MCQ CLOSED BOOK test

This is a closed-book test. The duration of the test is 40 minutes. You may not use computers/phones.

You *must* shade in your Matriculation Number clearly on the MCQ Answer Sheet provided (i.e. if your Matriculation identifier is t01234546, shade in 0123456) Write your Matriculation Number and name as well in the space provided.

There are 20 Multiple-Choice Questions. Each question has one BEST answer, unless Hugh has made mistakes. Shade your answers clearly on the MCQ Answer Sheet. Each correct answer will earn you 1 (one) mark. No penalty will be given for incorrect answers.

Hand in your MCQ Answer Sheet at the end of the test.

Question 1: The rotation cipher is an example of:

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

Question 2: Which cipher over the alphabet has a larger keyspace?

(A) substitution. (B) Cæsar. (C) rotation.

Question 3: In the attack on IP cameras discussed in class, if performing the attack from a Mac machine, the injected command would be:

(A) an SQL command. (B) a Mac OS command. (C) a Linux OS command. (D) None of A,B,C.

Question 4: It is common to use hashes for passwords. A password hash is...

(A) a password encrypted with a private key.(B) a password encrypted with a public key.(C) not encrypted at all.

Question 5: When a server uses CAPTCHA, it is trying to ...

(A) get your password. (B) see if you are a human. (C) see if you are a robot. (D) record your credentials.

Question 6: With which of Ross Anderson's four categories is the following sentence most closely associated? "The bank management are very sure that no money is lost".

(A) Policy. (B) Mechanism. (C) Incentives. (D) Assurance. (E) None of A,B, C,D.

Question 7: Which of the following ciphers has the least flat (ciphertext) frequency distribution?

(A) Rotation. (B) Playfair. (C) Vernam. (D) Vigenère.

Question 8: The so-called "Chinese Wall Model" is principally concerned with controlling...

(A) access to programs. (B) access to files. (C) insider trading. (D) integrity of data.

Question 9: Assume that you will recognize a correctly decrypted byte of a block when it happens. A block cipher has blocksize b and keysize k. An attack on this block cipher, which exhibits good confusion and good diffusion, would take ...

(A) $\mathscr{O}(k)$ (B) $\mathscr{O}(b)$ (C) $\mathscr{O}(2^k)$ (D) $\mathscr{O}(2^b)$ (E) None of A,B,C,D.

Question 10: Diffusion is primarily associated with the ...

(A) key, and plaintext. (B) key, and ciphertext. (C) plaintext, and ciphertext.

Question 11: Diffie Hellman key exchange makes use of the difficulty in calculating ...

(A) factors of primes.(B) factors of composites.(C) discrete exponentials.(D) discrete logs.(E) None of A,B,C,D.

Question 12: ECC (Elliptic Curve Cryptography) makes use of the difficulty in calculating ...

(A) elliptic curves. (B) if points are on a curve. (C) kP (sums of points). (D) None of A,B,C.

Question 13: Priority inversion might occur when ...

(A) ... a high priority task becomes a low priority task.

(B) ... a low priority task becomes a high priority task.

(C) ... a high priority task is blocked waiting on a resource held by a lower priority task.

(D) ... a low priority task is blocked waiting on a resource held by a higher priority task.

(E) ... none of A,B,C or D.

Question 14: SQL injections may lead to malicious code running on a victim's machine. The suggested best remedy is to...

(A) restrict access to the (web) server.

(B) maintain control over outputs.

(C) maintain control over inputs.

(D) None of A,B, C.

Question 15: In the CIA security triad, the letter A refers to keeping things:

(A) secret. (B) online. (C) trustworthy. (D) None of A,B,C.

Question 16: An asymmetric system for ensuring *authentic* traffic from a source to a target involves encryption with the:

(A) source's public key.(B) source's private key.(C) target's public key.(D) target's private key.

Question 17: The component of PKI responsible for signing a certificate is the:

(A) client. (B) server. (C) RA. (D) CA. (E) None of A,B,C,D.

Question 18: The Caesar cipher:

(A) exhibits "perfect secrecy". (B) is a rotation cipher. (C) uses a set of translation tables.

Question 19: If Ted intercepts Alice's messages to Bob, and passes on changed messages, the attack is called:

(A) snooping. (B) man in the middle. (C) service denial. (D) spoofing. (E) None of A,B,C,D.

Question 20: Which of the following tools is primarily used to monitor network traffic?

(A) nmap. (B) `arpspoof`. (C) `wireshark`.