School of Information Technology
Indian Institute of Technology, Kharagpur

IT60112 Information and System Security **End Semester Examination**
Date: April 26th, 2005. **Total Time: 3 Hours** **Max. Marks: 100**

Clearly write any reasonable assumption that you make. All explanations should be precise

Answer Question No. 1 and any 5 from the rest

Q1. Multiple Choice Questions – One or more options may be correct. You will get 2 marks for each correct answer. An answer will be considered correct if all and only the correct choices have been selected. 1 mark will be deducted for a wrong answer. Write only the choice in your answer script. **[5X2=10]**

a. “If a subject A cannot read a file F, then he should not be able to grant another subject B the right to read file F.” This is a consequence of applying the

i. Principle of Least Privilege
ii. Principle of Failsafe Default
iii. Principle of Attenuation of Privilege
iv. Principle of Least Common Mechanism

b. Starting with an initial set of integrity levels of subjects and objects, repeated application of Biba’s Low Watermark Policy can result in

i. Integrity levels of subjects reaching the highest integrity level
ii. Integrity levels of objects reaching the lowest integrity level
iii. Integrity levels of objects reaching the highest integrity level
iv. Integrity levels of subjects reaching the lowest integrity level

c. Diffie-Hellman protocol can be used for

i. Exchanging a symmetric key
ii. Digital Signature
iii. Digital Certificate
iv. Message Encryption

d. Which of the following is a process-oriented methodology for developing secure systems?

i. TCSEC
ii. ITSEC
iii. SSE-CMM
iv. CC

e. If M1 and M2 are two protection mechanisms for a program Q, then

i. $M1 \cup M2$ is as precise as M1
ii. $M1 \cup M2$ is as precise as M2
iii. $M1 \cup M2$ is as precise as $M2 \cup M1$
iv. M1 is as precise as M2

Q2. (a) Consider the use of the Vigenĕre cipher using the key - BAD. What will be the ciphertext corresponding to the plaintext – GOBACKBILL ?

(b) Perform encryption and decryption using the RSA algorithm for the following:

i. p=11; q=13; e=11; Plaintext M = 7

ii. p=11; q=13; e=11; Plaintext M = 147

Derive the decryption key, the ciphertext, and show that after decryption, the decrypted text is the same as the original plaintext **[6+(6+6)=18]**

Q3. (a) Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root a=2. If user A has private key 9 and user B has private key 3, what is the shared key? Show that both A and B get the same shared key.

(b) Consider a guessing attack on a password system using the authentication function. The system implements backoff with time interval between successive prompts forming an AP series with common difference of 1 second. What should be the password changing frequency set by the system administrator so that the probability of learning the password of a given user by an attacker is less than 0.5? Consider all passwords to be of the same length 4 drawn from an alphabet of 10 characters. You may assume that if the average time to guess a password is more than the time gap between two consecutive password changes, then the authentication system is secure.

[(6+2)+10=18]

Q4.

(a) Using a pseudocode, explain how a virus can spread from one executable file to another.

(b) Do you agree with the statement – "All viruses are Trojan horses but all Trojan horses are not viruses"? Justify your answer.

(c) Explain with an example what is a polymorphic virus.

(d) A computer system provides protection using the Chinese Wall security model. Explain to what extent can a macro virus spread in the system. **[5+2+3+8=18]**

Q5.

(a) Explain why Bell-LaPadula Model cannot emulate the Chinese Wall model completely.

(b) Can the Chinese Wall model emulate the Bell-LaPadula model? Explain.

(c) Explain how Clark Wilson's Integrity policy can meet Lipner's requirements of a commercial security system. **[6+6+6=18]**

Q6.

(a) Explain the possible levels/layers of penetration study.

(b) What are the steps of a flaw hypothesis methodology of penetration testing?

(c) Consider that you have to build a secure system for maintaining the grades of undergraduate students of IIT Kharagpur. Grades are currently sent by the faculty members through the departmental office to the academic section in envelopes marked as "Confidential". The academic section maintains the grades in a computer system and prints the Grade Sheets after Senate Meeting. Suggest a high assurance design and development methodology for the system, clearly identifying the secure system design principles that you can employ. Mention the confidentiality and integrity policies that you propose to implement in your system. **[4+4+10=18]**

Q7.

(a) Explain the working principles of the S/Key one time password based authentication system, clearly identifying the password generation, challenge-response and authentication mechanisms.

(b) What kind of dictionary attack can be launched on such an authentication system and how?

(c) Which secure system design principles are followed in designing this authentication system?

(d) How can you use this authentication system if you plan to access your files located in a secure remote server from a non-secure machine in a cybercafe?

(e) How is a pass algorithm based challenge-response system different from the S/Key one time password system? **[8+2+4+2+2=18]**