CSI4108 / SEC5101
(Fundamentals of) Cryptography

Assignment #3
Due: Friday, November 11, 2022 (before 16:00, to be submitted via Brightspace)

All questions in this assignment are to be done individually (i.e., not working with anyone else). Choose your own values for all variables other than t, e, and m.

1. **[1.5 marks]** A description of the Elgamal public key encryption algorithm can be found in many places, including Stallings 7th ed., pp. 300-303 (5th ed., pp. 305-308; 6th ed., pp. 292-294).

   Implement a toy version of this algorithm with prime $q = 89$ and primitive root $\alpha = 13$ (the "implementation" can be done in software or on paper, as long as you show your work). Demonstrate that encryption and decryption perform correctly. If two messages, m_1 and m_2, have been encrypted using the random integer $k = 37$, compute the value of m_2 if you know that $m_1 = 56$.

2. **[2 marks]** Implement the Miller-Rabin probabilistic primality testing algorithm to find a 14-bit integer that is probably prime with confidence $t = 5$. (Actually implement the Miller-Rabin algorithm; don't just call it from some library or toolkit.) Is your "probable prime" in this table: https://primes.utm.edu/lists/small/10000.txt ?

3. **[4 marks]** For this question you may use any big integer library or toolkit you wish in order to explore cryptographic algorithms with more realistically-sized numbers than are possible in a classroom setting.

   a. Using RSA with 1024-bit primes p and q and a public exponent $e = 65537$, encrypt the message $m = 466921883457309$. Use the Chinese Remainder Theorem to decrypt the resulting ciphertext c; how long does it take compared to decryption without using CRT (show your timing results if possible)?

   b. Using elliptic curve $E_p(a,b)$, where p is a 256-bit prime number and a and b are any appropriate integers, choose private and public values for both Alice and Bob and compute their shared secret, s, using ECDH. Show that both parties can compute the same s. Compare the speed of computing s using ECDH and using "ordinary" D-H at the same security level (show your timing results if possible).