

CS308/IT308

Roll No. :

Spl. 2018

INTRODUCTION TO NETWORK SECURITY AND CRYPTOGRAPHY

निर्धारित समय : तीन घंटे]

Time allowed : Three Hours]

[अधिकतम अंक : 70

[Maximum Marks : 70

नोट : (i) प्रथम प्रश्न अनिवार्य है, शेष में से किन्हीं पाँच के उत्तर दीजिये ।

Note : Question No. 1 is compulsory, answer any **FIVE** questions from the remaining.

(ii) प्रत्येक प्रश्न के सभी भागों को क्रमवार एक साथ हल कीजिये ।

Solve all parts of a question consecutively together.

(iii) प्रत्येक प्रश्न को नये पृष्ठ से प्रारम्भ कीजिये ।

Start each question on fresh page.

(iv) दोनों भाषाओं में अन्तर होने की स्थिति में अंग्रेजी अनुवाद ही मान्य है ।

Only English version is valid in case of difference in both the languages.

1. (i) डीक्रिप्शन को परिभाषित कीजिए ।

Define Decryption.

(ii) कम्प्यूटर सिक्योरिटी क्या है ?

What is computer security ?

(iii) एस एच टी टी पी (SHTTP) एवं टी एस पी (TSP) के पूरे रूप लिखिए ।

Write full form of SHTTP and TSP.

(iv) डीजिटल हस्ताक्षर को परिभाषित कीजिए ।

Define Digital Signature.

(v) फायरवाल से आप क्या समझते हैं ?

What do you understand by firewall ?

(2×5)

2. (i) सुरक्षा के सिद्धांतों से क्या तात्पर्य है, उन्हें समझाइये ।

What is meant by principles of security ? Explain them.

(ii) मैसेज डाइजेस्ट की उपयोगिता को उदाहरण से समझाइये ।

Explain importance of Message Digest with example.

(6+6)

(1 of 2)

P.T.O.

3. (i) प्ले फेयर साइफर एवं सामान्य स्तंभ परिवर्तन तकनीक को उदाहरण सहित समझाइये ।
Explain play fair cipher and simple columnar transposition technique with example.
- (ii) एन्क्रिप्शन क्या है ? यह कितने प्रकार के होते हैं ? उदाहरण एवं खण्ड आरेख की सहायता से समझाइये ।
What is Encryption ? What are its types ? Explain with the help of example and block diagram. (6+6)
4. क्रिप्टोग्राफी एल्गोरिथ्म के विभिन्न प्रकार कौन से हैं ? साइफर ब्लॉक चैनिंग को विस्तार से समझाइये ।
What are different modes of cryptography algorithm ? Explain cipher block chaining in details. (12)
5. (i) टी सी पी / आई पी की कार्यप्रणाली समझाइये ।
Explain the working of TCP/IP.
- (ii) DNS स्पूर्फिंग को समझाइये ।
Explain DNS spoofing. (6+6)
6. (i) पी ई एम क्या है ? समझाइये ।
What is PEM ? Explain.
- (ii) सिक्योर सॉकेट लेयर तथा सिक्योर इलेक्ट्रॉनिक ट्रांसेक्शन में अन्तर लिखिए ।
Write down the difference between secure socket layer and secure electronic transaction. (6+6)
7. (i) एप्लीकेशन गेटवेज़ की कार्यप्रणाली को समझाइये ।
Explain working of Application Gateways.
- (ii) फायरवाल के फायदे तथा सीमाओं का वर्णन कीजिए ।
Describe the advantages and limitations of firewall. (6+6)
8. निम्न पर संक्षिप्त टिप्पणियाँ लिखिए :
Write short notes on the following :
- (i) वायरस तथा वोर्म
Virus and worm
- (ii) कूकीज़
Cookies
- (iii) डी.एम.जेड.
DMZ (4×3)