CSc 4222/6222 – Assignment #5

Deadline: Wednesday, November 29th (midnight) / Late Deadline: Sunday, December 3rd (noon)

Make sure to justify all of your answers clearly – show all of your work
No handwritten submissions

1. What is the encryption of the following string using the Caesar cipher: INFORMATIONSECURITY
2. What are the substitutions for the decimal numbers 13, 8, and 4 using the following S-box:

	00	01	10	11
00	0011	0100	1111	0001
01	1010	0110	0101	1011
10	1101	1110	0100	0010
11	0111	0000	1001	1100

3. Compute the multiplicative inverse of 7 in Z_{23}.
4. Show the steps and intermediate results of applying the extended Euclidean algorithm to compute the GCD of 512 and 240.
5. Show the result of an Elgamal encryption of the message M = 9, using *k* = 4 for the public key (*p*,*g*,*y*) = (59, 2, 25)
6. Demonstrate that the hash function H(x) = 5x + 11 mod 19 is not weakly collision resistant, for H(4).
7. Use Euler's Theorem, not repeated squaring, to compute 20^{10211} mod 10401.