**Nova Southeastern University**

**College of Computing and Engineering**

**ISEC 620 Applied Cryptography**

**Fall 2020**

**(August 17– December 6, 2020)**

Written Assignment #2

Due Date: October 4, 2020

Instructor: Dr. Junping Sun

1. What is the difference between a block cipher and stream cipher? (10 points)

A **Block** **Cipher** can convert more bits then a **Stream** **Cipher**, this is because a Stream Cipher only converts by one Byte at a time which is 8 Bits. Theoretically since A Block Cipher converts by the block, it can convert 64 bits and up at a time. Decryption is more complex on a Block Cipher compared to a Stream Cipher. Also, the Block Cipher is a Feistel Cipher while the Stream Cipher is a Vernam Cipher. Since a Stream Cipher is less complex it is faster and less resource intensive while the Block Cipher is more cryptographically secure but also more resource intensive.

2. What is the difference between diffusion and confusion? (15 points)

**Confusion** aims to protect cryptographic integrity by using substitution. This confuses the cracker by ensuring the cipher text does not give way to the plaintext. An example of this would be the plain text “ABC” becoming the cipher text “XYZ” This way the assailant should be confused on what the original value of what “XYZ” was if they were able to obtain the cipher text.

**Diffusion** aims to protect cryptographic integrity using permutation through transposition. An example of this would be the plaintext “ABC” becoming the ciphertext “BCA”. This leaves the Ciphertext diffused making it hard for the algorithm cracker to fuse the plaintext back together.

So, in conclusion, Confusion is based off Substitution while Diffusion is based off transposition.

3. Which parameters and design choices determine the actual algorithm of a Feistel cipher? (35 points)

When it comes to a **Feistel Cipher** design choice’s the following come into discussion.

**Block Size:** The larger the size the more security but slower speeds. Generally, A Good block size is at least 128 bits for example as used in AES.

**Key Size:** The larger the sizes the more security but slower speeds. 128 bits or larger have become the new defacto standard compared to 64 bits which is considered inadequate.

**Number of Rounds:** More rounds the more security but slower speed. 1 round is not enough and typically there are at least 16 rounds.

**How the subkey is generated:** The more complex it is the harder it should be for cryptanalysis.

**Round function complexity:** The more complex it is the harder it should be for cryptanalysis, keeping in mind one might want to make an algorithm able to cryptanalyze so they can debug, learn from, and harden it.

4. What is the difference between differential and linear cryptanalysis? (10 points)

A **Linear cryptanalysi**s is known as a plaintext attack, in this the attacker gains insight about the algorithm by finding linear relations between bits of the plaintext, the ciphertext, and the key, in a piece by piece format. This is done by decrypting each cipher by trying all possibilities of sub-keys for one round of encryption. Then analyzing the cipher texts random results to derive the key.

In a **Differential Cryptanalysis**, the attacker puts different inputs to the encryption algorithm and studies the corresponding outputs. This compares the differences and analyzes where similarities and non-random behavior occurs compared to other inputs. This is called differential because it compares the differences between different inputs.

5. List three classes of polynomial arithmetic. (15 points)

**Ordinary Polynomial Arithmetic:**

Uses basic rules of algebra.

**Polynomial Arithmetic in Which the Arithmetic on Coefficients is performed modulo P:** Arithmetic on coefficients is performed over a finite field such the coefficients being in GF(P).

**Polynomial Arithmetic where Coefficients are in GF(P) and Polynomials are defined a Modulo M(X) whose highest power is an Integer N:**

Same as prior and polynomials are defined a modulo M(x) whose highest power is some integer N.

6. Does the set of residue classes modulo 3 form a group? (10 points)

1. with respect to addition?

No, it will NOT form a group with respect to modular addition.

This can be proven by showing that the inverse element A for 1 can NOT be determined.

**Inverse Addition:**

Example: A=1.

Residue Class of 1 = (… -10, -7, -4, 1, 4, 7, 10 …)

Let’s consider A=1, B= -4, C= -7

Formula: if(A+B) = ((A+C)Mod3) then B = ((C)Mod3)

Simplified: (1-4)=(1-7)mod3🡺-3=((-6)mod3)🡺 FALSE

Since, (-3) ≠ ((-6)mod3) , the inverse element A for 1 can NOT be determined making it un-

able to form a group in respect to modular addition.

1. with respect to multiplication?

Yes, it WILL form a group with respect to modular multiplication.

**Inverse Multiplication:**

Example: A=1.

Residue Class of 1 = (… -10, -7, -4, 1, 4, 7, 10 …)

Let’s consider A=1, B= 4, C= 7

Formula: if (A-1)(A\*B) = ((A-1)((A\*C))(Mod3) then B = (C)(Mod3)

Simplified: if (1-1)(1\*4) = ((1-1) (1\*7))(Mod3) 🡺4= 7mod3 🡺TRUE

Since, 4= 7mod3, the inverse property is satisfied showing that the residue class of modulo

3 CAN form a group with respect to modular multiplication.

7. Find integers *x* such that:

The following were found by trying all possibilities to match the argument until enough matches were found to deduce the value of integers x.

1. 5*x* ≡ 4 (mod 3) (5 points)

Means 5x -4 is a multiple of 3.

This will be true for all integers x =2, 5, 8, 11, 14 … (3N-1).

1. 7*x* ≡ 6 (mod 5) (5 points)

Means 7x-6 is a multiple of 5.

This will be true for all integers x = 3, 8, 13, 18, 23…(5N-2).

1. 9*x* ≡ 8 (mod 7) (5 points)

Means 9x-8 is a multiple of 7.

This will be true for all integers x= 4,11,18,25 …(7N-3).

8. In this text we assume that the modulus is a positive integer. But the definition of the expression *a* mod *n* also makes perfect sense if *n* is negative. (20 points)

Determine the following:

1. 5 mod 3

5Mod3 = 2+(3\*1) = 2Mod3 =2,

So that 1 is the Quotient and 2 is the remainder.

1. 5 mod -3

5mod-3 = -1+(-3\*-2) = -1Mod-3 =-1

So that -2 is the Quotient and -1 is the remainder.

1. -5 mod 3

-5mod3 = 1+(3\*-2) = 1mod3 =1,

So that -2 is the Quotient and 1 is the remainder.

1. -5 mod -3

-5mod-3 = -2+(-3\*1) = -2mod-3 =-2,

So that 1 is the Quotient and -2 is the remainder.

9. A modulus of 0 does not fit the definition, but is defined by convention as follows:

*a* mod 0 = *a*.

With this definition in mind, what does the following expression mean:

*a* ≡ *b* (mod 0) (10 points)

if A Mod 0 =A,

then B Mod 0 =B.

So that A=B Mod 0,

is the same as A=B.

So, the expression means A=B.

10. Using the extended Euclidean algorithm, and find the multiplicative inverse of

1. 1234 mod 4321 (5 points)

**Extended Euclidean Algorithm**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **i** | **ri** | **qi** | **xi** | **yi** |
| -1 | 4321 |  | 1 | 0 |
| 0 | 1234 |  | 0 | 1 |
| 1 | 619 | 3 | 1 | -3 |
| 2 | 615 | 1 | -1 | 4 |
| 3 | 4 | 1 | 2 | -7 |
| 4 | 3 | 153 | -307 | 1075 |
| 5 | 1 | 1 | 309 | -1082 |
| 6 | 0 | 3 |  |  |

Ax+ by = d = gcd(a,b)

If (gcd(a,b) =1) then y = multiplicative inverse of b( y=b-1)

a = 4321, b = 1234, x = 309, y = -1082

(4321\*309) + (1234\*-1082) = (1335189-1335188) = 1

Since gcd(a,b) = 1, **then -1082 is the multiplicative inverse.**

1. 24140 mod 40902 (5 points)

**Extended Euclidean Algorithm**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **i** | **ri** | **qi** | **xi** | **yi** |
| -1 | 40902 |  | 1 | 0 |
| 0 | 24140 |  | 0 | 1 |
| 1 | 16762 | 1 | 1 | -1 |
| 2 | 7378 | 1 | -1 | 2 |
| 3 | 2006 | 2 | 3 | -5 |
| 4 | 1360 | 3 | -10 | 17 |
| 5 | 646 | 1 | 13 | -22 |
| 6 | 68 | 2 | -36 | 61 |
| 7 | 34 | 9 | 337 | -571 |
| 8 | 0 | 2 |  |  |

Ax+ by = d = gcd(a,b)

If (gcd(a,b) =1) then y = multiplicative inverse of b( y=b-1)

a = 40902, b = 24140, x = 337, y = -571

(40902\*337) + (24140\*-571) = (13783974-13783940) = 34

Since gcd(a,b) = 34, **then there is NO multiplicative inverse.**

1. 550 mod 1769 (5 points)

**Extended Euclidean Algorithm**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **i** | **ri** | **qi** | **xi** | **yi** |
| -1 | 1769 |  | 1 | 0 |
| 0 | 550 |  | 0 | 1 |
| 1 | 119 | 3 | 1 | -3 |
| 2 | 75 | 4 | -4 | 13 |
| 3 | 45 | 1 | 5 | -16 |
| 4 | 29 | 1 | -9 | 29 |
| 5 | 16 | 1 | 14 | -45 |
| 6 | 13 | 1 | -23 | 74 |
| 7 | 3 | 1 | 37 | -119 |
| 8 | 1 | 4 | -171 | 550 |
| 9 | 0 | 3 |  |  |

Ax+ by = d = gcd(a,b)

If (gcd(a,b) =1) then y = multiplicative inverse of b( y=b-1)

a = 1769, b = 550, x = -171, y = 550

(1769\*-171) + (550\*550) = (-302,499+302500) =1

Since gcd(a,b) = 1, **then 1769 is the multiplicative inverse.**

11. Develop a set of tables similar to Table 5.1 for GF(5). (20 points)

**Addition:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| + | 0 | 1 | 2 | 3 | 4 |
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

**Multiplication:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| x | 0 | 1 | 2 | 3 | 4 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

**Additive and Multiplicative Inverses:**

|  |  |  |
| --- | --- | --- |
| x | -x | x-1 |
| 0 | 0 | - |
| 1 | 4 | 1 |
| 2 | 3 | 3 |
| 3 | 2 | 2 |
| 4 | 1 | 4 |

12. Develop a set of tables similar to Table 5.3 for GF(4) with *m*(*x*) = *x*2 + *x* +1 (20 points)

**Addition:**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | 000 | 001 | 010 | 011 |
|  | + | 0 | 1 | x | x+1 |
| 000 | 0 | 0 | 1 | x | x+1 |
| 001 | 1 | 1 | 0 | x+1 | x |
| 010 | x | x | x+1 | 0 | 1 |
| 011 | x+1 | x+1 | x | 1 | 0 |

**Multiplication:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 000 | 001 | 010 | 011 |
|  | x | 0 | 1 | x | x+1 |
| 000 | 0 | 0 | 0 | 0 | 0 |
| 001 | 1 | 0 | 1 | x | x+1 |
| 010 | x | 0 | x | x+1 | 1 |
| 011 | x+1 | 0 | x+1 | 1 | x |