Cybersecurity Mathematics

Chapter 1

Section 1 : Simple substitution ciphers :

Caser receive Encrypted message :

prkdphg vwxbh fbehv vhfxulwb (3 letters shift)

D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Original message: mohamed study cyber security

Section 2 : Greatest common divisor (GCD) :

Algebra , number theory (int numbers) Z

Add (a+b) , subtract (a-b) , multiple (a*b)

Commutative law

Associative law

Distributive law

Def : let a and b be integers , b not equal zero

We say b divides a , or a is divisible by b

If there is an integer c such that a = b*c

$b \mid a$: b divides a for example $7 \mid 21$	
$b \nmid a$: b is not dividing a for example $5 \mid 31$	

Remarks :

1 - All integers are divisible by 1

2 - All integers are divisible by 2 are even

3- All integers are not divisible by 2 are odd

Propositions :

1 - If $a|b$ and $b|c$, then $a|c$

2 - If $a|b$ and $b|a$, then $a = \pm b$

3- If $a|b$ and $a|c$ then $a|(b+c)$, $a|(b-c)$

<u>Def :</u> a common divisor of two integers a and b is positive integer d that divides both

<u>Def :</u>The GCD of <u>a</u> and <u>b</u> is the greatest positive integer <u>d</u>
$d|a$, $d|b$ for example

18: 1,2,3,6,9,18 the GCD =6

12 : 1,2,3,4,6,12

What is the GCD of (748 , 2024):

a= b *q +r

Solution :

2024= 748 * 2 + 528   a=2024 , b = 748

748 = 528 * 1 + 220   a=748 , b=528

528 = 220 * 2 + 88   a=528 , b=220

220 = 88 * 2 + 44   a= 220 , b =88

88 = 44 * 2 + 0 **(when r = 0 STOP , GCD =b)**

<u>GCD = 44</u>

Def : let a and b be positive integers then we say that $a|b$ has quotient q and reminder r if $a= b*q+r$ where $0 \leq r < b$

Suppose we need to get GCD (a,b) then at first divides a by b to get $a= b*q+r \quad 0\leq r<b$

If d is any common divisor of a and b then it is clear form equation that d is also the divisor of r .

What is the GCD of (72 , 120) ?

What is the GCD of (81, 144) ?

What is the GCD of (105 , 252) ?

What is the GCD of (56 , 98) ?

Theorem : (The Euclidean algorithm):

Let A and B be positive integers with a greater than or equal B the following algorithm computes gcd (a,b) in finite number of steps :

1- let r0 =a , r1=b

2- set i =1

3 - divide r i-1 by ri to get q

$$au + bv = \gcd(a,b)$$

$$a = b*2 + 528$$

$$a - 2b = 528$$

$$b = (a-2b) * 1 + 220$$

$$3b - a = 220$$

$$a - 2b = 2(3b-a) + 88$$

$$3a - 8b = 88$$

$$3b - a = (3a - 8b) * 2 + 44$$

$$19b - 7a = 44$$

$$19(748) - 7(2024) = 44$$

$$u = -7, \ v = 19$$

<u>GCD(748 , 2024)</u>

$$2024 = 748 * 2 + 528$$

$$748 = 528 * 1 + 220$$

$$528 = 220 * 2 + 88$$

$$220 = 88 * 2 + 44$$

$$88 = 44 * 2 + 0$$

<u>GCD = 44</u>

Set up box :

		q1	q2	q3	q4
0	**1**	**p1**	**p2**	**p3**	**p4**
1	0	Q1	Q2	Q3	Q4

In first two columns write 0 & 1 and 1 & 0, then starting from column 3 use formulas :

p1 = q1 , p2 = q2 * p1+1 , p3 = q3 *p2 +p1 , p4= q4 *p3 +p2

Q1= q1 *0 +1 , Q2 = q2 * Q1+0 , Q3 =q3 *Q2 + Q1 , Q4 = q4 *Q3+ Q2

$\frac{a}{gcd}$

u = Q3 * (-1)^t v = p3 * (-1)^t+1 t : is the number of quotients C1*u + C2*v =1

$\frac{b}{gcd}$

A= 73 , b =25

73= 25* 2 +23

25 = 23 * 1 +2

23 = 2 * 11 +1

2= 1 * 2 +0

GCD = 1

t=4

We will use these numbers in set up table

a= b*2 +23

a -2b = 23

B = (a-2b) * 1 +2

-a +3b =2

a-2b = (-a +3b) * 11 +1

12a -35b =1

12(73) – 35(25) = 1

u =12   v= -35

Set up box :

-V

u

a

b

		2	1	11	2
0	1	2	3	35	73
1	0	1	1	12	25

2*1+0 =2 , 1 *2 +1 =3 , 11 *3 +2 =35 , 2*35 +3 =73

2 *0 +1 =1 , 1 *1 +0 =1 , 11*1 + 1 =12 , 2*12 +1 =25

C1 = 73 C2 =25 <u>73 * (12) + 25 * (-35) = 1</u>

a = 291 , b=252

1 – find the gcd (291,252) using Ecalcidene algorithm ??

291 = 252 *1+39

252 = 39 *6 + 18

39 = 18 *2 +3

18 = 3*6 +0

Gcd = 3

2- use extended Euclidean algorithm to find u &v ??

a =b*1 +39

a-b = 39

b= (a-b) *6+18

7b – 6a= 18

a-b = (7b-6a)*2 + 3 a-b = 14b-12a +3 13a- 15b =3 u= 13 , v= -15

3- find u and v using set up box :

		1	6	2	6
0	**1**	**1**	**7**	**15**	**97**
1	0	1	6	13	84

$t = 4$

$u = 13*(-1)^4 = 13$

$v = 15*(-1)^{4+1} = -15$

$c1 = 97 \quad c2 = 84$

$97 * (13) + 84(-15) = 1$

- Clock Arithmetic

Def : let $m \geq 1$ be an integers we say that the integers a & b are congruent module m if their difference (a-b) is divisible by m we write $a = b \pmod m$

To indicate a & b are congruent module m . The number m is called the modulus

$m=12$

$$\overbrace{6 + 9}^{a} = \overset{b}{3} \longrightarrow 15 - 3 = 12 \longrightarrow 15 = 3 \pmod{12}$$

Propositions :

- let $m \geq 1$, b be an integers numbers

1- if $a1 = a2 \pmod{m}$ & $b1 = b2 \pmod{m}$

Then $a1 \pm b1 = a2 \pm b2 \pmod{m}$

- Let a be an integers , then $a*b = 1 \pmod{m}$ for some

integers b if and only if $\gcd(a, m) = 1$

further , if $a1*b1 = a2*b2 = 1 \pmod{m}$

Then $b1 = b2 \pmod{m}$ we call b the inverse of Modula m

Q1 . m=5 , a=2 and GCD(2,5) =1 , find the inverse :

$2*b= 1 \pmod 5$

$2b-1= 5$

b =3 $\quad$ **$2^{-1} = 3 \pmod 5$**

Q2 . Find the inverse of 3 modulo 11:

a= 3 , m=11

$3 * b = 1 \pmod{11}$

$3 * 4 \bmod 11 = 1$, so **b =4** $\quad$ **$3^{-1} = 4 \pmod{11}$**

Q3. Compute 5/7 (mod 11)

$5 * 7^{-1} = 1 \pmod{11}$

$7 * b = 1 \pmod{11}$

We to try b= 1,2,..... Until (7*b mod 11 =1

b =8

$7 * 8 = 1 \pmod{11}$, (7*8 mod 11 = 1

$7^{-1} = 8$

$5 * 8 = 40$, $40 = 7 \pmod{11}$

-Def : $Z / mZ = \{ 0,1,2,......,m-1\}$

Call Z / mZ the ring of integers Modula m (add or multiple)

Then divide b m to be in the range

Ex : $Z / 5 Z$ (Addition , multiplication)

+	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

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

a has inverse of Modula m if and only if $\gcd(a,m) = 1$

- numbers that have inverse are called **units**

- We denote the set of all units by $(Z / mZ)^*$

$(Z / mZ)^* = \{ a$ belong to $Z / mZ : \gcd(a,m) = 1\}$

a has an inverse modula m

The set $(Z / mZ)^*$ is called **the group of units modula m**

Ex : the group units of modula 24

$(Z / 24Z)^* = \{1,5,7,11,13,17,19,23\}$

$(\mathbb{Z}/7\mathbb{Z})^* = \{1,2,3,4,5,6\}$

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Note : The multiplication tables for $(Z / 7Z)^*$ and $(Z/ 24Z)^*$ are units but addition table doesn't produce a unite

Multiple inverse using EEA :

Ex : a= 2 , b= 5

A>B , always a must be greater than b

So, a =5 , b =2

T = T1 – T2* Q

Q	A	B	R	T1	T2	T
2	5	2	1	0	1	-2
2	2	1	0	1	-2	6
X	1	0	X	-2	6	X

M.I (2 mod 5)

Euler Phi function:

Def : $\emptyset$ (m) = number of $(Z / mZ)^*$ = { 0 < a <m : gcd(a,m) = 1}

Ex : $\emptyset$ (24) = ?? $\longrightarrow$ 8

1 2 3 4 5 6 7 8

$(Z / 24Z)^*$ = { 1, 5 ,7,11,13,17, 19, 23}

Euler Tolient function:

- if m is a prime $\longrightarrow$ $\emptyset(m) = m-1$
- if m is multiplication of two prime numbers $\longrightarrow$ $\emptyset(m) = (p-1)(q-1)$

- if m = a*b both or either a and b are composite

$$\emptyset(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$$

Ex: Find O (45)

Sol : m= 45 , 45= 9*5 , 9= 3^2 45(1 – 1/3) (1 – 1/5)= 24

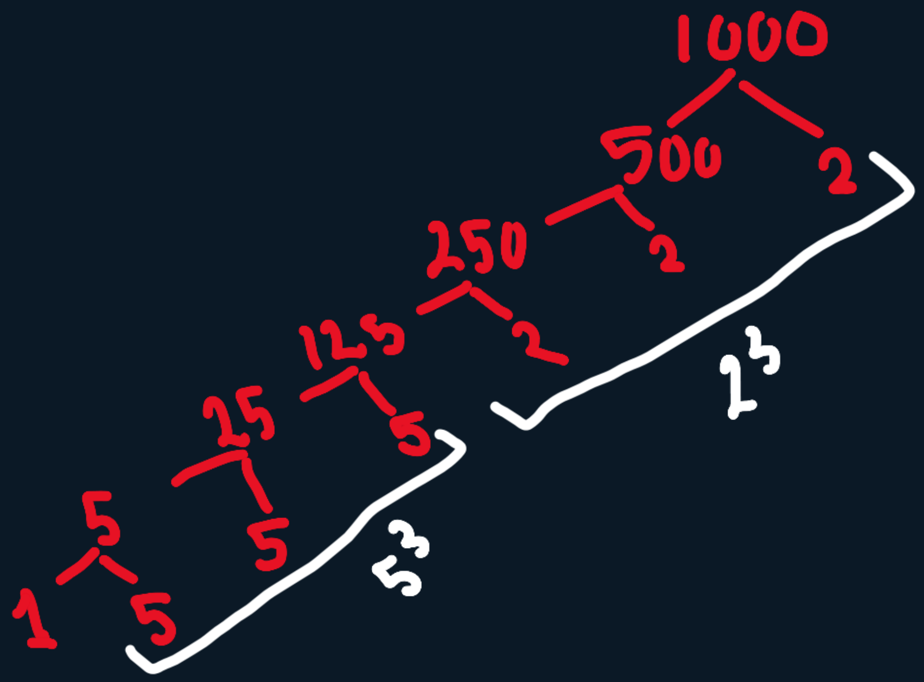
Ex : O (35)

Sol : m=35 , 35 = 7*5 , 7 & 5 are prime numbers so we will use this formula (q-1) * (p-1) , (7-1)(5-1) = 24

Ex : O (1000)

$1000(1 - 1/2)(1 - 1/5)$

$= 400$



fast powering algorithm

Ex : $23^3 \pmod{30}$

$23^3 \bmod 30 = -7^3 \bmod 30$

$49 * -7 \bmod 30 = -343 \bmod 30 = -13$

To find positive number add m $-13 + 30 = 17$

Ex : Find 31^{500} (mod 30)

$31^{500} \bmod 30 = 1^{500} \bmod 30 = 1$

Ex : Find $(242)^{329}$ mod (243)

$242^{329} \bmod 243 = -1^{329} \bmod 243 = -1$

$= -1 + 243 = 242$

Ex : Find 3^{218} (mod 1000)

Sol : use FPA

$218 = 128 + 64 + 16 + 8 + 2$

$(3^{128} * 3^{64} * 3^{16} * 3^{8} * 3^{2})$ mod(1000)

Solve 88^7 (mod 187) **big difference**

88 (mod 187) = 88

88^2 (mod 187) = 88 * 88 (mod 187) =77

88^4(mod 187) = 77 * 77 = 132

887(mod 187) = 88^4 * 88^2 * 88 (mod 187)

= 132 * 77 * 88 (mod 187) = 11

<u>Ex : Find the last two digits of 29^5</u>

$29^5 \pmod{100}$

$29^1 \pmod{100} = 29$

$29^2 \pmod{100} = 41$

$29^4 \pmod{100} = 41*41 \pmod{100} = 81$ or -19

$29^5 \pmod{100} = 29^4 * 29 \pmod{100} = -19 * 29 \pmod{100}$

$= -551 \pmod{100} = -51$, $-51+100 = 49$

Ex : $3^{100} \pmod{29}$

$3^1 \pmod{29} \equiv 3$, or 26

$3^2 \pmod{29} \equiv 9 \pmod{29} \equiv 9$

$3^4 \pmod{29} \equiv 3^2 \times 3^2 \pmod{29} \equiv 9 \times 9 \pmod{29} \equiv 23$ or -6

$3^8 \pmod{29} \equiv 3^4 \times 3^4 \pmod{29} \equiv 7$

$3^{16} \pmod{29} \equiv 3^8 \times 3^8 \pmod{29} \equiv 7 \times 7 \pmod{29} \equiv$

$49 \pmod{29} \equiv 20$

$3^{32} \pmod{29} \equiv 3^{16} \times 3^{16} \pmod{29} \equiv -9 \times -9 \pmod{29} \equiv 81 \bmod 29 \equiv 23$ or -

6 $3^{64} \equiv 3^{32} \times 3^{32} \pmod{29} \equiv 23 \times 23 \pmod{29} \equiv 36 \pmod{29} \equiv 7$

$3^{100} \equiv 3^{64} \times 3^{32} \times 3^4 \pmod{29} \equiv 7 \times \underbrace{-6 \times -6}_{36 \bmod 29 = 7} \pmod{29} \equiv 49 \pmod{29} \equiv 20$

Ex : 23^{16} (mod 30)

$\Rightarrow 23 \ (\text{mod } 30) = 23$ or -7

$\Rightarrow ((((-7)^2)^2)^2)^2 \text{ mod } 30$

$\Rightarrow (((49)^2)^2)^2 \text{ mod } 30 \Rightarrow 19$ or -11

$\Rightarrow (((-11)^2)^2)^2 \text{ mod } 30 \Rightarrow (121)^2 \text{ mod } 30 = 1$

Prime numbers unique factorization and finite fields

def : an integer p is called a prime if $p \geq 2$ and if only positive integers dividing p are 1 and p

Proposition : let p is prime number and suppose that p divides the product of integers a and b (a*b) more generally if p divide a product of integers say

$P \mid a1, a2 \ldots\ldots an$

then P divides at least one at the individual ai

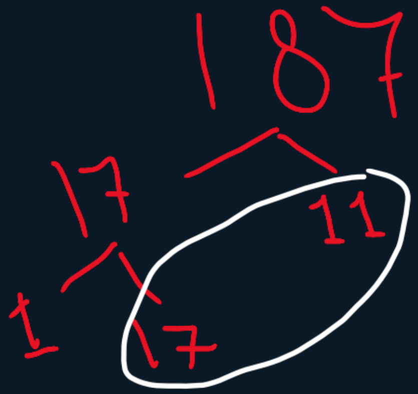
Theorem : the fundamental theorem of arithmetic
let a greater than or equal 2 be an integer , then a can be factered as product of prime numbers

$a = P_1^{e1} * P_2^{e2} * P_3^{e3} \ldots\ldots P_r^{er}$

Ex : 125

$5^3 = 125$

Ex : 187



$11 * 17 = 187$

Ex : 187

First, we use this formula $n = p^2 - q^2$ to find the value of p & q

$$187 = p^2 - q^2$$
$$p^2 = 187 + q^2$$
$$p = \sqrt{187 + q^2}$$
$$p = \sqrt{187 + 3^2}$$

p= 14 , q= 3

After we find p & q ,use this formula $n = (p - q)(p + q)$ to the get the numbers whose product is 187.

$$n = (14-3)\ (14+3) = 17 * 11$$

Ex : Factorize 3233

$P = \sqrt{3233 + (1)^2} \Rightarrow$ False

$P = \sqrt{3233 + (2)^2} \Rightarrow$ False

$P = \sqrt{3233 + (3)^2} \Rightarrow$ False

$P = \sqrt{3233 + (4)^2} \Rightarrow$ True $\Rightarrow 57$

$n = (57 - 4)(57 + 4) = (61)(53)$

Def : The fundamental theorem of arithmetic says that in factoring a positive integer a into primes, each prime p appears to a particular power. We denote this power by Ord$p(a)$ and call it the order (or exponent) of p in a . For convenience, we define Ord$p$(1)=0 for all prime numbers

Ex : $1728 = 2^6 * 3^3$

$\text{Ord}_2\,(1728) = 6$

$\text{Ord}_3\,(1728) = 3$

$a = \prod_{p \text{ (primes)}}^{n} {}^{\text{ord}_p(a)}$

$\text{ord}_p : \{1, 2, 3, \ldots\ldots\}$

If p is prime , then every nonzero number Modula p has multiplicative inverse (M.I) Modula P

Proposition : let p be a prime then every non-zero element in Z/pZ has MI that is number B satisfying

$a*b = 1 \pmod p$

$b = a^{-1} \pmod p$

Remark : The EA give us an effient computation method for computing
a^{-1} mod p , we simply solve the equation
$au + pv = 1$ and $u = a^{-1}$ mod p , if p is prime then the
$(Z/pZ)^* = \{1,2,3,......,p\}$

In otherwards , when remove zero element from Z/pZ , the remaining elements are units and closed under multiplication .

Powers and Prime have roots in finite fields

finite fields a several name for a (commutative)ring in which every non-zero element has MI

Ex :

R : real numbers

Q : fraction

C : complex

Z/pZ : for Ex (Z/5Z) : F5 ⟶ { 0,1,2,3,4}

(Z/24Z)* : F24 * ⟶ {1,3,5,.....}

Ex : $p = 7$

$1^1 \bmod 7 = 1$, $1^2 \bmod 7 = 1$ ………… $1^6 \bmod 7 = 1$
$2^1 \bmod 7 = 2$, $2^2 \bmod 7 = 4$ ……… $2^6 \bmod 7 = 1$
$3^1 \bmod 7 = 3$, $3^2 \bmod 7 = 2$ ………. $3^6 \bmod 7 = 1$
$4^1 \bmod 7 = 4$, $3^2 \bmod 7 = 2$ ………. $4^6 \bmod 7 = 1$
$5^1 \bmod 7 = 5$, $5^2 \bmod 7 = 4$ ………. $5^6 \bmod 7 = 1$
$6 \bmod 7 = 3$, $6^2 \bmod 7 = 2$ ………. $6^6 \bmod 7 = 1$

$a^6 = 1 \pmod 7$, $a = 1,2,3,4,5,6$
$a^6 = \{ 1 \pmod 7$ if $7 \nmid a \}$, $\{$ zero $\pmod 7$ if $7 \mid a \}$

If p is a prime number and a is a positive integer not divisible by P then $a^{p-1} = 1 \bmod p$

Ex : Does Fermat's theorem hold true for p = 5 and a =2 ??

$\boxed{5 \nmid 2}$ ✓

$2^4 = 1 \bmod 5$

$16 = 1 \pmod 5$

Ex : prove that Fermat's theorem holds true for p =13 , a= 11

$\boxed{13 \nmid 11}$

$a^{p-1} = 1 \bmod p$

$11^{12} = 1 \ (\bmod 13)$

$(-2)^{12} = 1 \ (\bmod 13)$

$(-2)^{4*3} = 1 \ (\bmod 13)$

$((-2)^4)^3 = 1 \ (\bmod 13)$

$(16)^3 = 1 \ (\bmod 13)$

$3^3 = 1 \ (\bmod 13)$

$27 = 1 \ (\bmod 13)$

Remark: Fermat's theorem and fast power algorithm provide us with reasonably efficient method for computing inverse Modula p namely

$a^{-1} = a^{p-2} \pmod{p}$

Ex : find inverse of (7814 modula 17449)

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

$7814^{-1} = 7814^{17447} \pmod{17449}$

$= 1284 \pmod{17449}$

2 - EEA

$au + bv = 1$

$7814u + 17449\,v = 1$

$(u, v) = (1284, -575)$

$\overset{a}{7784}^{-1} = \overset{u}{1284} \bmod \overset{p}{17449}$

Theorem : Primitive root theorem let p be a prime number there exists an element g belong to Fp* Where powers give every element of Fp*

$Fp^* = \{1, g, g^2, g^3 \ldots\ldots, g^{p-2}\}$

Element with this property are called primitive roots of Fp* or generate of Fp* they are the elements of Fp* having order P – 1

Ex : the filed F11 has 2 as primitive root ??

$2^0 \bmod 11 = 1$, $2^1 \bmod 11 = 2$, $2^2 \bmod 11 = 4$,

……….. $2^9 \bmod 11 = 6$

Yes , because there is no similarity in the result

Is 2 a primitive root for F17 ??

$2^0 = 1 \bmod 17 = \boxed{1}$

$2^1 = 2 \bmod 17 = 2$

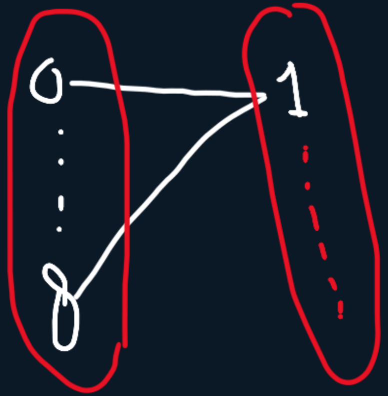
⋮

$2^8 = 256 \bmod 17 = \boxed{1}$

⋮

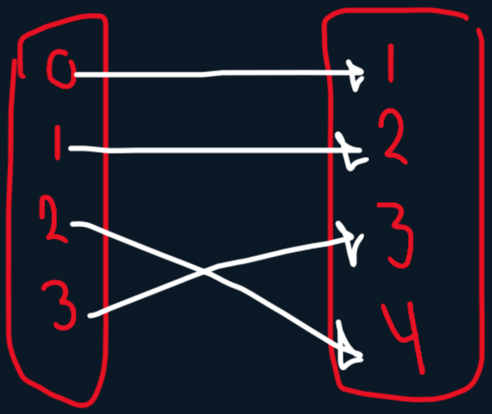
same, so the answer is No

otherwords, It's not 1 to 1 so 2 isn't primitive root



Is 2 a primitive root of prime number 5 ??

$2^0 \bmod 5 = 1$
$2^1 \bmod 5 = 2$
$2^2 \text{ Mod } 5 = 4$
$2^3 \bmod 5 = 3$



Yes , because there is no similarity in the result