COMPSCI 4CR3 - Assignment 3

1. (45 points) Let $a, m > 0$ be n-bit integers such that $\gcd(a, m) = 1$.

   (a) How can we use Euler's theorem to compute the inverse of a modulo m.

   (b) Show that we can also compute a^{-1} mod m using the Extended Euclidean Algorithm.

   (c) Implement your algorithms for (a) and (b), and run the algorithms on the following input:
   $a = 109536956202570255640303367305951471998565784606099903800127275419371$
   $203612871447511034347295983315808389427749958007877011675170788731306635$
   $0958894258,$
   $m = 148684946254813103839107574453201833974896959303081166542920455715589$
   $877138635251282146324575518333688378500756427295157965132554028777985134$
   $8210497897.$
   What is a^{-1} mod m? Which algorithm is faster? What are the running times of the algorithms in milliseconds. (No need to include the source code)

2. (30 points) Recall that in class we discussed that, in an RSA public key (n, e), e the exponent e is often chosen to be a small value. The reason for this choice is to speed up the encryption process. Now, consider the following RSA public key:
   $n = 508281196310201376192554864656699346831575429768465482788715190735760361687281737746563113895010157,$
   $e = 7.$

   (a) Alice wants to encrypt the plaintext $x = 38745745356349$. Explain why, if Trudy knows that the plaintext x is small enough (as it is in this case), he can recover x.

   (b) Find the small plaintext corresponding to the ciphertext $y = 4066488477440339689$
   $911514138508998613662966982287543919056006242924596335364286584668317646217011.$

3. (25 points) Suppose there is a `key-gen` server that generates RSA public keys. Bob queries the server and receives a key pair $(n, e_1), d_1$, where n is the modulus, and e_1, d_1 are the public and private exponents, respectively. Alex also queries the server for a public key. By chance (albeit with low probability), he receives the key pair $(n, e_2), d_2$, where the modulus n is the same as Bob's. Assume that $\gcd(e_1, e_2) = 1$. Now, Alice wants to send a message to her friends, including both Bob and Alex. Explain how Trudy, having access to the public keys (n, e_1) and (n, e_2), and the ciphertexts sent to Bob and Alex, can recover Alice's original message.