USN | | | | | | | | | | |

Internal Assessment Test 1 – Sept. 2019

Sub:	Cryptography and Network Security					Sub Code:	15TE71	Branch:	TCE
Date:	06/09/2019	Duration:	90 min's	Max Marks:	50	Sem / Sec:	A		OBE

Answer any FIVE FULL Questions

		MARKS	CO	RBT
1 (a)	Solve this using Euclidean Algorithm GCD (1160718174, 316258250).	[5]	CO1	L3
1 (b)	Quote the properties of modular arithmetic.	[5]	CO1	L1
2	Find the inverse of the following using extended Euclidean Algorithm i. 550 mod 1759 ii. 17 mod 60	[10]	CO1	L2
3	Define abelian group and explain its property.	[10]	CO1	L2
4	Prove that $\langle Z_6, + \rangle$ is a cyclic group and find the generator of this group.	[10]	CO1	L3
5	Find the inverse of (x^5) in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.	[10]	CO1	L2
6 (a)	Define these following terms i. Cipher Text ii. Encryption iii. Decryption iv. Cryptanalyst v. Cryptography	[5]	CO1	L2

USN | | | | | | | | | | |

Internal Assessment Test 1 – Sept. 2018

Sub:	Cryptography and Network Security					Sub Code:	15TE71	Branch:	TCE
Date:	18/09/2018	Duration:	90 min's	Max Marks:	50	Sem / Sec:	A		OBE

Answer any FIVE FULL Questions

		MARKS	CO	RBT
1 (a)	Solve this using Euclidean Algorithm GCD (1160718174, 316258250).	[5]	CO1	L3
1 (b)	Quote the properties of modular arithmetic.	[5]	CO1	L1
2	Find the inverse of the following using extended Euclidean Algorithm i. 550 mod 1759 ii. 17 mod 60	[10]	CO1	L2
3	Define abelian group and explain its property.	[10]	CO1	L2
4	Prove that $\langle Z_6, + \rangle$ is a cyclic group and find the generator of this group.	[10]	CO1	L3
5	Find the inverse of (x^5) in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.	[10]	CO1	L2
6 (a)	Define these following terms i. Cipher Text ii. Encryption iii. Decryption iv. Cryptanalyst v. Cryptography	[5]	CO1	L2

6 (b)	Find the result of the following $(a)\ 5^{15}\ mod\ 13$ (b) $456^{17}\ mod\ 17$ (c) $20^{62}\ mod\ 77$ (d) $71^{81}\ mod\ 100$ (e) $60^{160}\ mod\ 187$	[5]	CO1	L3
7	Explain the types of cryptanalytic attacks on encrypted messages.	[10]	CO1	L2
8	Define the Term Cryptography. Explain the essential components of conventional encryption.	[10]	CO1	L2

-----All The Best-----

6 (b)	Find the result of the following $(a)\ 5^{15}\ mod\ 13$ (b) $456^{17}\ mod\ 17$ (c) $20^{62}\ mod\ 77$ (d) $71^{81}\ mod\ 100$ (e) $60^{160}\ mod\ 187$	[5]	CO1	L3
7	Explain the types of cryptanalytic attacks on encrypted messages.	[10]	CO1	L2
8	Define the Term Cryptography. Explain the essential components of conventional encryption.	[10]	CO1	L2

-----All The Best-----