

2017

**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) कम्प्यूटर सुरक्षा को परिभाषित कीजिए ।  
Define Computer Security.
- (ii) कुकीज को परिभाषित कीजिए ।  
Define Cookies.
- (iii) एनक्रिप्शन को परिभाषित कीजिए ।  
Define Encryption.
- (iv) SSL का पूर्ण रूप लिखिए ।  
Write the full form of SSL.
- (v) फायरवाल की कोई दो सीमाएँ बताइये ।  
Write any two limitations of Firewall.

(2×5)

2. (i) इंटेग्रिटी तथा एक्सेस कण्ट्रोल सुरक्षा के सिद्धांतों को समझाइये ।  
Explain the Integrity and Access Control Principles of Security.
- (ii) सुरक्षा की उपयोगिता को समझाइये ।  
Explain the utility of Security.

(6+6)

3. (i) सीज़र साइफर (Caesar Cipher) को किस प्रकार तोड़ा जा सकता है ? समझाइये ।  
How can Caesar Cipher be cracked ? Explain.
- (ii) साधारण कोलुम्नर ट्रांसपोजिशन तकनीक (Simple Columnar Transposition Technique) किस प्रकार कार्य करती है ? उदाहरण से समझाइये ।  
How does Simple Columnar Transposition Technique work ? Explain with example. (6+6)
4. (i) स्ट्रीम साइफर (Stream Cipher) साधारण टेक्स्ट (Plain Text) को साइफर टेक्स्ट (Cipher Text) में किस प्रकार परिवर्तित करती है ? उदाहरण से समझाइये ।  
How does Stream Cipher convert the Plain Text into Cipher Text ? Explain with example.
- (ii) असिमेट्रिक की क्रिप्टोग्राफी को संक्षेप में समझाइये ।  
Explain Asymmetric Key Cryptography in short. (6+6)
5. (i) समय स्टाम्पिंग प्रोटोकॉल (Time Stamping Protocol) की कार्यप्रणाली को समझाइये ।  
Explain the working of Time Stamping Protocol.
- (ii) Secure Socket Layer (SSL) को समझाइये ।  
Explain Secure Socket Layer (SSL). (6+6)
6. (i) प्राइवैसी एनहांस्ड मेल (Privacy Enhanced Mail) किस प्रकार एनक्रिप्शन तथा नॉन-रेपुडिएशन सुरक्षा के सिद्धांतों को सपोर्ट करती है ? समझाइये ।  
How does Privacy Enhanced Mail support the Encryption and Non-Repudiation principles of Security ? Explain.
- (ii) सीक्योर मल्टीपरपस इन्टरनेट मेल एक्सटेंशन (Secure Multipurpose Internet Mail Extension) को संक्षेप में समझाइये ।  
Explain Secure Multipurpose Internet Mail Extension in short. (6+6)
7. (i) पैकेट फिल्टर फायरवॉल की सुरक्षा को अटैकर्स किस प्रकार तोड़ सकते हैं ? समझाइये ।  
How can the attackers break the security of Packet Filter Firewall ? Explain.
- (ii) डीमिलिट्राइज्ड जोन नेटवर्क्स (Demilitarized Zone Networks) को संक्षेप में समझाइये ।  
Explain Demilitraized Zone Networks in short. (6+6)
8. निम्न पर संक्षिप्त टिप्पणियाँ लिखिए :  
Write short notes on the following :
- (i) ट्रोजन हॉर्स  
Trojan Horse
- (ii) स्पूफिंग  
Spoofing (6+6)