

0. :				
COR	(2014 Adm E COURSE II	pril 2019 ilssion Onwa N COMPUTE	irds) R SCIENCE	Examination,
3 Hours				Max. Marks: 40
0110010				
	F F	PART – A		
is a p	orinciple of sec	urity.		
mear	ns converting p	olain text to cip	her text.	
DOS stands for				
If each occurrent substitution.	ce of a characte	er has different	substitution, it	is
Expand NIST.				
After parity drop operation, if a key consists of all 0's or 1's or half 0's and half 1's, they are keys.				
feiste	rounds are pr			(8×0.5=4)
		PART - B		
ver any seven :				
	COR 6B 3 Hours is a p mean The science and DOS stands for If each occurrence substitution. Expand NIST. After parity drop half 1's, they are	mester B.Sc. Degree (CBCS A (2014 Adm CORE COURSE II 6B16CSC : E06 3 Hours is a principle of sec means converting in The science and art of breaking DOS stands for If each occurrence of a characte substitution. Expand NIST. After parity drop operation, if a half 1's, they are key feistel rounds are principle.	mester B.Sc. Degree (CBCSS – Reg./Sup April 2019 (2014 Admission Onwa CORE COURSE IN COMPUTE 6B16CSC : E06 : Information 3 Hours PART – A is a principle of security. means converting plain text to cip The science and art of breaking secret code is DOS stands for If each occurrence of a character has different substitution. Expand NIST. After parity drop operation, if a key consists of half 1's, they are keys. feistel rounds are present in encrying part of the parity drop operation. PART – B	Mester B.Sc. Degree (CBCSS – Reg./Supple./Improv.) April 2019 (2014 Admission Onwards) CORE COURSE IN COMPUTER SCIENCE 6B16CSC : E06 : Information Security 3 Hours PART – A is a principle of security. means converting plain text to cipher text. The science and art of breaking secret code is DOS stands for If each occurrence of a character has different substitution, it substitution. Expand NIST. After parity drop operation, if a key consists of all 0's or 1's of half 1's, they are keys feistel rounds are present in encryption in DES. PART – B

- 2. Define confidentiality.
- 3. Differentiate passive attacks and active attacks.
- 4. Define digital signature.
- 5. Define Kirchhoff's principle.

K19U 0098



- 6. Give and explain any two properties of a block cipher.
- 7. What is a private key?
- 8. What is steganography?
- 9. What do you mean by cipher text?
- Explain linear cryptanolysis.
- 11. What is Trojan Horse?

 $(7 \times 2 = 14)$

PART - C

Answer any four:

- 12. What is public key encryption? Explain its main elements.
- 13. Explain security attacks.
- 14. What are cryptanolysis attacks?
- 15. Explain keyless and keyed transposition ciphers.
- 16. Explain the weaknesses of DES.
- 17. Explain digital signature process.

 $(4 \times 3 = 12)$

PART - D

Answer any two:

- 18. Explain DES structure.
- 19. Write notes on RSA digital signature scheme.
- 20. Explain the applications of key crypto systems.
- 21. Explain the various types of attacks.

 $(2 \times 5 = 10)$