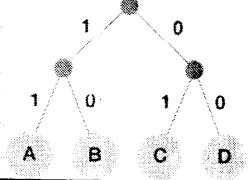


Q1.(20 Marks)	Choose the correct option for following questions. All the Questions are compulsory and carry equal marks
1.	In the LZ77 approach, buffer that contains a portion of recently encoded sequence is called as
Option A:	Look ahead buffer
Option B:	Search Buffer
Option C:	Look in buffer
Option D:	Search buffer
2.	In Audio and Video Compression, voice is sampled at 8000 samples per second with
Option A:	5 bits per sample
Option B:	6 bits per sample
Option C:	7 bits per sample
Option D:	8 bits per sample
3.	A _____ cipher replaces one character with another character.
Option A:	transpositional ciphers
Option B:	substitution ciphers
Option C:	Expansion cipher
Option D:	quadratic ciphers
4.	The correct encoding of the letter C in this tree is... 
Option A:	11
Option B:	10
Option C:	01
Option D:	00
5.	_____ is a popular session key creator protocol that requires an authentication server and ticket granting server
Option A:	KDC
Option B:	Kerberos
Option C:	CA
Option D:	SSL
6.	LZ77 and LZ78 algorithms published in papers by Abraham Lempel and Jacob Ziv in 1977 and 1978 removes
Option A:	Coding redundancy

Option B:	Physicovisual redundancy
Option C:	Interpixel redundancy
Option D:	Temporal redundancy
7.	Which of the following process is not performed in the final round of the AES?
Option A:	Substitution bytes
Option B:	Shift rows
Option C:	Mix columns
Option D:	Add Round Key
8.	$\phi(37)=$
Option A:	24
Option B:	22
Option C:	13
Option D:	36
9.	The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
Option A:	Man-in-middle attack
Option B:	Meet in Middle attack
Option C:	Birth day Attack
Option D:	Brute force Attack
10.	JPEG 2000 uses the transform
Option A:	DWT
Option B:	DCT
Option C:	DFT
Option D:	Hadamard

Q2. (20 Marks)	Solve any Four out of Six	5 marks each
A	A Source emits three symbols a, b, c with probabilities 0.8, 0.02 and 0.18 respectively. Find out the tag generated for the sequence 'baac' using arithmetic coding	
B	What are the various components of SSL Architecture?	
C	What is the role of Hash function in cryptography?	
D	Discuss the working of H – 261 Encoder and Decoder with neat diagram.	
E	Why do you need substitution box in DES? How many substitution boxes are used in standard DES?	
F	Compare lossy compression techniques with lossless compression techniques.	

Q3. (20 Marks)	Solve any Two Questions out of Three	10 marks each
A	Take an alphabetic string 'wabbba wabba woo'. Show the encoding and decoding process using LZW algorithm.	
B	With neat block diagram, explain the working of JPEG for image compression? Why DCT is needed in JPEG?	
C	What is a digital signature? Can we use public key encryption technique for generating a digital signature?	

Q4. (20 Marks)	Solve any Two Questions out of Three	10 marks each
A	Analyse Secure Electronic Transaction with neat diagram.	
B	What is μ law companding in Audio compression? What are the steps involved in generating a code word in μ law companding?	
C	What is public key encryption? In a public-key system using RSA, you intercept the cipher text $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M ?	