Note: Answer seven (7) questions only
Each question (10 mark)

Q1: Tracing the following mathematical procedures
   1. Inverse (3, 26)
   2. Fast exponential (3, 11, 26)

Q2: If (plaintext = Yahoo77) and (n= 62) then
   1. Encrypt and decrypt using Bifid cipher
   2. Encrypt and decrypt using playfair cipher

Q3: If (plaintext = Iraqi) and (key = H4) and (alphabet n = 62) then
   1. Encrypt and decrypt using Vigenère
   2. Encrypt and decrypt using Beaufort

Q4: If (plaintext = 1001110000010111100110010) and (knapsack = [1,2,4,9]) and (w = 15)
   and (w’ = 8) and (n=17) then
   1. Encrypt and decrypt using simple knapsack
   2. Encrypt and decrypt using hard knapsack

Q5: If (plaintext = BC) and (p=11) and (q=13)
   1. Encrypt and decrypt using Polling hellman
   2. Encrypt and decrypt using RSA
Q6: If (plaintext = 01110001110101011001101010101) and the key will be generated using Geffe generator where (LFSR1 = x^4 + x^3 + 1) and (LFSR2 = x^7 + x^6 + 1) and (LFSR3 = x^{10} + x^7 + 1) where the initial key for each LFSR will be as you select.

Q7: Explain in figures the following
1. Encryption and decryption with DES
2. One round with DES in details
3. S-Boxes operations in details
4. Digital Signature in Public Key Cryptography

Q8: From your experience in cryptography suggest modifications on the following method
1. Shrinking generator
2. Geffe Generator

Good Luck

Ass. Prof. Dr. Soukaena Hassan Hasheem