University of Mumbai

Examinations Commencing from 25th July 2022 to 3rd August 2022
Program: Master of Computer Applications
Curriculum Scheme: (MCA 2year) –(R-2020-21)
Examination: M.C.A Semester II
Course Code: MCA23and Course Name: Information Security

Time: 3Hours Max. Marks: 80

==

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	The operation of a cipher usually depends on a piece of auxiliary information, called
Option A:	Plain text
Option B:	Cipher Text
Option C:	Key
Option D:	Cipher
2.	The mechanism used for authenticating a user only once is called as
Option A:	Single Sign On
Option B:	System Security Office
Option C:	Single Sign Off
Option D:	Single Security Opportunity
Q3.	Cryptanalysis is used ___________
Option A:	To find some insecurity in a cryptographic scheme.
Option B:	To increase the speed.
Option C:	To encrypt the data.
Option D:	To make new ciphers.
4.	MD5 produces ___________ bits hash data
Option A:	128
Option B:	150
Option C:	160
Option D:	112
5.	If the recipient of a message has to be satisfied with the identity of the sender, the principle __________ comes into picture.
Option A:	Integrity
Option B:	Access control
Option C:	Authentication
Option D:	Confidentiality
6.	PGP Key Management has the following functionality
Option A:	Every user is own CA
Option B:	Cannot forms a “web of trust”
Option C:	Users cannot revoke their keys
Option D:	Rely on certificate authorities

7.	To encrypt a message from Alice to Bob using public key cryptography, which of the following is needed?
Option A:	Alice's private key
Option B:	Alice's public key
Option C:	Bob's private key
Option D:	Bob's public key
8.	A __________ attack involves the passive capture of a data unit and its subsequent re-transmission to produce an unauthorized effect
Option A:	Release of message contents
Option B:	Replay
Option C:	Masquerade
Option D:	Traffic analysis
9.	A Substitution Box of DES provides
Option A:	Diffusion only
Option B:	Confusion only
Option C:	Both diffusion and confusion
Option D:	Neither diffusion nor confusion
Q10.	Intrusion detection approach that involves the collection of data relating to the behavior of legitimate users over a period of time.
Option A:	Statistical anomaly detection
Option B:	Rule-based detection
Option C:	Audit Records
Option D:	Penetration identification

Q2 (Total 20 Marks)	
A	**Solve any Two** **5 Marks Each**
i	Explain algorithm modes CBC uses for secret key cryptography.
ii	Explain Cross-Certification.
iii	Using Euclidean algorithm, find the greatest common divisor of the following: i. 300 and 42 ii. 88 and 220
B	**Solve any One** **10 Marks Each**
i	What is Message Digest? Explain the working of MD5 in detail.
ii	Discuss Inference. What are the various approaches to deal with it?

Q3 (Total 20 Marks)	
A	**Solve any Two** **5 marks each**
i	Explain the various Information Security principles.
ii	What is intrusion detection? What are the various systems used for detecting intrusions?
iii	In an RSA cryptosystem, a particular A uses two prime numbers p =

	13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is?
B	**Solve any One 10 Marks Each**
i	Explain PGP to provide security? Discuss the concept of PGP keys and rings.
ii	What is Kerberos? Explain the working of Kerberos

Q4 **(Total 20 Marks)**	
A	**Solve any Two 5 marks each**
i	Differentiate between Symmetric and Asymmetric Cryptography
ii	What are Firewalls? Discuss its types.
iii	Explain MAC in detail.
B	**Solve any One 10 Marks Each**
i	Discuss SSL as an internet security protocol and three major protocol use at SSL?
ii	Explain one round structure of DES.