Tutorial-2

Date:
Page No:

Q.1.

Ans a cyclic group of order n generator α.

$$\text{order}(\alpha^k) = \frac{n}{\gcd(n,k)}$$

We need to find smallest integer m such that $e = a^{km}$

To prove $m = \frac{n}{\gcd(n,k)}$

$\Rightarrow a^{km} = e$

Since the order of a is n, it follows that $n \mid km$ or equivalently n/d divides $m(k/d)$. Since d is the GCD of n & k, n/d and k/d are relatively prime.

Hence for n/d to divide $m(k/d)$ it must divide m.

So $\frac{n}{\gcd(n,k)} \leq m$ $\quad$ m is smallest +ve integer

$$m = \frac{n}{\gcd(n,k)}.$$ proved

Date:
Page No:

Q.2.

Ans. We know that α is a primitive root modulo p, then the integers powers of α, when reduced modulo p, comprise all the possible remainders modulo except 0. Hence, every integer that is not divisible by p is congruent modulo p to some power of α.

If α is not primitive root, then d decryption key is not unique.

For eg. $p = 5$

1) $4^1 = 4 \bmod 5 = 4$
2) $4^2 = 4^2 \bmod 5 = 1$
3) $4^3 = 4^3 \bmod 5 = 4$
4) $4^4 = 4^4 \bmod 5 = 1$
5) $4^0 = 1 \bmod 5 = 1$

Here 4 is not primitive root modulo p. for a particular β there exist multiple x such that $a^x \equiv \beta \bmod p$.

Date:
Page No:

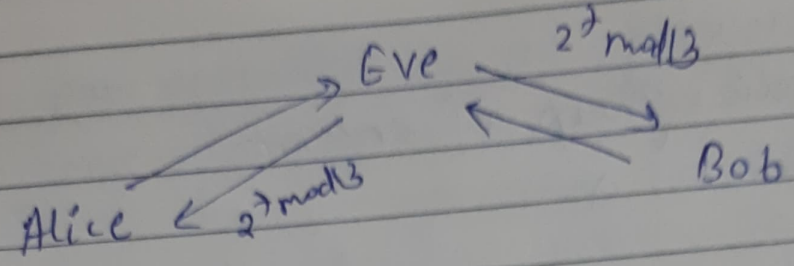
Here (97, 8, 33) is public key.

$8^1 \bmod 97 = 8^{12} \bmod 97 = 8$

Here $g = 8$ is not generator or primitive root.
Hence it is not good for El-gamal public cryptosystem.

Date:
Page No:

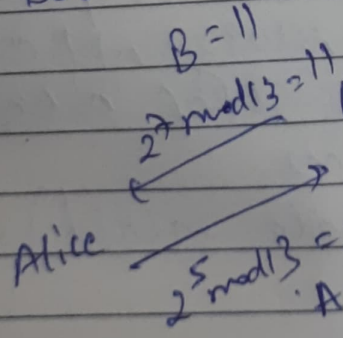
Q.3.



private key of A = 5
private key of B = 4 private key of E = 7
generator g = 2
prime p = 13

Eve uses e = 7 & sends both Alice & Bob $2^7 \bmod 13$ = 11.

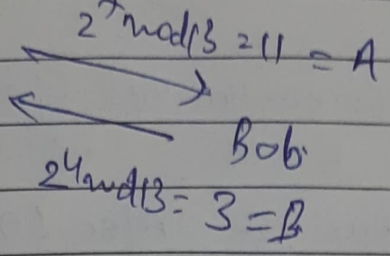
In doing so, Eve imitates Bob when talking with Alice and imitates Alice when talking to Bob.



key generated by Alice = $(B)^a \bmod p$
$= (11)^5 \bmod p = 7$

key generated by Eve for Alice = $(A)^e \bmod p$
$= 6^7 \bmod 13 = 7$

Date:
Page No:



Key generated by Bob = $(A)^b \bmod p = (11)^4 \bmod 13 = 3$

Key generated by Eve for Bob = $B^e \bmod p$

$\Rightarrow 3^4 \bmod 13 = 3$

Eve has calculated two keys for Alice & Bob.

For Alice = 7

for Bob = 3

When alice sends a message to Bob, she will use the key that she actually shares with Eve, allowing eve to see the message.

Date:
Page No:

Q.4.
Ans. G is a non-commutative group of order 10.

Let G be a group of order 10.
As we know from Lagrange's theorem, that order of the subgroup H is the divisor of the order of the Group G.
Therefore order of H possible are 1, 2, 5 or 10.

1, 10 are trivial subgroups here.

Let's assume that there is no subgroup of order 5.
Let, $a \neq e \in G$.
We know that order of element divides order of group. So $O(a) \mid O(G)$.
If every element of G is of order 2, then
$a^2 = e \Rightarrow a * a^{-1} = e$
$a = a^{-1}$ for all $a \in G$
Now G is group is abelian because
$a * a^{-1} = a^{-1} * a$
$a * b = b * a$.
Thus, it creates contradiction to the original part.

Therefore, every element of G is not of order 2
Thus $O(a) = 5$. If $O(a) = 5$, then H is a cyclic subgroup of order 5.

Date:
Page No:

Q.5.
Ans.

$(ab)^3 = a^3b^3$ for all $a, b \in G$

We have

$ababab = a^3b^3$

$abababab = aaabbbbb$

$\Rightarrow baba = aabb$

$\Rightarrow (ba)^2 = a^2b^2$

Now consider

$(ab)^4 = [(ab)^2]^2$

$\Rightarrow (b^2a^2)^2$

$\Rightarrow a^4b^4$

$= aaaabbbb$

also $(ab)^4 = abababab$

$= a(ba)^3b$

Therefore, we get

$aaaabbbb = a(ba)^3b$

$(ba)^3 = (ab)^3$

$(ab)^{-3}(ba)^3 = e$

$e \in G$

$[(ab)^{-1}(ba)]^3 = e$

Date:
Page No:

Now for $x = (ab)^{-1}(ba)$ divides 3 by which $|x|$ can be 3 or 1.

By Lagrange's theorem if $|x| = 3$ then 3 divides $|G|$ which is not true.

Thus.

$$|x| = 1.$$
$$= x = e$$
$$(ab)^{-1}(ba) = e$$

Multiply both sides by ab

$$ba = ab$$

Thus, for $a, b \in G$ Thus, G is abelian

Date:
Page No:

6 (a) x^2+1 is irreducible over Z_7.

We can check the roots over Z_7. we have

$0^2+1=1$ $\quad 1^2+1=2$ $\quad 2^2+1=5$

$3^2+1=3$ $\quad 4^2+1=\overline{3}$ $\quad 5^2+1=5$

$6^2+1=2$

None of them equals to zero.
So ~~Zp~~ irreducible for x^2+1.

(c) x^3-9 is reducible over Z_{11}.

From fermat's theorem

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

$$2^{10} \equiv 1 \bmod 11$$

$$2^{12} \equiv 4 \bmod 11$$

$$= 4^6 \equiv 4 \bmod 11 \qquad 4^3 \equiv \pm 2 \bmod 11$$

So 4^3 is either 2 or 9 modulo 11.

Date:
Page No:

So, a it's a candidate to satisfy the congruence

b) $x^3 - 9$ is irreducible over Z_{31}.

1) $|x^3-9|_{x=0} = 22 \bmod 31$

2) $|x^3-9|_{x=1} = 23 \bmod 31$
3) $|x^3-9|_{x=2} = 30 \bmod 31$
4) $|x^3-9|_{x=3} = 18 \bmod 31$
5) $|x^3-9|_{x=4} = 24 \bmod 31$
6) $x=5 = 23 \bmod 31$
7) $x=6$ $21 \bmod 31$
8) $x=7 = 24 \bmod 31$
9) $x=8 = 7 \bmod 31$
10) $x=9 = 7 \bmod 31$
11) $x=10 = 30 \bmod 31$
12) $x=11 = 20 \bmod 31$
13) $x=12 = 14 \bmod 31$
14) $x=13 = 18 \bmod 31$
15) $x=14 = 7 \bmod 31$
16) $x=15 = 18 \bmod 31$
17) $x=16 = 26 \bmod 31$
18) $x=17 = 6 \bmod 31$
19) $x=18 = 26 \bmod 31$
20) $x=19 = 30 \bmod 31$
21) $x=20 = 24 \bmod 31$
22) $x=21 = 14 \bmod 31$
23) $x=22 = 6 \bmod 31$
24) $x=23 = 6 \bmod 31$
25) $x=24 = 20 \bmod 31$
26) $x=25 = 23 \bmod 31$
27) $x=26 = 21 \bmod 31$
28) $x=27 = 20 \bmod 31$
29) $x=28 = 26 \bmod 31$
30) $x=29 = 14 \bmod 31$
31) $x=30 = 21 \bmod 31$

So $x^3 - 9 \neq 0 \ \forall \ x \in Z_{31}$

So $x^3 - 5$ is irreducible in $Z_{31}[x]$

Date:
Page No:

Q.3.

$Z[i] : a+ib \quad a,b \in Z$

Addition

$\Rightarrow a+ib+c+id = (a+c) + i(b+d)$

$= a' + ib'$

where $a; b' \in Z$

Multiplication of $Z[i]$

$= (a+ib)(c+id) = (ac-bd) + (bc+ad)i$

$= a' + ib'$

$s.t \; a', b' \in Z$

Multiplication table:

.	1	2	i	1+i	2+i	2i	1+2i	2+2i
1	1	2	i	1+i	2+i	2i	1+2i	2+2i
2	2	1	2i	2+2i	1+2i	i	2+i	1+i
i	i	2i	2	2+i	2+2i	1	1+i	1+2i
1+i	1+i	2+2i	2+i	2i	1	1+2i	2	i
2+i	2+i	1+2i	2+2i	1	i	1+i	2i	2
2i	2i	i	1	1+2i	1+i	2	2+2i	2+i
1+2i	1+2i	2+i	1+i	2	2i	2i+2	i	1
2+2i	2+2i	1+i	1+2i	i	2	2+i	1	2i

Date:
Page No:

Therefore $\mathbb{Z}[i]$ is a commutative ring with identity

Now for $(a+ib) \bmod 3$ for inverse

$a, b \in \{0, 1, 2\}$

$3 \times 3 = 9$ combination

$$(a+ib)^{-1} = \frac{1}{(a+ib)} \times \frac{a-ib}{a-ib} = \frac{a-ib}{a^2+b^2}$$

$$\Rightarrow (a^2+b^2)^{-1}(a-ib)$$

∴ For non-zero elements of $\mathbb{Z}[i] \bmod 3$, we need to find that.

Date:
Page No:

a	b	$(a^2+b^2) \bmod 3$	$(a^2+b^2)^{-1} \bmod 3$
0	0	0	-
0	1	1	1
0	2	1	1
1	0	1	1
1	1	2	2
1	2	2	2
2	0	1	1
2	1	2	2
2	2	2	2

Therefore, for non-zero values of $(a+ib) \bmod 3$ the multiplication inverse of $(a+ib)^{-1}$

$= (a^2+b^2)^{-1}(a-ib) \bmod 3$ exists in $Z[i] \bmod 3$

$Z[i] \bmod 3$ is a field

proved.

Characteristics:

We know that characteristics be the smallest number of times one must use the ring's Multiplicative identity in a sum to get the additive inverse.

1) $1+1 = 2 \bmod 3 \neq 0$

2) $1+1+1 = 3 \bmod 3 = 0$

Date:
Page No:

$0+0+0 = 0 \bmod 3 = 0$

$1+1+1 = 3 \bmod 3 = 0$

$2+2+2 = 6 \bmod 3 = 0$

$i+i+i = 3i \bmod 3 = 0$

$1+i+1+i+1+i = 3+3i \bmod 3 = 0$

$2+i+2+i+2+i = (6+3i) \bmod 3 = 0$

$2i+2i+2i = (6i) \bmod 3 = 0$

$1+2i+1+2i+1+2i = (3+6i) \bmod 3 = 0$

$2+2i+2+2i+2+2i = (6+6i) \bmod 3 = 0$

Hence characteristic is 3 of the given gaussian ring.

Q.8.

Ans. $f(x) = x^3 + 2x + 1 \in Z_3[x]$

It is easy to show that $f(x)$ has no roots in Z_3

$f(0) = 0^3 + 2(0) + 1 = 1$ $\quad f(0) = 1$

$f(1) = 1^3 + 2(1) + 1 =$ $\quad 4 \bmod 3 = 1$

$f(2) = 2^3 + 2(2) + 1 = 13 \bmod 3 = 1$

Thus it is irreducible Polynomial

Date:
Page No:

Now $\frac{Z_3[x]}{x^3+2x+1} = I$. is a field with $3^3 = 27$ elements.

$3 \times 3 \times 3 = 27$

$a_0 + a_1 x + a_2 x^2 + I$ for $a_0, a_1, a_2 \in Z_3$.

Q.9.

Ans. Proof By contradiction:

Suppose f is not square-free & write $f^a = g^2 h$ for $g, h \in F[x]$ with $\deg(g) > 0$

Now taking formal derivatives, we have.

$$D(f) = 2g\,D(g)h + g^2 D(h)$$

We can see clearly g is a common divisor of f and $D(f)$. which contradicts our original statement.

So f is square-free.

Date:
Page No:

Q.10.

Suppose we have a homomorphism

$\phi : F \to R$

(F: Field, R: Ring)

Suppose ϕ is not a monomorphism.

By definition, ϕ is not an injection.

So there exist $a, b \in F$ $\phi(a) = \phi(b)$

let $K = a +_F (-b)$

then $\phi(K) = \phi(a +_F (-b))$

$= \phi(a) +_R \phi(-b)$

$= \phi(a) +_R -(\phi(b))$

$= 0_R$ as $\phi(a) = \phi(b)$

Now $a \neq b$ then $K \neq 0$ and so has a product inverse $\exists K^{-1} \in F$

Date:

Page No:

So for any $x \in F$, we can write $x = K \circ (K^{-1} \circ x)$ & so,

$$\Phi(x) = \Phi(K \circ (K^{-1} \circ x))$$

$$= \Phi(K) * \Phi(K^{-1} \circ x)$$

$$= 0_R * \Phi(K^{-1} \circ x)$$

$$= \Phi_R$$

So, if Φ is not a monomorphism, it is the zero homomorphism.

Date:
Page No:

Q.11 $f(n) = x^4 + x + 1$ Irreducible polynomial

$p(\alpha) = \alpha^4 + \alpha + 1 = \alpha^4 = \alpha + 1$

Ex. Representation	Polynomial Representation	Vector Representation $a_0\ a_1\ a_2\ a_3$
αi		
0	0	0 0 0 0
1	1	1 0 0 0
α	α	0 1 0 0
α^2	α^2	0 0 1 0
α^3	α^3	0 0 0 1
α^4	$1+\alpha$	1 1 0 0
α^5	$\alpha+\alpha^2$	0 1 1 0
α^6	$\alpha^2+\alpha^3$	0 0 1 1
α^7	$1+\alpha+\alpha^3$	1 1 0 1
α^8	$1+\alpha^2$	1 0 1 0
α^9	$\alpha+\alpha^3$	0 1 0 1
α^{10}	$1+\alpha+\alpha^2$	1 1 1 0
α^{11}	$\alpha+\alpha^2+\alpha^3$	0 1 1 1
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	1 1 1 1
α^{13}	$1+\alpha^2+\alpha^3$	1 0 1 1
α^{14}	$1+\alpha^3$	1 0 0 1

Date:
Page No:

Q12

The modified hash function h' is not preimage resistant, since for any hash value of y of the form 0||x, a preimage of x.

Therefore, we can find a preimage for atleast one half of all possible hash values.

Now, we prove that h' inherits second pre-image and collision resistance from h. We show that if we can find a collision or a second preimage for h', then we can easily do so for h.

Suppose

$\exists x_0 \neq x_1 : h'(x_0) = h'(x_1)$

Two cases:

(a) first bit of $h'(x_0)$ is 0.
It is impossible as it implies $x_0 = x_1$.

(b) first bit of $h'(x_0)$ is 1. Then $h(x_0) = h(x_1)$ a contradiction, as h is collision resistant.

Q.13.

Ans. Given sequence = 100000001

We can say that sequence has 7 consecutive zeroes. This means that an LFSR of seven or less would lead to an all-zero state after the first bit & then just produce zeroes.

So, we can construct an LFSR of size 8 that produces the given output.

for eg. We use $C_8 = 1$ & other random values. size ≥ 8.

Eg:

Initial state 10000000

1) 10000000
2) 00000001
3) 00000010
4) 00000100
5) 00001000
6) 00010000
7) 00100000
8) 01000000
9) 10000000