Comp (1)
Crypt & Sys Secu

K J Somaiya Institute of Engineering and Information Technology

14/12/2022

K. J. Somaiya Institute of Engineering and Information Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)
End Semester Exam
Nov/Dec 2022
B.Tech-Program – Computer Engineering
Examination: TY Semester VI
Course Code: 1UCEC602 and Course Name: Cryptography and System Security

Duration: 03Hours **Max. Marks: 60**

Instructions:
(1) All questions are compulsory.
(2) Draw neat diagrams wherever applicable
(3) Assume suitable data, if necessary.

Q. No.	Question	Max. Marks	CO	BT Level
Q 1	**Solve any six questions out of eight:**	**12**		
i)	If n=77, find Φ(n).	**2**	CO1	Ap
ii)	Differentiate between confusion and diffusion	**2**	CO2	U
iii)	A ----- attaches itself to execute files. When the infected program is executed, it replicates itself by finding other executable files to infect. a. Macro virus b. Stealth Virus c. Polymorphic virus d. Parasitic virus.	**2**	CO6	U
iv)	Explain MAC in brief.	**2**	CO3	U
v)	Compare AES and DES in terms of block size, key size, rounds, encryption primitives and Cryptographic primitives.	**2**	CO2	U
vi)	Explain two-factor authentication method.	**2**	CO4	U
vii)	What is the main difference between tunnel and transport mode of SSL protocol.	**2**	CO5	U
viii)	Which of the following is not a threat to the integrity of data? a. Replay b. Masquerade c. Snooping d. Modification of message contents	**2**	CO1	U
Q.2	**Solve any four questions out of six.**	**16**		

i)	Users A and B use the Diffie-Hellman key exchange technique. They agree with a common prime n=41 and a primitive root g=13 If user A has private key XA=27, what is A's public key YA? If user B has private key XB=18, what is B's public key YB? What is the shared secret key?	4	CO2	Ap
ii)	Encrypt the text "We are the best" by applying monoalphabetic ciphers. Is cryptanalysis of this cipher easy? If yes then explain how?	4	C01	Ap
iii)	Explain CMAC in detail.	4	CO3	U
iv)	What is token-based authentication. Explain its types in detail.	4	CO4	U
v)	What is IP spoofing? Explain with an example.	4	CO5	U
vi)	What are different viruses and worms? How do they propagate?	4	CO6	U
Q.3	**Solve any two questions out of three.**	**16**		
i)	Explain RSA digital signature scheme. Analyze its security aspects.	8	CO4	An
ii)	Explain MD5 in detail.	8	CO3	U
iii)	Compare and contrast block cipher and stream ciphers with examples of both	8	CO2	An
Q. 4	**Solve any two questions out of three**	**16**		
i)	Apply Hill cipher to encrypt the message "ESSENTIAL". The key for encryption is "ANOTHERBZ" and decrypt the encrypted message.	8	CO1	Ap
ii)	Generate the subkey for the first round of the AES algorithm. The key in hexadecimal is: 64 46 5A 65 82 AB 7C 73 4E 5B 47 8D 9A 12 35 57	8	CO2	Ap
iii)	What is the need of SSL? Explain its protocols in detail.	8	CO5	U