Homework # 4 Due 11pm on Sat Feb 29

CS 178 Intro to Crypto

1. In the AES algorithm, compute the following and give the results in polynomial, hex, and binary notations:
   (a) SubBytes($x^7 + x^6 + x^5$)
   (b) SubBytes($A7$)
   (c) SubBytes(10010110)

2. Suppose the key for round 0 in AES is zero (consisting of 128 bits of 0s).
   (a) Show that the key for the first round is $W(4), W(5), W(6), W(7)$, where

$$W(4) = W(5) = W(6) = W(7) = \begin{pmatrix} 01100010 \\ 01100011 \\ 01100011 \\ 01100011 \end{pmatrix} = [62, 63, 63, 63]^T$$

   (b) Show that $W(8) = W(10) \neq W(9) = W(11)$ (Hint: This can be done without computing $W(8)$ explicitly).

3. Consider the prime $p = 9929$ and the primitive element 2.
   a) Show the steps of the Diffie-Hellman between Alice and Bob for $a = 1983$ and $b = 2014$.
   b) What is the value of the agreed secret key?

4. The ciphertext 5859 was obtained from the RSA algorithm using $n = 11413$ and $e = 7467$. Using the factorization $11413 = 101 \cdot 113$, find the plaintext.

5. RSA with three primes would also work: $n = pqr$, $\phi(n) = (p-1)(q-1)(r-1)$, $\gcd(e, \phi(n)) = 1$, and $d = e^{-1} \pmod{\phi(n)}$.
   a) Setup an example RSA public/private key pair using primes 29, 31, 37, and $e = 17$.
   b) Encrypt $m = 10000$ and then decrypt the ciphertext.
   c) Explain why 3-prime RSA is not preferred.