Required Algorithms in Security Package 2015/2016

Requirement	Serial	Algorithm	Input	
			Plaintext	Key
Mandatory	1	General Ceaser.	Text	integer
	2	Monoalphabetic.	Text	Text
	3	Autokey vigenere.	Text	Text
	4	Repeating key Vigenere.	Text	Text
	5	PlayFair.	Text	Text
	6	Hill Cipher.	Text OR Numbers	Text OR Numbers 2X2 OR 3X3
	7	Rail Fence of depth Level n.	Text	Integer (n)
	8	Columnar	Text	Integers
Choose one	9	DES. And 3-DES	Text OR HEX	Text OR HEX
	10	Multiplicative Inverse using Extended Euclid's.	Integers (No., Base)	
		AES.	Text OR HEX	Text OR HEX
Choose two	11	RC4.	Text OR HEX	Text OR HEX
	12	RSA.	Integers (p, q, M, e)	
	13	Diffie-Hellman key exchange.	Integers (q, α, Xa, Xb)	
	14	MD5	TEXT	

- This Package is a team work task, Please Formulate your groups of maximum 6 members
- All the Group members Must be from the same department
- Algorithms from [1 to 8]are mandatory to implement (encryption and decryption and cryptanalysis)
- Choose one algorithm to implement from algorithms [9,10],
- Choose two algorithms to implement from algorithms from [11 to 14]
- Delivery will be scheduled on practical exams week.
- Registration Form click here (https://docs.google.com/forms/d/1KhdgAt0yY5sRb5Eh-Iwe9QNHQvvySb06Rze_b2gD28A/viewform), Registration deadline 31 March 2016.
- You are asked to deliver a dll with the implemented algorithms. A project template will be available maximum by 31 March 2016 in order to automate the algorithms validation.

Prof.Dr. Mohamed Hashem
T.A. (Mirvat Al-Qutt – Hanan Yousry – Salma Khaled – Yomna Mohsen – Hoda Gharib)