DAYANANDA SAGAR COLLEGE OF ENGINEERING
(An Autonomous Institute Affiliated to VTU, Belagavi)
ShavigeMalleshwara Hills, Kumaraswamy Layout, Bengaluru-560078
Department of Telecommunication Engineering
Continuous Internal Assessment Test - I

Course: **Cryptography and Network security**   Date: **07/10/2020**
Course Code**: 17TE7DECNS**   Maximum marks: **50**
Semester: **VII**   Duration: **90 Min**

Note: Answer 5 full questions.   **Marks**

(a)	_____ensures that information is in a format that is true and correct to its original purposes. i) Availability ii) Confidentiality iii) Cryptography iv) Integrity	
(b)	_____is the process of giving individuals access to system objects based on their identity. i) Authentication ii) Authorization iii) Signature iv) Integrity	
(c)	Use Caesar's Cipher to decipher the following **HQFUBSWHG** i) ABANDONED ii) ENCRYPTED iii) ENCRYPTES iv) DECRYPTED	1x10
(d)	An attack in which the site is not capable of answering valid request. i) Smurfing ii) Denial service iii) E-mail bombing of iv) Ping storm	
(e)	On Encrypting "**HELLO**" using Monoalphabetic ciphers using the Keyword "**DEQQH**" we get cipher text i) KIPPV ii) KIPVV iii) KIBBV iv) KIBBU	
(f)	Shift ciphers sometimes referred as i) Play fair ii) Caesar iii) Hill iv) Rail fence	
(g)	Key used in the symmetric key cryptography is i) Public key ii) Private key iii) Permanent key iv) Session key	
(h)	Which are the most frequently found letters in the English language? i) E ,T ii) E ,A iii) T, A iii) E , S	
(i)	On double encrypting a plaintext " **CRYPTOGRAPHY**" using rail fence cipher we get i)CYTGAHRPORPY ii)CTAROPYGHPRY iii)CTARAPYGHPRY iv)CTAROPYGHPPY	
(j)	A substitution cipher substitutes one symbol with i) Keys ii) other symbol iii) Multi Parties iv) Single Party	
2	Encrypt the message "**INVESTMENT IN KNOWLEDGE**" using play fair cipher with a key "**INTEREST**". And also give the rules for encryption.	10
3	Encrypt the plaintext "**DON'T LIE TO YOURSELF**" using a hill cipher with a key K=**LIED** and also show the corresponding decryption of the cipher text to recover the original text back	10
4	With neat diagram and necessary equations discuss about symmetric cryptosystem	10
	OR	
5	Encrypt the message "**CHANGE YOUR THOUGHTS AND YOU CHANGE YOUR WORLD**" using Columnar transposition cipher with a key "**451236**" and perform double encryption on cipher text by using rail fence cipher.	10
6	Encrypt the message "**CRYPTOGRAPHY**" using caesar cipher with a key K=7 and also show the corresponding decryption of the cipher text to recover the original text back	10
	OR	
7	Discuss the working of the mono alphabetic ciphers with an example? And also discuss about the strength of mono alphabetic cipher	10