CS3235 MCQ mid-semester test

October 9th 2003

a. This is a closed-book test. The duration of the test is 1hr. You may not use computers during this test.

b. You *must* shade in your Matriculation Number clearly on the MCQ Answer Sheet provided. Write your Matriculation Number as well in the space provided.

c. There are 35 Multiple-Choice Questions. Each question has one correct answer. Shade your answers clearly on the MCQ Answer Sheet.

d. Each correct answer will earn you 1 (one) mark. No penalty will be given for incorrect answers.

e. Hand in your MCQ Answer Sheet at the end of the test. The results of the test will be announced in the course website.

f. Do not bend, fold or soil your MCQ Answer Sheet.

Question 1: If a source's entropy is higher than other sources, then the source's bytes are:

(A) less predictable. (B) more predictable. (C) just as predictable. (D) None of A,B,C.

Question 2: If a source's entropy is lower than other sources, then the source's bytes are:

(A) less compressible. (B) more compressible. (C) just as compressible. (D) All of A,B,C.

Question 3: SHA and MD5 are examples of:

(A) symmetric block ciphers. (B) asymmetric block ciphers. (C) stream ciphers. (D) message signing algorithms.

Question 4: RC4, RC5 are examples of:

(A)block ciphers. (B) hashes. (C) stream ciphers. (D) public key systems. (E) ciphers.

Question 5: If the signal to noise ratio of a channel increases, then the channel capacity:

(A) increases. (B) decreases. (C) remains the same.

Question 6: The keyspace of a Cæsar-like number coding formed by rotating the digits 0-9 is:

(A) 7. (B) 8. (C) 9. (D) 10.

Question 7: The Vigenère cipher is an example of:

(A) a Cæsar cipher. (B) a monoalphabetic cipher. (C) a polyalphabetic cipher. (D) None of A,B,C.

Question 8: In a *good* cipher system, if you changed a single bit in the plaintext, approximately what percentage of the ciphertext should change?

(A) 1%. (B) 50%. (C) 100%. (D) None of A,B,C.

Question 9: In a *good* cipher system, if you changed every bit in the plaintext, approximately what percentage of the ciphertext should change?

(A) 1%. (B) 50%. (C) 100%. (D) None of A,B,C.

Question 10: If the relative entropy of a 30,000 byte file was 0.3333, then it may be compressed to about

(A) 10,000 bytes. (B) 30,000 bytes. (C) 90,000 bytes. (D) None of A,B,C.

Question 11: The *unicity* distance approximates:

(A) the distance between cities in Asia.

(B) the bit difference between two similar strings.

(C) the minimum ciphertext length for which there is only one correct key.

(D) the minimum key length for which there is only one correct ciphertext.

Question 12: The *index of coincidence*:

(A) can tell you the likelihood that a key is the same length as the ciphertext.

(B) can tell you the likelihood that some ciphertext has the same frequency counts as English.

(C) can distinguish between mono and polyalphabetic substitution ciphers.

(D) A and B only.

Question 13: On which of the following does RSA cryptography rely on?

(A) the difficulty in calculating the factors of a large prime number.

(B) the difficulty in calculating the prime factors of a large composite number.

(C) the difficulty in calculating the composite factors of a large composite number.

(D) the difficulty in calculating the inverse of a large number.

In some of the following questions, we are referring to coding systems, where we start with an m-bit code, to which we add r bits to get a new $m + r = n$-bit code. An inequality that may (*or may not*) be useful is $(n + 1)2^m \leq 2^n$.

Question 14: If we start with a 32 bit code, the number of extra bits needed to *detect* a single bit error is:

(A) 1. (B) 2. (C) 4. (D) 6. (E) None of A,B,C,D.

Question 15: If we start with a 32 bit code, the number of extra bits needed to *correct* a single bit error is:

(A) 1. (B) 2. (C) 4. (D) 6. (E) None of A,B,C,D.

Question 16: Kerberos is considered secure because it:

(A) has no single point of failure. (B) uses DES for encryption. (C) uses public key cryptography.

Question 17: A convolutional encoder and decoder is used for:

(A) stream error correction. (B) block error correction. (C) stream error detection. (D) block error detection.

Question 18: Calculate $(36^{106} \bmod 107) \bmod 37$ (note that 107 and 37 are primes).

(A) 1. (B) 36. (C) 105. (D) None of A,B,C.

Question 19: Calculate $6^{214} \bmod 107$

(A) 1. (B) 36. (C) 105. (D) None of A,B,C.

Euler's theorem states that if n is any positive integer and a is any positive integer less than n with no divisors in common with n, then

$$a^{\phi(n)} \bmod n = 1,$$

where $\phi(n)$ is the *Euler phi function* $\phi(n) = n(1 - 1/p_1)\ldots(1 - 1/p_m)$, and $p_1 \ldots p_m$ are all the prime numbers that divide evenly into n, including n if it is a prime.

Question 20: If $n = 77 = 7 * 11$, then $\phi(n)$ is:

(A) 1. (B) 6. (C) 10. (D) 60. (E) None of A,B,C,D.

Question 21: If $n = 143 = 11 * 13$, calculate $15^{241} \bmod n$

(A) 1. (B) 10. (C) 12. (D) 15. (E) None of A,B,C,D.

Given a sequence of symbols from a source, the source *entropy* is

$$H(X) = \sum_{i=1}^{n} P_{x_i} \log_2 \frac{1}{P_{x_i}}$$

where P_{x_i} is the probability of the i-th symbol.

Question22: Calculate the source entropy for a system transmitting the two symbols "A" and "B" with equal probability:

(A) 0. (B) 0.5. (C) 1. (C) 2. (E) None of A,B,C,D.

Question23: Calculate the source entropy for a system transmitting the four symbols "A", "B", "C" and "D" with equal probability:

(A) 0. (B) 0.5. (C) 1. (C) 2. (E) None of A,B,C,D.

Question24: Calculate the source entropy for a system transmitting the four symbols "A", "B", "C" and "D" with probabilities of 0.5 for "A" and "B", and 0 for the other symbols:

(A) 0. (B) 0.5. (C) 1. (C) 2. (E) None of A,B,C,D.

Question 25: The extended Euclidean algorithm is of interest to cryptographers because

(A) It allows us to quickly factorize large composites.

(B) It provides a mechanism to calculate a multiplicative inverse.

(C) It allows us to quickly check primality of large primes.

(D) None of A,B,C.

Question 26: In the Bell-LaPadula model, the property that prevents *Trojan Horses* is commonly called:

(A) no-read-up. (B) no-write-down. (C) top-secret. (D) confidential.

Question 27: The Bell-LaPadula and Biba models are concerned with

(A) confidentiality only.

(B) integrity only.

(C) confidentiality and integrity respectively.

(D) integrity and confidentiality respectively.

Question 28: The CBC mode of operation used in DES is provided

(A) to increase diffusion. (B) to support bidirectional use. (C) for public keys. (D) to combat replay attacks.

Question 29: In Kerberos, a client sends a ticket $\{T_{c,s}\}K_s$ to a server. The server is convinced that the ticket is genuine because

(A) it came from the KDC. (B) it can decode it. (C) it came from the client. (D) it is new.

Question 30: In a Kerberos site, the KDC (Key Distribution Center) has been compromised. This is

(A) OK if network is secure. (B) OK in all cases. (C) BAD if network is insecure. (D) BAD in all cases.

Question 31: A message is authentic and digitally signed if sent with:

(A) a message digest/hash encrypted with the receiver's public key

(B) a message digest/hash encrypted with the receiver's private key

(C) a message digest/hash encrypted with the sender's public key

(D) a message digest/hash encrypted with the sender's private key

Question 32: Which of the following issues is not addressed by Kerberos:

(A) availability. (B) privacy. (C) integrity. (D) authentication.

Question 33: An encryption algorithm has a weak key if the key

(A) is too short. (B) allows attacks. (C) has many more 0s than 1s. (D) can only be used as a public key.

Question 34: If a digital signal on a channel starts changing more quickly, to accurately represent the data the bandwidth of the channel should

(A) increase. (B) decrease. (C) remain the same.

Question 35: If we sample an analog signal on a channel using a shorter and shorter sample, to accurately represent the data the bandwidth of the channel should

(A) increase. (B) decrease. (C) remain the same.