APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
Scheme for Valuation/Answer Key
Scheme of evaluation (marks in brackets) and answers of problems/key
SEVENTH SEMESTER B.TECH DEGREE EXAMINATION (S), MAY 2019
Course Code: CS409
Course Name: CRYPTOGRAPHY AND NETWORK SECURITY

Max. Marks: 100   Duration: 3 Hours

PART A
Answer all questions, each carries 4 marks.
Marks

1	S box explanation – 4 marks	()
2	Confusion – 2 marks, Diffusion – 2 marks	()
3	Key expansion – 3 marks, complex function – 1 mark.	()
4	Definition – 2 marks, proof – 2 marks	()
5	d = 17 – (2 marks), M = 2 – (2 marks)	()
6	MAC is a many to one function and Encryption is a one to one – 2 marks	()
	Illustration - 2 marks	
7	Header format – 4 marks	()
8	3 methods – 4 marks	()
9	Services – 4 marks	()
10	Any 4 points – 4 marks	

PART B
Answer any two full questions, each carries 9 marks.

11	a)	Differences – 3 marks, example – 2 marks	()
	b)	4 techniques – 4 marks	()
12	a)	Diagram – 2 marks, explanation – 2 marks	()
	b)	Mix Column matrix – 2 marks, explanation – 2 marks	()
13	a)	Rail fence cipher explanation – 1 mark, encryption – 3 marks, Answer :	()
		ttnaaptmtsuoaodwcoixknlypetz	
	b)	Inverse S box creation steps	()
		Initialization 1 mark	
		Map each byte to its multiplicative inverse 1 mark	
		Applying transformation to each bit - 3 marks	

PART C
Answer any two full questions, each carries 9 marks.

14	a)	Answer = 2, Table and steps – 4 marks	()

	b)	Explanation – 5 marks	()
15		Steps – 3 marks, compression function and explanation – 3 marks, diagrams – 3 marks	()
16	a)	Proof – 2 marks, $X_A = 6$ (1 mark), Secret key K = 3 (2 marks)	()
	b)	Diagram – 1 mark, Signing – 1.5 marks, verification – 1.5 marks	()

PART D
Answer any two full questions, each carries 12 marks.

17	a)	Steps explanation – 6 marks	()
	b)	Message format – figure – 3 marks	()
	c)	Steps – 3 marks	()
18	a)	Dual signature – 2 marks, relevance – 2 marks	()
	b)	Explanation – 4 marks, diagram – 2 marks	()
	c)	Requirements – 2 marks	()
19	a)	SPD concept – 2 marks, working – 2 marks	()
	b)	Explanation – 2 marks	()
	c)	3 configurations 2 marks each	()

****