CSI 4108
Cryptography

Assignment #4
Due: Friday, December 1, 2017 (before 16:00)

1. *Sage* (https://cloud.sagemath.com/) is a free, open-source mathematics package that allows the user to quickly and easily do many things (such as calculus, number theory, algebra, graph theory, etc.), including cryptography. For this assignment you can use Sage or any other library or toolkit you wish in order to explore various cryptographic algorithms with more realistically-sized numbers than are possible in a classroom setting. Note that to use Sage, you will need to set up a Sage account and open a worksheet (you can view some published Sage worksheets to help you get started; see also Stallings, *Cryptography and Network Security, 6th ed.*, Appendix B, and http://doc.sagemath.org/html/en/tutorial/index.html for helpful tutorials). Once completed, worksheets may be printed and handed in. **[4 marks]**

a. Using RSA with 1024-bit primes p and q and a public exponent e of 65537, encrypt the message m = 399621883454709. 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 512-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).

2. Using 10-bit primes p and q, an appropriate seed, and a simple calculator, compute the first 20 outputs of the Blum, Blum, Shub (BBS) pseudorandom bit generator. What size primes would be required for real-world security of minimally sensitive information (e.g., if the BBS output string was used for encryption in a Vernam cipher setting)? What size primes would be required to match the security of AES-128? **[2 marks]**

3. Consider elliptic curve $E_{2^5}(g^3, g^2)$ with irreducible polynomial $x^5 + x^2 + 1$. Using the generator representation, show all the elements of the field as powers of g and as the corresponding binary strings, and find 3 points on this curve. **[2 marks]**