Cryptography: Assignment 3

Due: 11:59 pm, Wednesday, March 3, 2021
Total Marks: 100

Both undergraduate and graduate students should complete all 5 questions and submit their completed assignments to the Assignment 3 folder in Brightspace.

Show all your work in your submitted solutions. Although it is tempting to write programs to answer some questions, be sure to apply the algorithms by hand so that you get familiar with the steps involved.

Question 1 (25 MARKS)

Consider a "block" cipher (of 4-bit blocks) constructed as an affine cipher based on finite field GF(2^4) generated with the irreducible polynomial $m(x) = x^4+x^3+1$. A 4-bit plaintext block, x, is encrypted into a 4-bit ciphertext block, y, with key $k_{enc} = (a, b)$ using

$$y = a\cdot x + b$$

where operations are defined according to the finite field. Note that a and b are 4-bit values. Encryption key $k_{enc} = (a, b) = (0101, 1101)$ is selected for the system.

(a) Derive the sequence of ciphertext blocks for the following plaintext inputs, where the leftmost block is first:

1011, 0111, 0111

using (i) ECB mode, (ii) CBC mode, and (iii) counter mode.
For CBC and counter modes, assume an initialization vector / initial count of 1001. The counter in counter mode should behave as a binary counter so that for each block operation, the count is incremented by 1. For example, count value of 0101 would increment to 0110 for the next block. For counter mode, all bits of the block are used as keystream in the XOR operation to produce the ciphertext.

(b) Derive the decryption key $k_{dec} = (c, d)$ for $k_{enc} = (a, b) = (0101, 1101)$.
Note that, although you could use the Extended Euclidean algorithm to find any necessary inverses, for convenience all inverses in the field are listed below:

$(0001)^{-1} = 0001$, $(0010)^{-1} = 1100$, $(0100)^{-1} = 0110$, $(1000)^{-1} = 0011$,
$(1001)^{-1} = 1101$, $(1011)^{-1} = 1010$, $(1111)^{-1} = 0101$, $(0111)^{-1} = 1110$

(c) Now given the following sequence of ciphertexts (leftmost first), derive the sequence of plaintexts:

0101, 0000, 0101

using (i) ECB mode, (ii) CBC mode, and (iii) counter mode. Assume that the IV / initial count is 0100 for CBC and counter modes.

Question 2 (20 MARKS)

(a) **By hand**, execute the Euclidean algorithm to calculate the greatest common divisor of the following pairs:

(1) 69 and 89 (2) 142 and 217 (3) 222 and 351

(b) **By hand**, execute the Extended Euclidean algorithm and compute the following multiplicative inverses, if such an inverse exists:

(1) 34^{-1} (mod 81) (2) 117^{-1} (mod 209) (3) 213^{-1} (mod 621)

Question 3 (20 MARKS)

(a) Using Fermat's theorem, find

(i) 10^{37} mod 37 and (ii) 10^{110} mod 37.

(b) Find the factors of 539 (by trying division by primes up to $\sqrt{539}$). If possible, make use of Euler's theorem to find

(ii) 66^{843} mod 539 and (ii) 20^{843} mod 539.

For each case, explain why you are able to or not able to apply Euler's theorem.

(c) Simplify $(25)^{802}$ mod 187. (HINT: Do not use the square-and-multiply algorithm, but consider whether Fermat's theorem or Euler's theorem can be used.)

Question 4 (20 MARKS)

(a) Using the square-and-multiple algorithm **by hand**, perform encryption for the following RSA cryptosystems and given plaintexts:

(1) $p = 13$, $q = 17$, $b = 11$, Plaintext: $x = 14$

(2) $p = 19$, $q = 29$, $b = 13$, Plaintext: $x = 137$

(b) Using the square-and-multiple algorithm **by hand**, perform decryption for the following RSA cryptosystem and given ciphertext:

$p = 13$, $q = 17$, $b = 5$, Ciphertext: $y = 48$

(c) For the RSA cipher parameters $p = 13$ and $q = 23$, what would be the problem with selecting public key exponent $b = 9$?

Question 5 (15 MARKS)

In an RSA cryptosystem, the public key exponent is $b = 83$ and modulus $n = 713$. Given the ciphertext received is 162, what is the plaintext sent? (HINT: Find the factors of n using trial-and-error division, not the Miller-Rabin algorithm.)