Program: T.Y.B.Sc CS **Semester:** V **Program Code:** UGCS02

Course: Information Security **Course Code:** NUCS502

Duration: 1 Hour **Examination Pattern:** NEP-Autonomous - External **Max. Marks:** 30

Instructions:

1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Draw neat diagrams wherever necessary.
4. CO (Course Outcome), KL (Knowledge Level).

Examination:

REGULAR

Q. 1		**Attempt any TWO of the following.**	[10]	CO's	KL's
	(a)	Explain the concept of Computer Security and discuss its major objectives/principles.		CO1	L2
	(b)	Define Terms: i) The Avalanche Effect ii) Cryptanalysis iii) Brute Force Attack		CO1	L1
	(c)	Solve the following : i) Encrypt INFORMATION using Caesar cipher with key = 5. ii) Encrypt FIREWALL using Play Fair Cipher with key - NETWORK		CO2	L3
	(d)	Explain the working of Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes. Compare their security characteristics.		CO2	L4
Q. 2		**Attempt any TWO of the following.**	[10]	CO's	KL's
	(a)	Explain the working principle of a public-key cryptosystem.		CO3	L2
	(b)	Alice and Bob want to securely communicate using the Diffie-Hellman Key Exchange method. Given the following parameters : Prime number p = 5 Generator g = 3, Alice's private key = 3, Bob's private key = 2 Calculate Alice's public key, Bob's public key. And also compute the shared secret key using the public keys.		CO3	L3
	(c)	Write a note on Kerberos.		CO4	L2
	(d)	Describe X.509 certificate format with suitable diagram.		CO4	L2
Q. 3		**Attempt any TWO of the following.**	[10]	CO's	KL's
	(a)	State the types of Passive and Active Attacks.		CO1	L1
	(b)	Draw the feistel structure of encryption & decryption.		CO2	L2
	(c)	Demonstrate the application of cryptographic hash functions in information security with suitable examples, such as password storage, data integrity verification, and digital signatures.		CO4	L2
	(d)	Explain the essential properties of a secure cryptographic hash function.		CO4	L2

- - X - - X -