Cybersecurity Mathematics

Chapter 2

Using Fermat's theorem and fast powering algorithm Find the inverse of 7 (mod 11) ??

a= 7 , p = 11

$a^{-1} = a^{p-2}$ (mod p)

$7^{-1} = 7^9$ (mod 11)

$= (-4)^9$ (mod 11)

$= ((-4)^3)^3$ (mod 11)

$= (-64)^3$ (mod 11)

$= (-9)^3$ (mod 11)

$= 2^3$ mod 11

$7^{-1} = 8$ mod 11

Discrete logarithm problem (DLP) : $g^x = h \pmod p$

solve $\log_2 9 \bmod 11 = n$

$g^x = h \pmod p$

$g = 2,\ h = 9,\ p = 11$

$2^x = 9 \pmod{11}$

$2^1 = 9 \pmod{11}$ ✗

$2^2 = 9 \pmod{11}$ ✗

$2^3 = 9 \pmod{11}$ ✗

$2^4 = 9 \pmod{11}$ ✗

$2^5 = 9 \pmod{11}$ ✗

$2^6 = 9 \pmod{11}$ ✓

$\boxed{\text{so } x = 6}$

An Overview of the Theory of Groups

Properties of multiplication in F*p :

1- Identity Element:

There is an element 1 ∈ F*p satisfying:

$1 * a = a$ for every a ∈ F*p.

2- Inverse:

Every a ∈ F*p has an inverse

a^{-1} ∈ F*p satisfying:

$a * a^{-1} = 1$

3- Associative :

Multiplication is associative:

$a * (b * c) = (a * b) * c$ for all a, b, c ∈ F*p

4- Commutativity:

Multiplication is commutative:

$a * b = b * a$ for all a, b ∈ F*p .

In addition , we use 0 in place of 1 , and all operations are still true .

1. Identity : $0 + a = a$ for all $a \in F^*p$

2. Every $a \in F^*p$ has a inverse $-a \in F^*p$, with $a+(-a) =0$

3. Addition is associative :

$$a + (b+c) = (a+b) + c$$

for all $a, b, c \in Fp$

4. Addition is commutive:

$a+b = b+a$ for all $a,b \in Fp$

Is (Z , +) a group ??

N : Natural numbers
W : Whole numbers
Z : Set of all integers
C : Complex number
Q : Rational numbers
R : Set of all real numbers

$$G_5 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \ a, b, c, d \in \mathbb{R} \text{ and } 2ad - bc \neq 0 \right\}$$

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Definition: A group consists of a set G and a rule which is denoted by $*$ for combining two element $a, b \in G$, $a*b \in G$. The composition operation $*$ is required to have the following three properties:

1.Identity law: There is an element $e \in G$ such that $a * e = e * a = a$

2.Inverse law: For every $a \in G$ there is a unique $a^{-1} \in G$ $a * a^{-1} = a^{-1} * a = e$

3.Associative law: $a*(b * c) = (a * b)*c$

- If G has finitely many elements, we say that G is a finite group.
The order of G is the number of elements in G, denoted by $|G|$.

- **Definition :** Let G be a group and let $a \in G$ be an element of the group. Suppose there exists a positive integer d with $a^d = e$
The smallest such d is called the order of 2 , If no such d , then a is said to have infinite order.

- **Proposition:** Let G be a finite group. Then every element of G has finite order.
If $a \in G$ has order d and if $a^k = e$ then $d \mid k$

(Lagrange's Theorem) : Let G be a finite group and let $a \in G$ Then the order of a divides order g

Ex : suppose that G is group with an element x of order 9 and an element g of order 5. what is min possible order of G

$$|x| \mid |G| \ , \ |g| \mid |G|$$

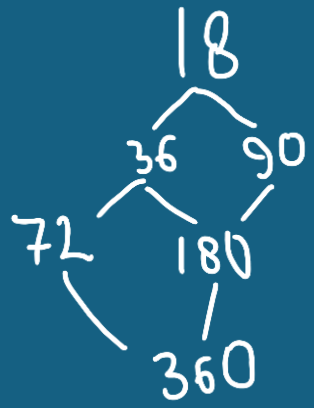
$$9 \mid |G| \ , \ 5 \mid |G|$$

$9 * 5 = 45$

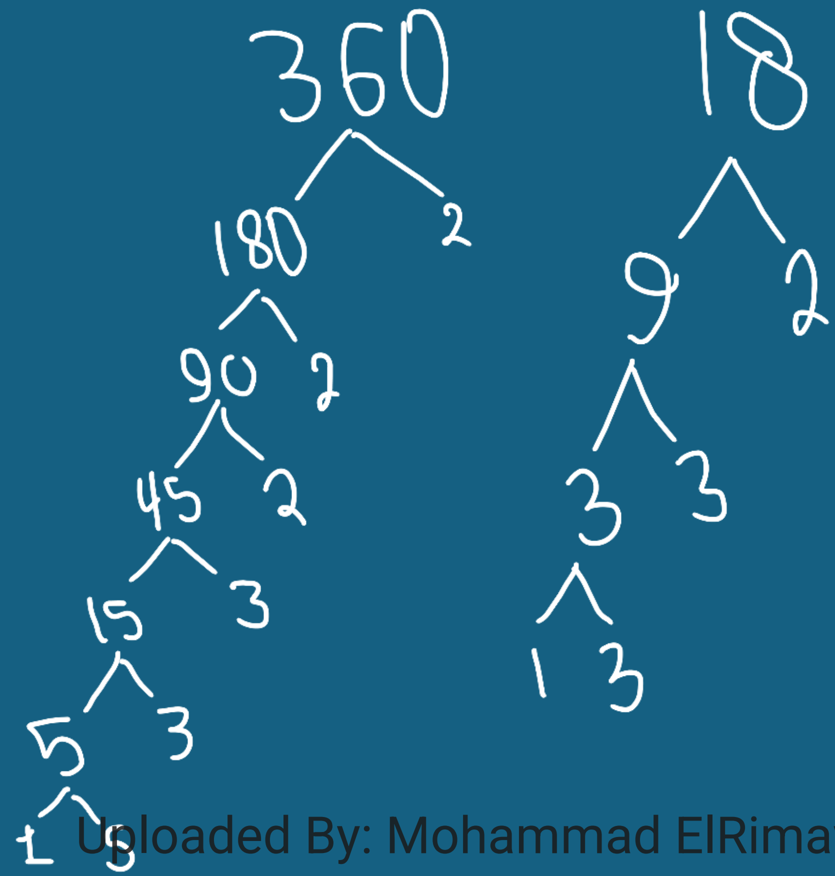
Ex : suppose that G is a group of order 360 with nested subgroup , $k \leq H \leq G$, where $|k| = 18$, What are the possible value of $|H|$??

$|G| = 360 = 2^3 * 3^{\cancel{2}} * 5^1$

$|k| = 18 = 2^1 * 3^{\cancel{2}}$



$2^2 * 5$



Answer : H = { 18 , 36 ,72 , 90 , 180 , 360 }

Collision Algorithm for DLP :

Proposition : let G be a group and let $g \in G$ be an element of order N . Recall that means $g^N = e$ and that no smaller positive power of g is equal to identity element e . Then the DIP $g^x = h$

Shanks baby step :

Let G be a group and $g \in G$ be an element of order $N \geq 2$
The following algorithm .solve the DIP in O(N log(N))

Using Shanks baby step gaint step algorithm

$g^x = h \bmod p$

Find value of x for $6^x = 2 \bmod 41$

$N = \text{Ord}_p\, g = \text{Ord}_{41}\, 6 = \cancel{\phi}\,(N-1) = 40$

$n = 1 + \lfloor \sqrt{N} \rfloor = 1 + \lfloor \sqrt{40} \rfloor = 1 + 6 = 7$

List 1 = $\{1, g, g^2, g^3, \ldots\ldots\ldots, g^n\} \rightarrow g^i \bmod p$

$\{1, 6, 36, 11, 25, 27, 39, 29\}$

5

List 2 = $\{hu^0, hu, hu^2, \ldots\ldots\ldots, hu^n\}$ $u = g^{-n} = 6^{-7} = 17 \bmod 41$

3

$\{2, 34, 4, 27, 8, 13, 16, 26\}$

X = (list 1 power) + n * (list 2 power) = $(5+7*3) \bmod 41 = \underline{26}$, $6^{26} = 2 \bmod 41$

Chinese remainder theorem :

let m1, m2 , ..., mk be a collection pair twice relatively prime integer this mean that gcd (mi ,mj) =1 for all i = J

Let a1,a2 , ..., ak be arbitrary integers .Then the system of congruent
X= a1 (mod m1) , x = a2 (mod m2)
X= ak (mod mk) has solution x=c

Further , if x=c and x =c' are both solution then
c = c' (mod m1, m2 , ..., mk)

Ex : x = 2 (mod 3) , x = 3 (mod 7) , x = 4 (mod 16)

The C.R says : There is u unique solution Modula 336 (3 * 16 * 17)

a = b (mod p)
a = by + p

by C.R

Solve The following equations using C.R

X = 2 (mod 3)
X = 3 (mod 5)
X = 2 (mod 7)

$M = m1 * m2 * m3 = 3 * 5 * 7 = 105$

$a1 = 2, \quad a2 = 3, \quad a3 = 2$

$M1 = M / m1 = 105 / 3 = 35$ ⟶ $M1 * M1^{-1} = 1 \ (\text{mod } 3)$

$35 * M1^{-1} = 1 \ (\text{mod } 3)$

$M1^{-1} = 2$

$M2 = M / m2 = 105 / 5 = 21$ ⟶ $M2 * M2^{-1} = 1 \ (\text{mod } 5)$

$21 * M2^{-1} = 1 \ (\text{mod } 5)$

$M2^{-1} = 1$

$M3 = M / m3 = 105 / 7 = 15$ ⟶ $M3 * M3^{-1} = 1 \ (\text{mod } 7)$

$15 * M3^{-1} = 1 \ (\text{mod } 7)$

$M3^{-1} = 1$

$X = (\ (a1 * M1 * M1^{-1}) + (a2 * M2 * M2^{-1}) + (a3 * M3 * M3^{-1}) \ ) \ (\text{mod } M)$

$X = (\ (2 * 35 * 2) + (3 * 21 * 1) + (2 * 15 * 1) \ ) \ (\text{mod } 105)$

$X = 23$

Q : Solve The following equations using C.R

$X = 5 \ (\text{mod } 3)$

$X = 2 \ (\text{mod } 5)$

$X = 1 \ (\text{mod } 11)$

Using CRT solve $X^2 = 21 \bmod 70$ → $7 * 5 * 2$

$X^2 = 21 \bmod 2$, $X^2 = 21 \bmod 5$, $X^2 = 21 \bmod 7$

$X^2 = 1 \bmod 2$, $X^2 = 1 \bmod 5$, $X^2 = \text{zero} \bmod 7$

$X = 2k + 1$ $\quad$ $X = 5k + 1$ $\quad$ $X = \text{zero}$

$X = 2k + (2-1)$ $\quad$ $X = 5k + (5-1)$

$X = 2k + 1$ $\quad$ $X = 5k + 4$

$a1 = 1$ $\quad$ $M1 = M/m1 = 70/2 = 35$ $\quad$ $M1 * M1^{-1} = 1 \ (\bmod 2)$, $M1^{-1} = 1$

$a2 = 4$ $\quad$ $M2 = M/m2 = 70 / 5 = 14$ $\quad$ $M2 * M2^{-1} = 1 \ (\bmod 5)$, $M1^{-1} = 4$

$a3 = 0$ $\quad$ $M3 = M/m3 = 70 / 7 = 10$ $\quad$ $M3 * M3^{-1} = 1 \ (\bmod 7)$, $M1^{-1} = 5$

$$X = (1*35*1 + 4*14*4 + 0) = 49$$

Or

$$4*14*1 = 21$$

$$X = 49 \text{ or } X = -49$$

$$X = 21 \text{ or } X = -21$$

Pohlig – hellman Algorithm :

Compute Discreet logarithms problem (DLP)

Works when : (p-1) has only small factors

The goal find x :

$a^x = b \quad 0 < x < p-1$

$g^x = h$

Note: $n^{\phi p} \bmod p = 1$

Solve $3^x = 22 \pmod{31}$

Find $0(p) = 31 - 1 = 30$

$30 = 5*6 \longrightarrow$ P1= 5 , P2 =6

Assume $x = a0 + P1 * a1$

$3^{(a0 + P1*a1)} = 22 \bmod 31$

$3^{(a0 + 5*a1)*6} = 22^6 \bmod 31$

$3^{6a0} * \overset{1}{\cancel{3^{30a1}}} = 22^6 \bmod 31$

$(3^6)^{a0} = 22^6 \bmod 31$

$(729)^{a0} \bmod 31 = 8 \bmod 31$

$16^{a0} \bmod 31 = 8 \bmod 31 \longrightarrow a_0 = 2 \ , \ X \equiv a_0 \bmod P_1$

$X = 2 \bmod 5$

Assume $x = b0 + P2 * b1$

$3^{(b0 + 6*b1)*5} = 22^5 \bmod 31$

$3^{5b0} * 3^{\overset{1}{\cancel{30}}b1} = 22^5 \bmod 31$

$(3^5)^{b0} = 22^5 \bmod 31$

$(243)^{b0} \bmod 31 = 6 \bmod 31$

$243^{b0} = 6 \bmod 31 \longrightarrow b_0 = 5 \ , X \equiv b_0 \bmod P_2 \ , X \equiv 5 \bmod 6$

$X \equiv 2 \bmod 5$

$x \equiv 5 \bmod 6$

Solve it using CRT

.....

.....

The final answer $x = 17$

Ring

Examples :

Z = { integers }

R = { real numbers }

R^{2x3} { $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$ }

Q [x] = { complex numbers}

1) Identity law

2) Inverse law

3) Associative law

4) Commutative law

Arithmetic operations

	+	-	*	÷
Z	✓	✓	✓	✗
R	✓	✓	✓	✓
R^{2x3}	✓	✓	✗	✗
Q[x]	✓	✓	✓	✗

(+) Addition

(-) Additive inverse

(*) multiplication

(/) multiplicative inverse

+ / -	Closed	Additive Inverse	Commutative	Identity &Associativity
Z	✓	✓	✓	✓
R^{2x2}	✓	✓	✓	✓
R^{2x3}	✓	✓	✓	✓
Q[x]	✓	✓	✓	✓
Z/ 5Z	✓	✓	✓	✓
Z /6Z	✓	✓	✓	✓

	Closed Under *	Multiplication Inverse	Identity &Associativity
Z	✓	✗	✓
R^{2x2}	✓	✗	✓
R^{2x3}	✗	✗	✗
Q[x]	✓	✗	✓
Z/ 5Z	✓	✓	✓
Z /6Z	✓	✗	✓

In this example, the word **closed** means the set is closed under multiplication if we multiplying any two elements in the set then the result of multiplication belong to the set

Multiplicative inverse : this property checks if each non-zero element in the set has multiplicative inverse within the set

Identity and associativity : this checks if there exist and identity element for multiplication and if multiplication is associative

Z , R , R^{2x3} , $Q[x]$: are commutative group

Z , R , $Q[x]$: have multiplication

R has multiplication inverse

Ring : is a set R with two operations + , * , Both operation are closed

If $x , y \in R$, then $x + y \in R$ and $x * y \in R$

Addition

Group Axioms

1) $X \in R \rightarrow -X \in R$ (inverse)
2) $X + 0, 0 + y = y$ (identity)
3) $x + (y + z) \rightarrow (x + y) + z$ (associative)
4) $x, y \in R \rightarrow x + y \in R$ (closed)

Multiplication

1) a^{-1} exists ?? (Not required)
2) $a * b = b * a$ (not required)
3) $x * (y * z) \rightarrow (x * y) * z$ (associative)
4) 1 in R (most required)

Distributive properties : $a*(b + c) = (a * b) + (b*c)$

Note : (+ , -) group

(+ , - , *) Ring

(+ , - , * , /) field

Congruences classes

$[\,x\,] = \{\, a \in Z \mid a \equiv x \pmod{n} \,\}$

Exp : Find the congruence classes corresponding to mod 4

$[\,0\,]_4 = \{\, \ldots\ldots , -8 , -4 , 0 , 4 , 8 , 12 , \ldots\ldots \,\}$

$[\,1\,]4 = \{\, \ldots\ldots , -7 , -3 , 1 , 5 , 9 , 13 , \ldots\ldots \,\}$

$[\,2\,]4 = \{\, \ldots\ldots , -6 , -2 , 2 , 6 , 10 , 14 , \ldots\ldots \,\}$

$[\,3\,]4 = \{\, \ldots\ldots , -5 , -1 , 3 , 7 , 11 , 15 , \ldots\ldots \,\}$

Polynomial Rings and EA :

If R is any ring, then we can create a polynomial ring with coefficients taken from R

$R[x] = \{ a0 + a1x + a2x + \dots\dots + an\, x^n \}$ $n \geq 0$

and $a0, a1, \dots\dots, an \in R$

Ex :

$$f(x) = x^5 + 2x^4 \quad , \quad g(x) = x^3 - 5$$

$$\require{cancel} \begin{array}{r|l} & x^2 + 2x \\ \hline x^3 - 5 & \cancel{x^5} + 2x^4 \\ & -\ \cancel{x^5} \qquad\qquad -5x^2 \\ \hline & \cancel{2x^4} + 5x^2 \\ & -\ \cancel{2x^4} \qquad\qquad -10x \\ \hline & 5x^2 + 10x \end{array}$$

G(x)

Q(x)

R(x)

Find Q(x) , R(x) ?

F(x)

$$\overset{F(x)}{a} = \overset{}{q} * b + r$$

a = q * b + r

Q(x)   G(x)   R(x)

F(x)

$$x^5 + 2x^4 = \underbrace{(x^2+2x)}_{Q(x)}\underbrace{(x^3-5)}_{G(x)} + \underbrace{5(x^2+2x)}_{R(x)}$$

Let $f(x) = x^3 + x^2 - x - 1$, $g(x) = x^2 + 3x + 2$ be polynomial in Q [x]

a) Use the E.A for Q [x] to compute the gcd(f,g)

b) Use the fundamental theorem of arithmetic for Q [x] to compute gcd(f , g)

a)

$$
\begin{array}{r|l}
 & x - 2 \\
\hline
x^2+3x+2 & \cancel{x^3} + x^2 - x - 1 \\
 & -(\cancel{x^3} + 3x^2 + 2x) \\
\hline
 & -2x^2 - 3x - 1 \\
 & -(-2x^2 - 6x - 4) \\
\hline
 & 3x + 3
\end{array}
$$

$$
\begin{array}{r|l}
 & 1/3\,x + 2/3 \\
\hline
3x+3 & x^2 + 3x + 2 \\
 & -(x^2 + x) \\
\hline
 & 2x + 2 \\
 & -(2x + 2) \\
\hline
 & 0
\end{array}
$$

gcd = 3x+3 or 3(x+1)

gcd = x+1

Find gcd (a(x) , b(x)) using EA , In Galois field (2) . (F2)

$a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$b(x) = x^4 + x^2 + x + 1$

$$
\begin{array}{r|l}
 & x^2 + x \\
\hline
x^4 + x^2 + x + 1 & \cancel{x^6} + x^5 + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + x + 1 \\
 & - \cancel{x^6} + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} \\
\hline
 & \cancel{x^5} + \cancel{x} + 1 \\
 & - \cancel{x^5} + x^3 + x^2 + \cancel{x} \\
\hline
 & -x^3 - x^2 + 1 \\
 & (+2)\downarrow \quad x^3 + x^2 + 1
\end{array}
$$

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
x^3 + x^2 + 1 & \cancel{x^4} + x^2 + \cancel{x} + 1 \\
 & - \cancel{x^4} + x^3 + \cancel{x} \\
\hline
 & -x^3 + x^2 + 1 \\
 & (+2)\downarrow \quad x^3 + x^2 + 1 \\
 & - x^3 + x^2 + 1 \\
\hline
 & 0
\end{array}
$$

$$\boxed{gcd = x^3 + x^2 + 1}$$

Given $f(x) = x^6 + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5$

$g(x) = x^4 - x^2 - 2x - 1$

In Q

Using EEA find $u(x)$ and $v(x)$

$x^2 + 2x + 3$

$x^4 - x^2 - 2x - 1 \;\big)\; \cancel{x^6} + 2x^5 + 2x^4 - 3x^3 - 9x^2 - 9x - 5$

$- \;\cancel{x^6} \quad - x^4 \quad - 2x^3 - x^2$

$\cancel{2x^5} + 3x^4 - x^3 - 8x^2 - 9x - 5$

$- \;\cancel{2x^5} \quad - 2x^3 - 4x^2 - 2x$

$\cancel{3x^4} + x^3 - 4x^2 - 7x - 5$

$- \;\cancel{3x^4} \quad - 3x^2 - 6x - 3$

$x^3 - x^2 - x - 2$

$x + 1$

$x^3 - x^2 - x - 2 \;\big)\; \cancel{x^4} - \cancel{x^2} - \cancel{2x} - 1$

$- \;\cancel{x^4} - x^3 \; \cancel{-x^2} \; \cancel{-2x}$

$\cancel{x^3} \quad -1$

$- \;\cancel{x^3} - x^2 - x - 2$

$x^2 + x + 1$

$x - 2$

$x^2 + x + 1 \;\big)\; \cancel{x^3} - x^2 - x - 2$

$- \;\cancel{x^3} + x^2 + x$

$-2x^2 - 2x - 2$

$-2x^2 - 2x - 2$

0

$Gcd(f(x), g(x)) = x^2 + x + 1$

From step 2 : $r2 = g(x) - (q2 * r1)$

From step 1 : $r1 = f(x) - (q1 * g(x))$

$r2 = g(x) - (q2 * (f(x) - (q1 * g(x))))$

$= g(x) - (q2 * f(x) - q2 * q1 * g(x))$

$= g(x) - q2 * f(x) + q2 * q1 * g(x)$

$= -q2 * f(x) + (g(x) + q2 * q1 * g(x)$

$u(x) = -q2 = -(x + 1) = -x - 1$

$v(x) = 1 + q2 * q1 = x^3 + 3x^2 + 5x + 9$