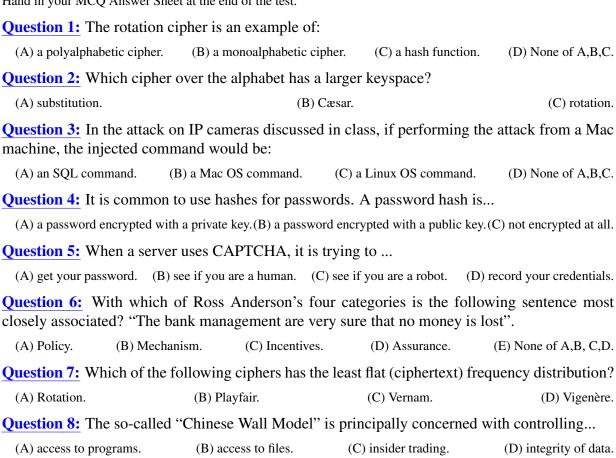
## MCQ CLOSED BOOK test

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.



	cipher has blocks	size $b$ and keysize	ze k. An attack or	byte of a block when it n this block cipher, which
(A) $\mathcal{O}(k)$	(B) $\mathcal{O}(b)$		(D) $\mathcal{O}(2^b)$	(E) None of A,B,C,D.
Question 10: Diffusion is primarily associated with the				
(A) key, and plaintex	it.	(B) key, and cipher	text.	(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.				
<b>Question 15:</b> 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 <i>authentic</i> 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) arpspoor	•	(C) wireshark.