**Homework for Section#2 (Approximate due date Aug 31st , 2020)**

1. Pick one prime number ***p*** greater than 5
	1. Generate the multiplication tables mod ***p***
	2. Find the inverses mod ***p*** for all numbers k ∈ $Z\_{p}$ :{1, 2, …, p-1}
	3. Validate Fermat: $5^{p-1}≡1 mod p$ (using arithmetic of 2.1)
	4. Validate Wilson: (p-1)!$≡-1 mod p$
	5. Check that $\left(\genfrac{}{}{0pt}{}{p}{5}\right)≡0 mod p$
2. Compute the Euler parameter $ф\_{3p}$
	1. Generate the multiplication tables mod 3***p***
	2. Find the inverses all numbers k ∈ $z'\_{3p}$ : {$a\_{1}$*,* $a\_{2}$*, …,* $a\_{ф\_{3p}}$}
	3. Verify Euler: $11^{ф\_{3p}}≡1 mod 3p$
	4. Check: (3p-1)!$≡0 mod 3p$
	5. Check (3p-1)! – (p-1)! ≡1 mod 3p

**Homework for section 9B**

Based on the circular group **ℱ**$2^{4}$

$y^{2}+xy$***≡***$x^{3}$***+***$g^{4}x^{2}$***+1 mod P(x)***

Irreducible ***P(***$x$***)*=** $x^{4}$ **+** $x$ **+1**

Generator ***g = (0010)***

Primitive element: P = ($g^{12}$, $g^{12}$)

Verify several points:

Point doubling 1: ($1$, $g^{13}$) + ($1$, $g^{13}$)

Point doubling 2: ($g^{5}$, $g^{3}$) + ($g^{5}$, $g^{3}$)

Point addition 1: ($g^{3}$, $g^{13}$) + ($g^{12}$, $0$)

Point addition 2: ($g^{3}$, $g^{8}$) + ($g^{5}$, $g^{3}$)

**Homework for Section#3 (approximate due date Sept 7th, 2020)**

-Decipher the following cipher text, and uncover the key for Caesar:

 **Alphabet:** abcdefghijklmnopqrstuvwxyz1234567;,./

 Cipher text 🡺U742 ,wt P7pqxr ;xu7 awxrw 2tp3 dt74n,wx; ,.73ts x3,4 rx5wt7 u47 p r43rtp1ts 2t;;pvtn P1;4 ,.73ts x3,4 rxu7t ,wt rwxuu7t x3

 u7t3rw awxrw 2tp3 3.2qt7n

- Use a 5-bit key to encrypt this message with Vigenere

Link: <https://cryptii.com/pipes/caesar-cipher>

**Homework for section#4 (approximate due date Sept 7th, 2020)**

- Find the 32-bit substitutions of the following 48-bit data streams with the S-Box of DES:

 Stream #1 🡺111010 001010 011010 101001 101110 110101 010001 110010

 Stream #2 🡺010101 110011 011011 101110 110101 101011 101010 111001

* Using DES key processor, find the first 4 sub-keys of:

 Key#1 🡺0110110101100101011010010111010101010001101001101101000101010110

 Key#2 🡺1101001001101011001000110101010101110110010011101011101010001101

* Using DES online tool, find the cipher text of the following data streams:

 Stream#1 🡺1010011001001110010011010101110010100110101011001101101001001011

 Stream#2 🡺0111000100111001001100010110011101100011011010011100100011101100

Example of resource: <https://www.tools4noobs.com/online_tools/encrypt/>

**Homework for section#5A (approximate due date Sept 14th, 2020)**

1-Arithmetic in extended Galois field with $GF \_{2^{8}}$; $P \_{(x)}$ ***=*** $x^{8}$ ***+*** $x^{4}$ ***+*** $x^{3}$ ***+*** $x$ ***+ 1***

 **Compute the following elements**:

1/21; 1/9f; 1/ab; 1/cd

2-Arithmetic in extended Galois Field with $GF \_{2^{3}}$ *;* $P \_{(x)}$ ***=*** $x^{3}$***+*** $x$***+ 1***

 Represented by polynomials: $A \_{(x)}$ *=*$ a\_{2}$$x^{2}$ *+* $ a\_{1}$$x $*+* $ a\_{0}$

 Elements: *(****0****,* ***1****,* $x $*,* $x $***+1****,* $x^{2}$*,* $x^{2}$***+1****,* $x^{2}$***+*** $x $*,* $x^{2}$***+*** $x $***+1****)*

 Find the 8 inverses:

**Compute the following:**

$x^{2}$**+1 ⨸** $x^{2}$**+** $x $**=?**

$x^{2}$**+** $x $**⨸** $x^{2}$**+1 =?**

 **Optional:**

$x^{2}$**+** $x$ **⊗** $x^{2}$**+** $x $**=?**

$x^{2}$**+** $x$ **+1⊗**$ x^{2}$**+** $x$**=**?

**Homework for section#5B (approximate due date: Sept 28th, 2020)**

**Part 1 Encryption:** Find the stream {C0 C1 C2 C3} from the initial steam {A0 A5 A10 A15}

|  |  |  |  |
| --- | --- | --- | --- |
| Initial | Inverse | After affine | After shift& Mix column |
| $$A\_{i}$$ | $$B'\_{i}$$ | $$B\_{i}$$ | $$C\_{i}$$ |
| A0 = 0101 1010 | B’0 =? | B0 =? | C0 =? |
| A5 = 0101 1001 | B’5 =? | B5 =? | C1 =? |
| A10 = 1010 0110 | B’10 =? | B10 =? | C2 =? |
| A15 = 1101 0001 | B’15 =? | B15 =? | C3 =? |

**Part 2 Decryption:** Find the stream {A0 A5 A10 A15} from the initial steam {C0 C1 C2 C3}

|  |  |  |
| --- | --- | --- |
| Initial | After reverse shift & Mix column | After reverse byte substitution |
| $$C\_{i}$$ | $$B\_{i}$$ | $$A\_{i}$$ |
| C0 = 1001 1100 | B0 =? | A0 =? |
| C1 = 1100 0101 | B5 =? | A5 =? |
| C2 = 0111 0001 | B10 =? | A10 =? |
| C3 = 0010 1101 | B15 =? | A15 =? |

**Homework for Section#6A (due date September 28th, 2020)**

**Alice uses the two following random numbers:**

* 1. Random numbers for polarizer (0=+ ; 1=x) are:

10101100 11110110 01000110 11000111 10001110 01011110 00001011 10100110

 00011001 11100001 01100001 11100001 10111001 00111010 01111111 11000101

 10101110 10001110 11001011 10000100 01000010 10100010 11010110 01001011

01101100 10100100 11100000 10101010 00101011 00110101 11111101 10011110

 b. Random numbers for data stream are:

01100111 00110001 10001101 10010011 11101000 01001111 10010011 01001000

00000001 00001011 10100111 01101001 00000101 01100101 10011101 00111000

10000010 11001110 00100000 10110110 10001100 10000011 00010111 11001100

11010000 00001001 10001111 00001011 10001000 01001010 01000100 01011111

**Bob random numbers for polarizer (0=+ ; 1=x) are:**

10100000 00000011 01111000 01010011 10001110 00000010 10000110 11001111

10100011 00101001 11010101 11111000 11001101 00011011 11110010 11111010

00001010 11110010 10100000 11001001 10100011 10010111 11111110 10000100

00100100 10000001 11000011 00100010 10010000 11011110 10100111 10010101

**QUESTION: Find two possible sequences of matching positions to send the following key:**

 00110100 00111001 11101101 01110100 10010001 10101101 10111101 00110001

**Homework for section 6B (approximate due date: Oct 5th, 2020)**

**Question 1:**

Pick two prime numbers p and q (between 5 and 37), N=pq;

Use Shor algorithm to find p and q from N:

* + 1. Pick a number ***a*** smaller than N
		2. Find the integer **r** verifying $f(r) = a^{r}$ **mod N**
		3. If r odd find a different ***a***
		4. Compute $a^{r/2}-1$ and $a^{r/2}+1$
		5. If the gcd is not uncovering **p**, and **q**, pick a different ***a***

**Question 2**:

Find the Discrete Fourier Transform (DFT) matrix for N=2, then for N=4:



 $w$ **=** $e^{2πi/N }$

**Homework for section 7 (due date tbd)**

**Question 1: Use on-line SHA-2 calculator:**

a) Pick a portion of your resume

b) Hash it with SHA-2

c) Modify one character

d) Hash it with SHA-2

f) Verify the differences in the resulting message digests

**Question 2: Create a blockchain**

1. Segment parts of your resume in 3 blocks
2. Hash the first part: H1
3. Hash (H1 + Part2): H2
4. Hash (H2 + Part 3): H3
5. Modify one character to verify the resulting message digests

**Homework for section 8A - part 1 (due date tbd)**

Use EA to find: gcd(9135,8070) and gcd(11296,8976)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **i** | **ri-1** | **ri** | **qi**  | **ri+1** |
| 1 | r0 =  | r1 =  | q1 =  | r2 =  |
| 2 | r1 =  | r2 =  | q2 =  | r3 =  |
| 3 | r2 =  | r3 =  | q3 =  | r4 =  |
| 4 | r3 =  | r4 =  | q4 =  | r5 =  |
| 5 | r4 =  | r5 =  | q5 =  | r6 =  |
| 6 | r5 =  | r6 =  | q6 =  | r7 =  |
| 7 | r6 =  | r7 =  | q7 =  | r8 =  |
| 8 | r7 =  | r8 =  | q8 =  | r9 =  |
| 9 | r8 =  | r9 =  | q9 =  | r10 =  |
| 10 | r9 =  | r10 =  | q10 =  | r11=  |

**Homework for section 8A - part 2: (Due date tbd)**

**F**ind **S** and **T** for 11296 and 8976

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| $$i$$ | **R**$$R\_{i}$$ | **Q**$$Q\_{i}$$ | **S**$$S\_{i}$$ | **T**$$T\_{i}$$ | **EA**$R\_{i}$ = $Q\_{i+1}R\_{i+1}+R\_{i+2}$ | **EEA: S** $S\_{i}$ = $S\_{i-2}$ – $Q\_{i-1}$ $S\_{i-1}$ | **EEA: T** $T\_{i}$ = $T\_{i-2}$ – $Q\_{i-1}$ $T\_{i-1}$ |
| **0** | $R\_{0}$ = | - | $S\_{0}$ = **1**  | $T\_{0}$ = 0 | R0 = $Q\_{1}$ R1 + R2 |  |  |
| **1** | $R\_{1}$ = | $Q\_{1}$ = | $S\_{1}$ = **0**  | $T\_{1}$ = **1** | R1 = $Q\_{2}$ R2 + R3 |  |  |
| **2** | $R\_{2}$ =  | $Q\_{2}$ = | $S\_{2}$ =  | $T\_{2}$ =  | R2 = $Q\_{3}$ R3 + R4 | S2 = S0 – $Q\_{1}$ S1 | T2 = T0 – $Q\_{1}$ T1 |
| **3** | $R\_{3}$ =  | $Q\_{3}$ =  | $S\_{3}$ =  | $T\_{3}$ =  | R3 = $Q\_{4}$ R4 + R5 | S3 = S1 – $Q\_{2}$ S2 | T3 = T1 – $Q\_{2}$ T2 |
| **4** | $R\_{4}$ = | $Q\_{4}$ =  | $S\_{4}$ =  | $T\_{4}$ =  | R4 = $Q\_{5}$ R5 + R6 | S4 = S2 – $Q\_{3}$ S3 | T4 = T2 – $Q\_{3}$ T3 |
| **5** | $R\_{5}$ =  | $Q\_{5}$ =  | $S\_{5}$ =  | $T\_{5}$ =  | R5 = $Q\_{6}$ R6 + R7 | S5 = S3 – $Q\_{4}$ S4 | T5 = T3 – $Q\_{4}$ T4 |
| **6** | $R\_{6}$ =  | $Q\_{6}$ =  | $S\_{6}$ =  | $T\_{6}$ =  | R6 = $Q\_{7}$ R7 + R8 | S6 = S4 – $Q\_{5}$ S5 | T6 = T4 – $Q\_{5}$ T5 |
| **7** | $R\_{7}$ =  | $Q\_{7}$ =  | $S\_{7}$ =  | $T\_{7}$ =  | R7 = $Q\_{8}$ R8 + R9 | S7 = S5 – $Q\_{6}$ S6 | T7 = T5 – $Q\_{6}$ T6 |
| **8** | $R\_{8}$ =  | $Q\_{8}$ =  | $S\_{8}$ =  | $T\_{8}$ =  | R8 = $Q\_{9}$ R9 + R10 | S8 = S6 – $Q\_{7}$ S7 | T8 = T6 – $Q\_{7}$ T7 |

**Homework for section 8B (due date tbd)**

Fast Exponentiation 2273

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Homework – for section 9A**

Calculate several points on the circular group by using the formula of point addition/doubling.

(without using the table presented in class)

 $y^{2}$ ***≡*** $x^{3}+$ ***2*** $x$ ***+2 mod 17***

Primitive element: **P = (5, 1)**

Point doubling 1: **(9, 1)** + **(9, 1)**

Point doubling 2: **(0, 6)** + **(0, 6)**

Point addition 1: **(10, 11)** + **(16, 13)**

Point addition 2: **(6,14)**+ **(5, 16)**

**Homework – for section 9B**

Based on the circular group G**ℱ**$2^{4}$

$y^{2}+xy$***≡***$x^{3}$***+***$g^{4}x^{2}$***+1 mod P(x)***

Irreducible ***P(***$x$***)*=** $x^{4}$ **+** $x$ **+1**

Generator ***g = (0010)***

Primitive element: P = ($g^{12}$, $g^{12}$)

Verify several points:

Point doubling 1: ($1$, $g^{13}$) + ($1$, $g^{13}$)

Point doubling 2: ($g^{5}$, $g^{3}$) + ($g^{5}$, $g^{3}$)

Point addition 1: ($g^{3}$, $g^{13}$) + ($g^{12}$, $0$)

Point addition 2: ($g^{3}$, $g^{8}$) + ($g^{5}$, $g^{3}$)

**Homework for section 10-A**

(this is the last HW for INF 638 2020)

Find an example of DSA signature, and verification using Elliptic Curves

* The elliptic curve is $y^{2}$≡$x^{3}$+$2x$+2 mod 17
* ***q***=19
* The primitive element is: **A** = ($5$, $1$)
* The private key is **d** = 5
* The hash of the message to sign is: $h\_{(X)}$= 8

 **Method:**

* + Find Public Key **B**
	+ Pick ephemeral key ***KE***
	+ Find ***r***
	+ Compute ***S***
* ***Send (r, s)***
	+ Compute: *w ≡* $s^{-1}$ *mod q*
	+ Compute: $u\_{1}$*≡ w.* $h\_{(X)} $*mod q*
	+ Compute: $u\_{2}$*≡ w. r mod q*
	+ Compute: ***P****=* $u\_{1}$*.****A*** *+* $u\_{2}$***B***🡺 $r$

**Practice for section 10-B**

(no need to submit this as HW)

Find an example of DSA signature, and verification using Elliptic Curves with GF24

* The elliptic curve is $y^{2}+xy$≡$x^{3}$+$g^{4}x^{2}$+1 mod P(x)
* P($x$)= $x^{4}$ + $x$ +1
* The generator is: **g** = (0010) ***q***=16
* The primitive element is: **A** = ($g^{12}$, $g^{12}$)
* The private key is **d** = 5
* The hash of the message to sign is: $h\_{(X)}$= 9

 **Method:**

* + Find Public Key **B**
	+ Pick ephemeral key ***KE***
	+ Find ***r***
	+ Compute ***s***
* ***Send (r,s)***
	+ Compute: *w ≡* $s^{-1}$ *mod q*
	+ Compute: $u\_{1}$*≡ w.* $h\_{(X)} $*mod q*
	+ Compute: $u\_{2}$*≡ w. r mod q*
	+ Compute: ***P****=* $u\_{1}$*.****A*** *+* $u\_{2}$***B***🡺 $r$