

**Fourth Semester
Information Technology
Scheme July 2010**

INFORMATION SECURITY

Time : Three Hours

Maximum Marks : 100

Note : i) Attempt total six questions. Question No. 1 (Objective type) is compulsory. From the remaining questions attempt any five.

कुल छः प्रश्न हल कीजिए। प्रश्न क्रमांक 1 (वस्तुनिष्ठ प्रकार का) अनिवार्य है। शेष प्रश्नों में से किन्हीं पाँच को हल कीजिए।

ii) In case of any doubt or dispute, the English version question should be treated as final.

किसी भी प्रकार के संदेह अथवा विवाद की स्थिति में अंग्रेजी भाषा के प्रश्न को अंतिम माना जायेगा।

1. Choose the correct answer.

2 each

सही उत्तर का चयन कीजिए।

i) _____ is a message digest algorithm.

वैसेज digest एल्गोरिथम _____ है।

(a) DES

☒ (b) MD - 5

(c) RSA

(d) IDEA

ii) When two different message digest have the same value it is called as _____

(a) Attack

☒ (b) Collision

(c) Hash

(d) None of the above

जब दो अलग वैसेज द्वारा same value digest की जाती है, तो इसे कहते हैं।

(अ) Attack

(ब) Collision

(स) Hash

(द) उपरोक्त में से कोई नहीं

iii) This type of virus is activated when application such as word processor is run.

(a) Trojan Virus

(b) Worm

(c) Boot sector Virus

(d) None of these

यह वायरस सक्रिय होता है, जब एप्लीकेशन जैसे वर्ड प्रोसेसर रन होती है।

(अ) Trojan Virus

(ब) Worm

(स) Boot sector Virus

(द) इनमें से कोई नहीं

iv) A _____ is a small program embedded inside of GIF image.

_____ एक प्रोग्राम है जो GIF इमेज के साथ सलग्न होता है।

(a) Web buy

(b) Spam

(c) Cookies

(d) Spyware application

v) RSA _____ be used for digital signature.

डिजिटल सिग्नेचर के लिए RSA का उपयोग।

(a) Must not

(b) Can not

(c) Can

(d) Should not

2. a) Explain the basic types of security in detail. 9

Security के बेसिक टाइप्स को विस्तारपूर्वक समझाइए।

b) What is Information Security ? Write the principles of security ? 9

Information security क्या है ? Security के सिद्धांतों को लिखिए।

3. a) Explain Transposition cipher and its implementations using suitable examples. 9
ट्रान्सपोझीशन cipher को उसके अनुप्रयोगों के साथ समझाइए एवं उदाहरण भी दीजिये।
- b) Explain the operation of RSA algorithm used for public key cryptography. 9
RSA algorithm की कार्यप्रणाली को समझाइए जो कि public key cryptography के लिए उपयोग में लाई जाती है।
4. a) Explain digital signature and its applications. 9
Digital signature को समझाइए एवं उसके applications बताएं।
- b) Explain Hash function in detail. 9
Hash फंक्शन को विस्तारपूर्वक समझाइए।
5. a) Explain steganography and cryptography and compare it. 9
Steganography और cryptography को समझाइए एवं उनके बीच तुलना करें।
- b) What is importance of password in authentication Explain. 9
पासवर्ड का authentication में क्या महत्व है, समझाइए।
6. a) Explain digital certificates and their utility in identity management. 9
Digital Certificates को समझाइए एवं उसकी उपयोगिता identity management में बताएं।
- b) Explain the brute force attack and how can it be handled. 9
Brute force attack क्या है एवं उसे किस प्रकार से handle किया जाता है।
7. a) Explain Man-in-middle attack and dictionary attack. 9
Man-in-middle attack एवं dictionary attack को समझाइए।
- b) Explain SSL and its application. 9
SSL को समझाइए एवं उसकी application बताइए।

8. Write short notes on the following (Any three) 6 each
निम्नलिखित पर संक्षिप्त टिप्पणियाँ लिखिये (कोई तीन)
- a) Evolution of cyber law
- b) Computer ethics
- c) Smart card
- d) Ip security architecture
- e) Dos attack