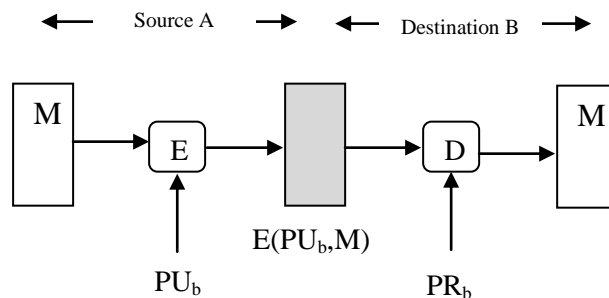
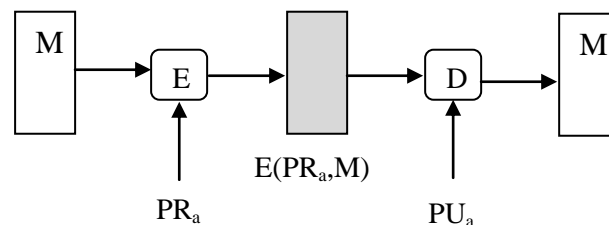


GUJARAT TECHNOLOGICAL UNIVERSITY**BE - SEMESTER-VII (NEW) EXAMINATION – WINTER 2017****Subject Code: 2170709****Date: 07/11/2017****Subject Name: Information and Network Security****Time: 10:30 AM TO 01:00 PM****Total Marks: 70****Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
1. Figures to the right indicate full marks.

		MARKS
Q.1	(a) Discuss the following terms in brief: - Passive attack - Cryptanalysis	03
	(b) What are the essential ingredients of a symmetric cipher?	04
	(c) Explain transposition techniques with appropriate example.	07
Q.2	(a) What are the differences between stream cipher and block cipher?	03
	(b) Which of the following figure provides authentication (only) and which provides confidentiality only? Justify your answer in brief.	04

**(Figure-1)****(Figure-2)**

Where M is plain text message, E is encryption function, D is decryption function, PR_a and PR_b are private keys of Source-A and Destination-B respectively while PU_a and PU_b are public keys of Source-A and Destination-B.

- | | |
|--|-----------|
| (c) Explain Playfair Cipher in detail. Find out cipher text for the following given plain text and key.
Key = GOVERNMENT
Plain text = PLAYFAIR | 07 |
|--|-----------|

OR

	(c)	Discuss Data Encryption Standard with neat sketches.	07
Q.3	(a)	Explain Avalanche effect in DES.	03
	(b)	Write a brief note on hill cipher.	04
	(c)	Explain AES encryption in detail.	07
OR			
Q.3	(a)	State the basic difference(s) between message authentication code and hash function.	03
	(b)	What is meant by meet-in-the-middle attack in double DES? Explain the same in brief.	04
	(c)	Discuss the following block cipher modes of operation in detail with neat sketches:	07
		- Cipher block chaining mode	
		- Counter mode	
Q.4	(a)	Briefly explain source repudiation and destination repudiation.	03
	(b)	Enlist the practical applications of hashing.	04
	(c)	Discuss RSA Algorithm with suitable example.	07
OR			
Q.4	(a)	List the requirements of Public Key Cryptography.	03
	(b)	Calculate the shared secret (K_A and K_B) key using Diffie Hellman Key Exchange Algorithm. Take $q=23$, $\alpha = 5$, $X_A = 6$ and $X_B = 15$.	04
	(c)	Write a detailed note on Secure Hash Algorithm.	07
Q.5	(a)	Explain the concept of Realm in Kerberos in brief.	03
	(b)	Briefly discuss web security threats.	04
	(c)	Explain various general categories of schemes for the distribution of public keys.	07
OR			
Q.5	(a)	Explain HTTPS in brief.	03
	(b)	Briefly discuss the working of SSL Record Protocol.	04
	(c)	Elaborate any one approach to Digital Signatures.	07
