MCQ CLOSED BOOK test

This is a closed-book test. The duration of the test is 30 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 15 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: A card skimmer is:

(A) copying postcards. (B) a cheater. (C) a device for getting card details. (D) None of A,B,C.

Question 2: AES is an example of which kind of cipher?

(A) block. (B) stream. (C) mixed. (D) None of A,B,C.

Question 3: In the CIA security triad, the letter C refers to keeping things:

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

Question 4: A brute force attack on a AES-encrypted message involves trying all possible:

(A) keys. (B) passwords. (C) hashes. (D) None of A,B,C.

Question 5: Given two primes p and q, with $p < q$ then $2p - q$ can never be

(A) odd. (B) even. (C) 5. (D) None of A,B,C.

Question 6: The term keysize refers to the number of different bits needed for a key for a cipher. For example, if the keyspace was 1024 $(= 2^{10})$, then the keysize is 10 bits. A cipher which gives you the same protection (against brute force attacks) as a rotation cipher over the alphabet A-Z, a-z and 0-9 (62 characters) would have a keysize of

(A) exactly 1 bit. (B) 5 bits. (C) 6 bits. (D) 26 bits. (E) None of A - D.

Question 7: An asymmetric system for ensuring *confidential* 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 8: 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 9: The Chinese wall model is concerned with...

(A) confidentiality. (B) integrity. (C) confidentiality and integrity. (D) None of A,B,C.

Question 10: 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 11: The Windows Scripting Encoder from laboratory 1 would be a ____________ cryptosystem.

(A) rotation (B) monoalphabetic (C) polyalphabetic (D) chosen plaintext

Question 12: In the BLP model, the policy that prevents subjects from corrupting a higher level object is called:

(A) no-read-down. (B) no-write-up. (C) low-watermark. (D) There is no such policy.

Question 13: What is the keyspace of a poly-alphabetic rotation cipher over the digits, with a repeated key-length of 3 (i.e. 3 different rotations), in which no digit can encrypt to itself?

(A) 30. (B) 300. (C) 504. (D) 720. (E) None of A,B,C,D.

Question 14: Shannon's notion of the diffusion property of a cryptosystem involves making the relationship between ____________ and ____________ as complex as possible.

(A) source/destination. (B) ciphertext/plaintext. (C) ciphertext/key. (D) plaintext/key.

Question 15: On which of the following does RSA cryptography rely on?

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

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

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