Question 1

I used these tools from http://pythonfiddle.com/binary-finite-field-multiplication/ to calculate GF products

a) The product of x^7+ x^6+ x^4+x^3+x^2+1 and x^7+x^5+ x^3+ x^2+x gives x^6 + x^5 + 1
b) The product of the first and second equations should be 1 for it to be the inverse.

Question 2

By following the slides I implemented a way to calculate the passwords (details on code) ['RAF!MX', 'IZSROR', '.I,BA,', 'AC.B,A', 'ZHKVHG', 'CMDLNJ', '?G.D,N', 'KOGSLE', 'AM!?OU', 'TKCQZA']

Question 3

a) So if we know cp or cq we can take the gcd of one of them and n to find p or q. This is because when we multiply both equations we get cp * cq = k^(2e) * (pq)^e (mod n) which is 0 since pq = n cp * cq is a multiple of n hence taking the gcd of one of them and n will give us a factor of n. Once we found p or q we can find q or p, hence finding the factors of n. Then we are able to decrypt the message.
b) Insanity is doing the same thing, over and over again, but expecting different results.

Question 4

a) The attacker can choose an integer x which is relatively prime to n. Then they can generate a ciphertext c_x by taking the modulus of x to the power e. (c_x = x^e (mod n)). Next, they can multiply c_x with the given ciphertext and give it to the oracle. The oracle will return us with a message m times x to the power of e*d mod N. (c_x * c = (m*x)^(e*d) (mod n)). We know that d is the modular inverse of e so e*d = 1 and since x is relatively prime with n we can multiply each side to get our message. (c_x * c)/x = m (mod n)
b) You discovered my verry secret message:) Bravo