University of Mumbai

Examinations Summer 2022

Time: 02 hours 30 minutes Max. Marks: 80

==========

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	Which of the following is lossless Text compression technique?
Option A:	MPEG
Option B:	JPEG
Option C:	Arithmetic Coding
Option D:	JBIG
2.	In a public-key system using RSA, you intercept the cipher text C = 256 sent to a user whose public key is e = 17, n = 341. What is the plain text M? _____.
Option A:	786
Option B:	28
Option C:	07
Option D:	16
3.	Cryptographic hash function takes an arbitrary block of data and returns _____.
Option A:	fixed size bit string
Option B:	variable size bit string
Option C:	both fixed size bit string and variable size bit string
Option D:	variable sized byte string
4.	Data Encryption standard, DES encoder uses a key generator to generate sixteen _____ round keys.
Option A:	32 bits
Option B:	64 bits
Option C:	48 bits
Option D:	42 bits
5.	The _____ method provides a one-time session key for two parties.
Option A:	Diffie-Hellman
Option B:	RSA
Option C:	DES
Option D:	AES
6.	Choosing a discrete value that is near but not exactly at the analog signal level leads to _____.
Option A:	PCM error
Option B:	Quantization error
Option C:	PAM error
Option D:	Sampling error
7.	In JPEG and JPEG 2000 standards, compression of still images is based on _____ and _____ respectively.
Option A:	Cosine Transform, Hadamard Transform,
Option B:	DCT, Walsh Transform

Option C:	IDCT, Discrete Wavelet Transform (DWT)
Option D:	DCT, Discrete Wavelet Transform (DWT)
8.	In digital signature algorithm, the responsibility of a certification authority is to authenticate the _____.
Option A:	private keys of subscribers
Option B:	public keys of subscribers
Option C:	key used in DES
Option D:	hash function used
9.	Which of the following is not a type of symmetric-key cryptography technique?
Option A:	Diffie Hellman cipher
Option B:	Data Encryption Standard (DES)
Option C:	Caesar cipher
Option D:	Playfair cipher
10.	In Data Encryption Standard, Triple DES used by the operator _____.
Option A:	can be broken only if the algorithm is known using even slow computer.
Option B:	is impossible to break ever.
Option C:	cannot be broken in reasonable time using presently available computers.
Option D:	can be broken with presently available high-performance computers.

Q2.	**Solve any Four out of Six questions.**	**05 marks each**
A	Explain Authentication, Data Integrity and Authorization in cryptography.	
B	Write a short note on DPCM.	
C	Solve the following. 1. 17^{-1} mod 23 2. 23^{-1} mod 29	
D	List advantages of AES over DES.	
E	What is the importance of Ethical Hacking?	
F	Write a short note on H.264 encoder and decoder.	
Q3.	**Solve any Two Questions out of Three.**	**10 marks each**
A	Consider a source with alphabet A= {a_1, a_2, a_3} with probability model of {0.6, 0.02, 0.38} respectively. Perform Arithmetic Coding and generate a decimal tag for the sequence $a_1a_2a_3a_2a_1$.	
B	Convert plain text "HIDE THE GOLD IN THE TREE STUMP" using Playfair Cipher technique. Use encryption key as "PLAYFAIR EXAMPLE".	
C	Discuss various types of Block Ciphers with examples.	
Q4.	**Solve any Two Questions out of Three.**	**05 marks each**
A		
i.	State the advantages of JPEG-2000 over JPEG-LS.	
ii.	What is the significance of HASH functions in message integrity and authentication?	
iii.	How firewall is design to provide security.	
B	**Solve any One**	**10 marks each**
i.	Explain RSA algorithm to encrypt the plain text message, M=2 for prime numbers p=17 and q=31, public key e =7. Verify that the decrypted text is the same as plain text.	
ii.	Illustrate Diffie-Hellman key exchange algorithm with example.	