Roll No.: .....

Total No. of Questions : 11] [Total No. of Printed Pages : 12

PK-265

B.C.A. VI Semester (Reg./ATKT) Examination May 2018

INTERNET TECHNOLOGY AND SECURITY

Paper - I

Time Allowed : Three Hours] *[Maximum Marks : 85*

नोट : सभी प्रश्न अनिवार्य हैं।

Note : All questions are compulsory.

खण्ड - अ / Section - A

वस्तुनिष्ठ प्रश्न / Objective Type Questions

15×1=15

Q.1. सही उत्तर का चयन कीजिए।

Choose the correct answer.

i) क्रिप्टोग्राफी में साइफर क्या होता है

(अ) इंक्रिप्शन एवं डिक्रिप्शन करने हेतु ऐल्गोरिथम

(ब) इंक्रिप्शन मेसेज

(स) दोनों (अ) और (ब)

(द) इनमें से कोई नहीं

In Cryptography, what is cipher

(a) Algorithm for performing encryption and decryption

(b) Encryption message

(c) Both (a) and (b)

(d) None of these

ii) साइफर टेक्स्ट को प्लेन टेक्स्ट में परिवर्तित करने हेतु एल्गोरिथम कहलाती है

(अ) इंक्रिप्शन

(ब) डिक्रिप्शन

(स) या तो (अ) या (ब)

(द) न ही (अ) न (ब)

An _____ algorithm transforms cipher text to plaintext.

(a) Encryption

(b) Decryption

(c) Either (a) or (b)

(d) Neither (a) nor (b)

iii) क्रिप्टोग्राफी के हेश फंक्शन में स्वेच्छा से लिये गये डाटा ब्लॉक को परिवर्तित करता हैं

(अ) निश्चित साइज के बिट स्ट्रिंग में

(ब) अनिश्चित साइज के बिट स्ट्रिंग में

(स) दोनों (अ) व (ब)

(द) इनमें से कोई नहीं

Cryptography Hash function takes an arbitrary block of data and returns

(a) Fixed size bit string

(b) Variable size bit string

(c) Both (a) and (b)

(d) None of these

iv) निम्न में से कौन-सी एल्गोरिथम असिमेट्रिक की क्रिप्टोग्राफी में उपयोग में नहीं लाई जाती हैं

(अ) RSA (ब) Diffie-Hellman

(स) ECB (द) इनमें से कोई नहीं

Which of the following algorithm is not used in asymmetric - key cryptography ?

(a) RSA (b) Diffie-Hellman

(c) ECB (d) None of these

v) दो पार्टियों से मध्य one-time session key देने वाली विधि कहलाती है।

The _____ method provides a one-time session key for two parties.

(a) Diffie-Hellman (b) RSA

(c) DES (d) AES

vi) DES के की जेनरेटर में कितने बिट सोलह राउण्ड 'कीज' जेनरेट होती है?

DES uses a key generator to generate sixteen _____ round key.

(a) 32 bit (b) 48 bit

(c) 54 bit (d) 64 bit

vii) CMAC किस अन्य नाम से जाना जाता हैं

Another name of CMAC is

(a) Code-based MAC

(b) Cipher-based MAC

(c) Construct-based MAC

(d) Collective-based MAC

viii) MAC किस और अन्य नाम से जाना जाता है

(अ) क्रिप्टोग्राफिक कोड ब्रेक

(ब) क्रिप्टोग्राफिक कोड सम

(स) क्रिप्टोग्राफिक चेक सम

(द) क्रिप्टोग्राफिक चेक ब्रेक

MAC is also known as -

(a) Cryptographic code break

(b) Cryptographic code sum

(c) Cryptographic check sum

(d) Cryptographic check break

ix) SHA-I का message digest होता है

SHA-I has a message digest of -

(a) 160 bits (b) 512 bits

(c) 628 bits (d) 820 bits

x) e-mail से संबंधित security protocol होता है

One security protocol for e-mail system

(a) IPsec (b) SSS

(c) PGP (d) None of these

xi) निम्न में से कौन सा सबसे मजबूत पासवर्ड है

Which of the following is a strong password-

(a) 19th August

(b) Delhi88

(c) p@assword2!

(d) delhi123

xii) कौन-सा एक इंक्रिप्शन स्टेंण्डर्ड नहीं हैं?

Which is not an encryption standard ?

(a) AES (b) TES

(c) Triple DES (d) DES

xiii) एक पाब्लक की क्रिप्टोग्राफी की एल्गोरिथम ह

An Public key cryptographic is -

(a) RSS (b) RAS

(c) RSA (d) RAA

xiv) वाइरस है

(अ) मानव निर्मित (ब) प्राकृतिक घटना

(स) मशीन निर्मित (द) उपरोक्त सभी

Viruses are -

(a) Man made (b) Natural event

(c) Machine made (d) All of the above

xv) निम्न में से कौन-सा फायरवॉल का प्रकार है

(अ) वाइरस (ब) सुरक्षा में खतरा

(स) वॉर्म (द) इनमें से कोई नहीं

Which one is an type of Firewall

(a) Virus (b) Security Threat

(c) Worm (d) None of these

खण्ड - ब / Section - B

लघु उत्तरीय प्रश्न / Short Answer Type Questions

$5 \times 5 = 25$

Q.2. स्टेग्नोग्राफी से आप क्या समझते हैं?

What do you understand by Steganography?

अथवा / OR

Block Cipher के बारे में संक्षिप्त में बताये।

Briefly discuss Block Cipher.

Q.3. Key management से आपका क्या तात्पर्य है?

What do you mean by Key management?

अथवा / OR

Authentication की जरूरते क्या हैं?

What are Authentication requirements?

Q.4. सिक्योर हेश एल्गोरिथम क्या हैं?

What is Secure Hash Algorithm?

अथवा / OR

HMAC का संक्षिप्त वितरण दें।

Briefly discuss HMAC.

Q.5. वेब सुरक्षा क्यों आवश्यक है?

Why Web Security is important?

अथवा / OR

IPsec के लाभों को लिखिये।

Write the benefits of IPsec.

Q.6. Intrusion Detection के बारे में लिखिये।

Write about Intrusion Detection.

अथवा / OR

Firewalls की जरूरते बताये।

Write the needs of Firewalls.

खण्ड - स / Section - C

दीर्घ उत्तरीय प्रश्न / Long Answer Type Questions

5×9=45

Q.7. Differential एवं Linear Cryptoanalysis को विस्तार से समझाइये।

Explain Differential and Linear Cryptoanalysis.

अथवा / OR

Block Cipher Modes से Operations की व्याख्या करें।

Describe Block Cipher Modes of Operations.

Q.8. Elliptic Curve Cryptography की व्याख्या करें।

Describe Elliptic Curve Cryptography.

अथवा / OR

Message Authentication Functions क्या होते हैं?

What are Message Authentication Functions?

Q.9. हेश एल्गोरिथम क्या है? सुरक्षित हेश फंक्शन हेतु कौन-से गुणों की आवश्यकता होती हैं?

What is Hash Algorithm? What characteristics are needed in a secure Hash Functions?

अथवा / OR

MAC क्या है? One Way Hash Function एवं MAC में क्या भिन्नता हैं?

What is MAC? What is the difference between a MAC and a One Way Hash Function?

Q.10. Message Authentication क्या है? इसके अनुप्रयोग लिखिये।

What is Message Authentication? Write its applications.

अथवा / OR

IPsec द्वारा क्या सेवायें प्रदान की जाती है?

What securities are provided by IPsec?

Q.11. वाइरस एवं इससे संबंधित खतरों पर चर्चा करें।

Discuss viruses and its related threats.

अथवा / OR

Trusted System के बारे में लिखिये।

Write about Trusted System.

❖❖❖❖❖❖❖