification, non-repudiation.

Important Concepts (5)

- Encryption, decryption, keys (concepts, not details!)
  - Go back n, XOR, (DES, 3DES, AES, RSA)
  - Block ciphers, stream ciphers (CBC)
- Cryptographic hashes (SHA-256, SHA-512)
- Trust, trustworthiness
- Public key infrastructure (X.509)

Important Analyses

- Bandwidth and latency calculations
  - $10^3 \approx 2^{10}$; $10^{-.5} \approx 3$; $\log_{10} 3 \approx 0.5$; $\log_2 1000 \approx 10$
- Fourier analysis of a square wave
- Signalling rate (Nyquist limit)
- Information rate (Shannon limit)
- Crypto-protocol analysis
  - Goals: message integrity, message confidentiality, source authentication.
  - Attack models: interceptions, interruptions, fabrications, modifications.
  - Techniques: symmetric encryption, asymmetric encryption, secure hashing, time stamps. (But not: Diffie-Hellman key exchange, complex protocols, cryptanalysis, ...)