

Math 4100 Quiz 4

Name: _____

1. Hill Cipher: Let $a = 2$, $b = 7$, $c = 3$ and $d = 1$.
 - (a) Encipher the PlainText: EINSTEIN
 - (b) Find the inverse formula.
 - (c) Decipher the CipherText: KDPOMQTS
2. RSA: Let $p = 11$, $q = 17$ and $k = 23$
 - (a) So the public key is ($n = 187$, $k = 23$). Encipher the PlainText: HELLO
 - (b) Find the deciphering exponent.
 - (c) Decipher the CipherText: 1,88,113,64,180,83,35,51
3. Knapsack: Let $S = \{2, 4, 9, 20, 41\}$, $m = 85$ and $b = 63$
 - (a) Compute the public key.
 - (b) Encipher the PlainText: NEWTON
 - (c) Decipher the CipherText: 54,0,59,75,5,13,2
4. ELGAMAL: Let $p = 47$, $r = 19$ and $k = 11$.
 - (a) Compute the public key. That is, (p, r, r^k)
 - (b) Choose your own j and encipher the PlainText: THECAT
 - (c) Decipher the CipherText: $(37,12),(37,43),(37,5),(37,34),(37,6),(37,34),(37,0),(37,5)$
5. This problem is unrelated to Cryptography. For the following sequence

$1, 11, 111, 1111, 11111, 111111, \dots$

it is easy to see that 1 is a perfect square ($1^2 = 1$), while 11 is not. Find all the perfect squares in this sequence and prove your answer.

6. Explain the difference between a public key system and a private key system. What are some of the advantages and some of the disadvantages of each? Use proper English.
7. The following message was sent to the professor using RSA enciphering with public key ($n = 4757, k = 143$)

4184, 2717, 3246, 1772, 0401

Crack the message.