Enrol. No. / ID													

KADI SARVA VISHWAVIDYALAYA
LDRP INSTITUTE OF TECHNOLOGY AND RESEARCH, GANDHINAGAR

			Marks
Q.1	**(A)**	What is security attack, Mechanism and Service ? Explain active attacks in detail.	**[5]**
	(B)	Explain following terms. (1) Access Control (2) Non-repudiation (3) Permutation (4) Data Integrity (5) Diffusion	**[5]**
Q.2	**(A)**	Encrypt the message "hello world" using the hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$.	**[5]**
	(B)	Why block cipher modes of operations are required? List out them and state the application of each.	**[5]**
		OR	
	(A)	Construct a Playfair matrix with the key largest. And encrypt this message "THE ENEMY MUST BE STOPPED AT ALL COSTS. DO WHATEVER IS NECESSARY."	**[5]**
	(B)	Describe SubBytes, ShiftRows, MixColumns and AddRoundKey in AES (Advanced Encryption standard).	**[5]**
Q.3	**(A)**	Perform encryption and decryption using the RSA algorithm for p=3; q=11; e=7; M=5	**[5]**
	(B)	Explain diffie –hellman key exchange algorithm.	**[5]**
		OR	
Q.3	**(A)**	Find the multiplicative inverse of following using extended Euclidean algorithm. (1) 50 mod 71 (2) 43 mod 64	**[5]**
	(B)	(1) Explain fermat little theorem in detail.	**[5]**