PAPER ID-311474

Subject Code: KCA011

Roll No: | | | | | | | | | | | | | |

MCA

(SEM III) THEORY EXAMINATION 2023-24

CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 100**

Note: 1. Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. Attempt *all* questions in brief. **2 x 10 = 20**

Q no.	Question	Marks	CO
a.	Differentiate Active and Passive attack.	2	1
b.	State and prove Fermet's theorem	2	1
c.	What is the difference between Diffusion and Confusion?	2	2
d.	Differentiate between weak collision resistance and strong collision resistance property of hash function.	2	2
e.	Differentiate Authorization and authentication.	2	3
f.	Show 2 is the primitive root of 11.	2	3
g.	Between symmetric and asymmetric encryption which method is more convenient and why?	2	4
h.	What is key distribution center?	2	4
i.	What is the difference between direct and arbitrated digital signature?	2	5
j.	What do you understand by computer viruses and worms?	2	5

SECTION B

2. Attempt any *three* of the following: **10 x 3 = 30**

a.	While DES keys are 64 bits long, but effective key length is only 56 bits, why?	10	1
b.	Explain X.509 Authentication Service along with its format.	10	2
c.	Describe DSA (Digital Signature Algorithm).	10	3
d.	What basic arithmetical and logical functions are used in MD5? Explain SHA-1 logic.	10	4
e.	What do you understand by web security? What are the secure socket layers and their functions?	10	5

SECTION C

3. Attempt any *one* part of the following: **10 x 1 = 10**

a.	Describe network security model with neat and clean diagram.	10	1
b.	Describe Block Cipher Modes of Operation in DES.	10	1

4. Attempt any *one* part of the following: **10 x 1 = 10**

a.	State the Chinese Remainder Theorem. Hence use it to solve following Congruence to obtain the value of X. x≡2 (mod 3); X≡3 (mod 5); X≡2 (mod 7)	10	2
b.	In a public key system using RSA, if the Cipher text C = 20, public key e=5, n =35, what is the plain text corresponding to the Cipher text C?	10	2

QP24DP2_290 | 18-03-2024 13:28:44 | 117.55.242.132

PAPER ID-311474

Roll No: | | | | | | | | | | | | | |

MCA
(SEM III) THEORY EXAMINATION 2023-24
CRYPTOGRAPHY & NETWORK SECURITY

TIME: 3 HRS **M.MARKS: 100**

5. Attempt any *one* part of the following: 10 x 1 = 10

a.	What are the requirements for a Hash function? What is Birthday attack on Hash codes? What do you understand by Weak collision resistance and strong collision resistance?	10	3
b.	Describe DSA (Digital Signature Algorithm).	10	3

6. Attempt any *one* part of the following: 10 x 1 = 10

a.	What do you mean by firewall? Explain Packet filtering, Circuit gateways and Application gateways.	10	4
b.	Compare DSS and RSA approaches to digital Signature.	10	4

7. Attempt any *one* part of the following: 10 x 1 = 10

a.	What do you mean by Kerberos? Explain the role of Authentication Server (AS) and Ticket Granting Server (TGS) in Kerberos authentication Protocol.	10	5
b.	How is email security provided through PGP? Also describe the PGP message generation and PGP message reception	10	5

QP24DP2_290 | 18-03-2024 13:28:44 | 117.55.242.132

QP24DP2_290 | 18-03-2024 13:28:44 | 117.55.242.132