WILFRID LAURIER UNIVERSITY
LAURIER
Inspiring Lives.

CP460– Applied Cryptography – Fall 2024
Assignment 2

Due: Nov 20, 2024, 11:59 pm

Assignment Overview (10 Marks)

There are five tasks. Submit one file (a .pdf file for Task 1 to 5) to Assignment 2 Dropbox folder.

Task 1: Finite Field (2 Marks)

Compute in GF(2^8):

$$(x^4+x+1)=(x^7+x^6+x^3+x^2)$$

where the irreducible polynomial is the one used by AES, namely $P(x) = x^8+x^4+ x^3 +x+1$. Note that Table 4.2 contains a list of all multiplicative inverses for this field.

Task 2: Modes of Operation (2 Marks)

Propose a simple change to the OFB mode that encrypts one byte of plaintext at a time, e.g., for encrypting key strokes from a remote keyboard. The block cipher used is AES. Perform one block cipher operation for every new plaintext byte. Draw a block diagram of your scheme and pay particular attention to the bit lengths used in your diagram.

Task 3 RSA (2 Marks):

Computing modular exponentiation efficiently is central to using RSA in practice. Compute the following exponentiations x^e mod m using the square-and-multiply algorithm:

1. **x = 2, e = 79, m = 101**
2. **x = 3, e = 197, m = 101**
3. **x = 5, e = 54, m = 151**
4. **x = 8, e = 127, m = 151**

After every iteration step, show the exponent of the intermediate result in binary notation.

Task 4: Diffie-Hellman Key Exchange (DHKE) (2 Marks)

Assume Bob sends an Elgamal-encrypted message to Alice consisting of two pieces of plaintext. Since Bob is lazy, he applies the scheme incorrectly and uses the same parameter *i* for all messages. Assume we know that each of Bob's plaintexts starts with the number $x_1 = 21$, which happens to be Bob's ID. We now obtain the

following ciphertexts:

$(k_{E,1} = 6; y_1 = 12)$

$(k_{E,2} = 6; y_2 = 14)$

The Elgamal parameters are p = 31;a = 3;b = 18. Determine the second plaintext x_2.

Task 5 : ECC (2 Marks):

Given are the following elliptic curves:

$$\begin{aligned} E_1: &\quad y^2 \equiv x^3 + 5x + 4 \bmod 11 \\ E_2: &\quad y^2 \equiv x^3 + 15x + 29 \bmod 28 \\ E_3: &\quad y^2 \equiv x^3 + 12x + 11 \bmod 13 \end{aligned}$$

Which one is suited for use in a cryptosystem? Justify your answer!

Remark: You do not need to consider security-relevant attributes such as size of primes etc.

Good luck with your assignment!