Page No.

Date :

TUTORIAL-2

Submitted By :

Kashish Jain
2021JCS2240

Scanned by TapScanner

Page No.:
Date:

Ques-1) Let G be a cyclic group of order n with generator α. Prove that order of $\alpha^K \in G$ is $\frac{n}{gcd(n,K)}$.

Solution-1) Order of an element is an smallest +ve integer 'n' such that $(element)^n = e$, where 'e' is identity element $\in G$. In Case of Cyclic Groups, order of Generator is equal to the Order of Group. In Given Ques, order of Group is 'n', so Order of Generator α, also n : $|\alpha| = n$.

Now we need to show that $|\alpha^K| = \frac{n}{gcd(n,k)}$ where $\alpha^K \in G$

So we have to show two things:

1) $(\alpha^K)^{\frac{n}{gcd(n,K)}} = e$ where 'e' is identity element $\in G$ (definition of order of an element).

2) This $\frac{n}{gcd(n,K)}$ is the least +ve integer s.t:

$(\alpha^K)^{\frac{n}{gcd(n,K)}} = e$, so there is some $p > 0$ s.t

$(\alpha^K)^p = e$ & $\frac{n}{gcd(n,K)} \leq p$.

Let's Proove (1) :

$$(\alpha^K)^{\frac{n}{gcd(n,K)}} = (\alpha^n)^{\frac{K}{gcd(n,K)}} = e^{\frac{K}{gcd(n,K)}} = e$$

{As $\alpha^n = e$ and $\frac{K}{gcd(n,K)}$ is some integer}

Scanned by TapScanner

Page No. :
Date :

Now let's proove (2) :- Let for some 's' $\in N$,

$(\alpha^K)^s = e$ ie. $\alpha^{KS} = e$. Now Since Highest order is of α ie: n, so Ks must divide n or n/Ks, which we can also write as :-

$$\frac{n}{gcd(n,k)} \Big| \frac{k}{gcd(n,k)} \cdot s$$

Now we can easily see that $GCD\left[\frac{n}{gcd(n,k)}, \frac{k}{gcd(n,k)}\right] = 1$

Thus we can write $\frac{n}{gcd(n,k)} \Big| s$, as we found that $\frac{n}{gcd(n,k)}$ & $\frac{k}{gcd(n,k)}$ are relatively prime.

Hence $\frac{n}{gcd(n,k)} \leq s$.

Hence Proved.

Scanned by TapScanner

Page No.:
Date:

Ques- 2) In Elgamal P.K.C, the public key used is (p, α, β). Why is it important that α is primitive root modulo p?.....

Solution- 2) Primitive roots : A number 'α' is Primitive root mod n, if every integer 't' Coprime to n is Congruent to a power of α mod n, that means for every 't' Coprime to n, there is some 's' such that $\alpha^s \equiv t \pmod n$.

In case of Elgamal Public Key Cryptosystem, Public Key is choosen as follows:
First, a large prime p is choosen, then a primitive root modulo p, say 'α' is choosen. Finally for some integer 'k', $\beta = \alpha^k \pmod p$ is computed

And Public key becomes (p, α, β), and integer 'k' is kept as secret (used to calculate β.)
Primitive root is also defined as: If Multiplicative order of a number r modulo n is $= \phi(n)$, then 'γ' is Called a Primitive root.

Now the security of Elgamal P.K Cryptosystem is based on the fact that solving a discrete log problem is infeasible and very difficult.

If any attacker have to attack this Cryptosystem then he would first check whether α in Public Key is Primitive root or not.

Scanned by TapScanner

Page No.:
Date:

Because if α is not a primitive root mod n and is any random integer of Group then attacker would be easily able to find a integer $t < p-1$ such that:

$\alpha^t \equiv 1 \bmod p$. But if α is choosen as primitive root then attacker could never find $t < p-1$ such that $\alpha^t \equiv 1 \bmod p$. Because this is a definition of primitive root that for $t = 1, \ldots\ldots p-1$ $\alpha^t \pmod p$ gives distinct remainders and $\alpha^{p-1} \equiv 1 \bmod p$.

So after finding such a 't', attacker would understand that α is not a primitive root and Thus, discrete log problem has become feasible and attacker will easily find the secret key 'k' using which 'β' is computed and will use it decrypt the message.

But still this not true for all cases : For Eg : when order of α ie- q is large prime then still, attacker could not easily attack, so proposed cryptosystem is still safe.

If the attacker could not find any such $t < p-1$ st : $\alpha^t \equiv 1 \bmod p$, he will understand that α is a primitive root & Solving Discrete log problem is infeasible. Attacker wants either of 'k' or 'a' (use for encryption ie : Generating $\gamma = \alpha^a \bmod p$) to decrypt the message. So because of not being able to solve Discrete log problem & find 'k' or 'a' attacker could not decrypt the message.

Scanned by TapScanner

Page No.
Date :

Check whether (97, 8, 33) a suitable Elgamal Public Key. or not.

In above Public Key, 97 is a prime 'p', 8 should be primitive root mod 97 & $33 = 8^k \bmod 97$ for some k.

Now we shall check, whether 8 is Primitive root or not. Prime $p = 97$ has following primitive roots : 5, 7, 10, 13, ... so 8 is not a Primitive root.
[by finding all prime factors of $\phi(p)$,] and we can check primitive roots

As 8 is not Primitive root, hence (97, 8, 33) is not suitable Public Key.

Scanned by TapScanner

Page No.
Date :

Ques - 3) Man in the Middle attack (MITM).....

Solution - 3) Diffie-Hellman Key exchange is a method of securely exchanging cryptographic Keys over a public channel. Cryptographic Keys are the secret Keys.
In Diffie Hellman Key Ex. algorithm, there are two publicly known numbers :
1) a prime number q
2) a integer α that is primitive root of q.
Now if User A have to send a Key, he selects random integer $X_A < q$ & Computes $Y_A = \alpha^{X_A} \bmod q$ & User B to send a Key, selects random integer $X_B < q$ & Compute $Y_B = \alpha^{X_B} \bmod q$
Then each side makes Y publickly available. After which A Computes Key $K = (Y_B)^{X_A} \bmod q$ and B computes Key $K = (Y_A)^{X_B} \bmod q$.
So Both got the same Key.

Now Attacker uses Man In the Middle attack to exploit the Diffie-Hellman Key-E.A., As there is no means of authentication in D-H-K-E Algorithm.

So Attacker basically intercepts User's A public Value and sends his public Value to User B. When B sends his public Value, attacker substitute it with his own & send to A.

Scanned by TapScanner

Page No.
Date :

Thus User 'A' & attacker agree on one shared Key by following the Mentioned algorithm & Attacker & User 'B' agree on another shared key. After this, attacker can decrypts any messages sent by A or B.

This Vulnerability is present because D-H Key ex. does not authendicate the Users.

Now in Given Ques, Z_{13} is choosen Cyclic Group with 2 as a Generator (α).

And 'A' uses exponent 5 & 'B' uses 4 as exponent & attacker uses exponent 7.

Now if attacker uses MITM attack on the Key exchange between A & B, then :
As 'A' generates his Public Key as :

$\alpha = 2$, $q = 13$, X_A (secret Key) $= 5$

so $Y_A = \alpha^{X_A} \bmod q = 2^5 \bmod 13$
$= 6$

& 'B' generates his Public Key as :

$Y_B = \alpha^{X_B} \bmod q = 2^4 \bmod 13$
$= 3$

Now 'A' sends 6 to 'B' as his public Value & 'B' sends 3 to 'A' as his public Value.

Scanned by TapScanner

But Attacker is sitting between the A & B.

So Attacker also generates his public Value as per MITM attack as :-

$\alpha = 2$, $q = 13$, Exponent = 7

So $Y_{att} = \alpha^{Exp} \bmod q = 2^7 \bmod 13 = 11$

And Attacker sends his public Value 11 (Y_{att}) to User 'A' showing it as a public value came from 'B' only. Similarly sends 11 (Y_{att}) to 'B' also as if came from 'A' only.

Then Both User 'A' & User 'B' uses this $Y_{att} = 11$ to Compute their Key 'K'.

User 'A' Computes :- $K_A = (Y_{att})^{X_A} \bmod q$

$K_A = (11)^5 \bmod 13 = 7$

& User 'B' Computes :- $K_B = (Y_{att})^{X_B} \bmod q$

$K_B = (11)^4 \bmod 13 = 3$

& attacker Computes K_A using 'A' public Value as :- $K_A = (Y_A)^{Exp} \bmod q$

$K_A = (6)^7 \bmod 13 = 7$

& K_B using 'B's public Value

$K_B = (3)^7 \bmod 13 = 3$

So as attacker's K_B, K_A are same as User's B K_B & User 'A's K_A. Hence attacker authenticated himself as Right

Scanned by TapScanner

User to 'A' & 'B' and now would start Exchanging messages with them and User A & B would never come to Know that they were exchanging Messages with some intruder.

Scanned by TapScanner

Page No.:
Date:

Ques-4) G_7 is a non-communitative Group of order 10.....

Solution-4) As G_7 is given as a Non-Commutative Group of order 10, and each element of Group G_7 must be having a Order which is a divisor of 10 (Lagrange's theorem) ie- 1, 2, 5, 10. As Lagrange theorem: states that order of any $a \in G_7$ must divide the order of G_7.

Now as G_7 is Given as Non-Commutative, that means there is no element of order 10. Because if there is an element of Order 10, then it is a Generator & Group becomes Cyclic & Thus Abelian also (Property of Cyclic Groups, that they are Abelian also (Commutative also) but Converse need not true): But as it's Given 'G' is Non-Commutative so that Means there is no element with Order 10. So let's assume each non-identity element has order 2. Then $a \in G_7$, $a^2 = e$ because definition of 'Order' says: It's least +ve integer, to which if an element raised to it's power, we get identity element of Group.

So $a^2 = e \Rightarrow a = a^{-1}$ for all $a \in G_7$

Now if $a = a^{-1}$ because of order of all $a \in G_7$ being 2 then we can also show

Scanned by TapScanner

that $ab = (ab)^{-1}$ where $b \in G$ and $a*b \in G$ and because of $a = a^{-1}$, $ab = (ab)^{-1}$
& using property of inverse ie : $(ab)^{-1} = b^{-1}a^{-1}$

$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ [$\because a = a^{-1}$]

and $a*b = b*a$, makes a Gsoup Commutative [property of a Commutative Gsoup], but our Gsoup G is Given as Non Commutative . So That Means not all $a \in G$ can have an order 2 because if all have order 2 then Gsoup becomes Commutative . Hence there is some element $a \in G$, such that it's order is 5.

Now as we know from one of Theorem : That the "SubGsoup Generated by an element of order p is also has order p". so if surely there is an element of Order 5, then there must be Subgroup of Order 5.

Scanned by TapScanner

Page No. :
Date :

Ques-6) Proove that :

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

Sol-a) $f(x) = x^2+1$ where $F = Z_7$

A polynomial is Called Irreducible if it can not be factored into non-trivial polynomials over the same field, or a polynomial has no root. or if a polynomial cannot be expressed as a product of two polynomials $g(x)$ & $h(x)$ in $F[x]$, where the degrees of $g(x)$, $h(x)$ are both smaller than the degree of $f(x)$.

So if a $f(x) = x^2+1$ is reducible, then it must have roots in Z_7 where Z_7 is having all integers from $\{0, 1, \cdots, 6\}$

so let's check for $0 \in Z_7$

$f(0) = 1$ but on putting root in $f(x)$, result must be 0, but it's 1, that means '0' is not root for $f(x)$.

$f(1) = 2$, again not root as $2 \neq 0$

$f(2) = 5$

$f(3) = 3$

$f(4) = 3$

$f(5) = 5$

$f(6) = 2$

So None of $\{0, 1, \cdots, 6\}$ is a

Scanned by TapScanner

root of $f(x)$.

Hence $f(x) = x^2 + 1$, is irreducible polynomial.

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

Sol^n :- Let's suppose (x^3-9) is reducible in $Z_{31}[x]$. Now as (x^3-9) is Cubic, so it must have linear factor.

But if it has a linear factor say $(x-r)$ then we get 'r' as root in Z_{31}.

Now since we found 'r' as root we can write : $r^3 = 9$, also since 'r' is nonzero, we can write $r^{30} = 1$ as $r^{30} \pmod{31} = 1 \pmod{31}$ {r is coprime to 31 so FLT}

As $r^3 = 9$ or $r^3 = 3^2$

or $(r^3)^{10} = (3^2)^{10}$

$r^{30} = 3^{20}$

or $3^{20} = 1$ $[\because r^{30} = 1]$

but we can show that 3^{20} is not Congurent to 1 mod 31.

Hence our assumption was wrong that 'r' is a root in Z_{31}.

so (x^3-9) is irreducible over Z_{31}.

Scanned by TapScanner

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

$f(x) = x^3-9$

Let's check for each element of Z_{11} from $\{0, 1, 2, \cdots, 10\}$ whether it is root or not:

$f(0) = 2$, $f(1) = 3$, $f(2) = 10$,

$f(3) = 7$, $f(4) = 0$ {means 4 is root}

Hence we found 4 as root that is:

$x^3 - 9 = (x-4)(x^2+4x+5)$.

Hence polynomial x^3-9 is reducible over Z_{11}.

Shortcut Method: as x^3-9 is a Cubic polynomial, so it's one of the factors would have to be linear.

And the ~~form~~ factor would have to be of the form $(x-a)$, where a is a divisor of 9. So we can just check for the divisors of 9, whether it's root of the polynomial or not.

Scanned by TapScanner

Page No.:
Date:

Ques - 7) Gaussian integer is a complex number such that it's real and imaginary parts are.....

Solution - 7) Gaussian integer is a Complex number whose real and imaginary parts are both integers. Also, the Gaussian integers with addition and Multiplication of Complex Numbers, forms a integral domain [that's a Commutative ring].

So $Z[i] = \{ a + bi \mid a, b \in Z \}$ is a ring of Gaussian integers.

Now, we need to proove that $Z_3[i]$ that is: ring of Gaussian integers modulo 3 is a field.

As we Know that a ring is Called a field if:

1) It is Commutative
2) It has unity as a element [ie: 1]
3) And, every non-zero element possesses Multiplicative inverse.
4) Also a field can not have any zero divisors.

Zero Divisors :- If in a Ring R, there is r & s in R st. $rs = 0$ when $r \neq 0, s \neq 0$ then r is Called a left zero divisor and s is called a right zero divisor.

And a ring without zero divisors means if $rs = 0$ in a ring then this implies $r = 0$ or $s = 0$ for all $r, s \in R$.

So for ring to become field, it must not have Zero divisors.

Scanned by TapScanner

Page No. :
Date :

Now let us find our $Z_3[i]$ elements.

$$Z_3[i] = \{ a + bi \mid a, b \in Z_3 \}$$

where $Z_3 = \{ 0, 1, 2 \}$

If we choose a, b as $0 \in Z_3$, we get first element of $Z_3[i]$ as 0.
Similarly if we choose a as $1 \in Z_3$ & b as 0 we get second element of $Z_3[i]$ as 1.
Now, we have to keep doing this for every possible combination of a, b, after which we will get our all possible elements of $Z_3[i]$.

So We get $Z_3[i] = \{ 0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i \}$ where $i^2 = -1$

After Getting all the elements of $Z_3[i]$, we should now make it's Multiplication Table: To create a multiplication table, every possible Combination of 2 elements is multiplied with each other. Except the zero element, every non-zero element is multiplied with every other non-zero element. and then (Modulus 3) is taken.
For Eg: Let's choose first element as 2 and the other as $1+2i$, then upon multiplying these two: $2(1+2i) \bmod 3$
$= (2 + 4i) \bmod 3, \Rightarrow (2 + i) \bmod 3$
So That means $2 * (1+2i)$ gives $(2+i)$.

Scanned by TapScanner

So Our Multiplication Table looks like :

a \ b	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	i	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	2+2i	i	1
2+2i	2+2i	1+i	1+2i	i	2	2+i	1	2i

Note : for any $x \in Z_3[i]$, $3x = x+x+x = 0 \bmod 3$

Now, from above Multiplication table, we can see that none of the cell is 0, that means there are no Zero divisors in our ring because if they were present then we would have got one of the cell as 0.

But as none of the cell is 0, so there are no Zero divisors, and Hence Our Ring is free of Zero divisors. Also $Z_3[i]$, have a unity element ie : 1, & $Z_3[i]$ is Commutative also. As from above Multi. Table, we can see for any a, b we get

$a * b = b * a$ { eg : $(1+2i)*(2+2i) = (2+2i)*(1+2i) = 1$ }

Thus $Z_3[i]$ satisfies all properties of a field Hence it is a field, and also integral domain.

Scanned by TapScanner

Page No. :
Date :

Characteristic of a field :- The characteristic is the smallest Number n such that n times the identity element is zero
ie : $ne = e+e+---+e = 0$
As we Know, in Case of Z_p, characteristic is always p. (because $pn \pmod p = 0$)
Hence characteristic of Z_3 is 3.

Ques-8) Find a polynomial of degree 3 irreducible over the ring .....

Solution-8) Let's find the polynomial of degree 3 which is irreducible over the ring Z_3 :- Let's say $f(x)$ is a degree 3 polynomial in $Z_3[x]$ such that it's reducible. So to be reducible, $f(x)$ must have a factor of degree 1 and hence a root in Z_3. So in order to find a irreducible polynomial ie- a polynomial which has no roots in $Z_3[x]$, we should consider a polynomial $x(x-1)(x-2)$ which clearly have each of $0, 1, 2$ as roots where $\{0,1,2\} \in Z_3$.

Now simply add 1 to $x(x-1)(x-2)$: Obtained polynomial $p(x)$: $x(x-1)(x-2)+1$ will not have any roots in Z_3 because clearly $p(0) = 1$, $p(1) = 1$, $p(2) = 1$ and this isn't 0 in Z_3.

Scanned by TapScanner

Page No.:
Date:

Now, let's expand the polynomial:
$p(x) = x(x^2-3x+2)+1 = x^3-3x^2+2x+1$.

Now, since $-3=0$ in Z_3, just like $-2=1$ in Z_3 so final $p(x) = x^3+2x+1$ which is an irreducible polynomial of degree 3 in $Z_3[x]$.

Now, as we know for any irreducible polynomial $f(x)$ of degree n in $Z_p[x]$, we have:
$Z_p[x]/(f(x))$ is a field of order p^n.

And in our case $p(x) = x^3+2x+1$ is a monic irreducible polynomial, Thus we know:
$$Z_p[x]/(p(x)) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \text{ where } a_0, a_1, \cdots, a_{n-1} \in Z_p\}$$

So $Z_p[x]/(p(x)) = \{a_0 + a_1x + a_2x^2$ where $a_0, a_1, a_2 \in Z_p$ and $Z_p = Z_3$ & $Z_3 = \{0, 1, 2\}\}$

Now as we have 3 choices for each coefficient a_i & 3 such coefficients, so there are exactly 3^3 elements. or 27 elements in this field.

Scanned by TapScanner

Page No.:
Date:

Ques-9) If F is a field & $f \in F[x]$ with $\gcd(f, D(f)) = 1$ (where $D(f)$ is Derivative of f), then f is square free.

Solution-9) A square free polynomial is a polynomial defined over a field such that it does not have as a divisor any square of a non-Constant polynomial or simply, a square free polynomial is a polynomial if it don't have any factor that's a square. For Eg: $x^3 - 5x^2$ has x^2 as a factor and x^2 is a square so this polynomial is not square free.

Also, square free polynomial is also called as a polynomial with no repeated roots. — (1) That means it should not have any multiple root or simply a root of multiplicity 2. For Eg: $x^2 = 0$ has root ± 0, so 0 has multiplicity 2.

Now there is a statement: "If there is a Multiple root of a polynomial, the root is also a root of the derivative of Polynomial". We can show it like this: if there exists $G(x) \in F[x]$ such that: $G(x)^2 \mid f(x)$

Then definitely $G(x) \mid f'(x)$ where $f'(x)$ is derivative of $f(x)$.

Scanned by TapScanner

Now, since GCD (f, D(f)) = 1 (from ques)

that means f(x) & f'(x) are not sharing any common factor or polynomial.
and there is no G(x) ∈ F(x) such that G(x)²/f(x) & G(x) / f'(x).
Also, this shows that f(x) has no multiple roots or repeated roots, because if it having multiple roots then GCD(f, D(f)), would not have Comm = 1, it must be that factor.

Thus from ① we can say f(x) is a square free polynomial.

Scanned by TapScanner

Page No. :
Date :

(Ques-10) Prove that any homomorphism of a field is either a monomorphism or takes each element into 0.

Solution-10) In Order to proove above statement, first we need to find the Kernel of homomorphism function - f.

Now there is a Theorem : The Kernel of a ring/field homomorphism is an ideal.

So we need to find ideals of field, first :

Let say I is any non zero ideal of a field F. So I must Contain, atleast one non-zero element, let say p. Now since F is a field, so $p^{-1} \in F$. And One important pt about Ideals is : They are closed under external multiplication. That means for all $a \in F$, $x \in I$, $ax \in I$. So We use this property to find all elements of ideal.
As I said, $p \in I$ and $p^{-1} \in F$, so $pp^{-1} \in I$
ie. $1 \in I$. Therefore any $w \in F$, $w \cdot 1 \in I$
Hence $I = F$
So Two ideals of a field F are : F (itself) & (0)

Now let's understand the Kernel of Homomorphism :

The Kernel of a (ring) homomorphism is the set of elements mapped to 0.

Scanned by TapScanner

That is : if $f : R \to S$ is a ring homomorphism, then $Ker(f) = f^{-1}(0) = \{ r \in R \mid f(r) = 0 \}$.
ie - inverse image of 0.

In Case of ring homomorphism, Kernel is the ideal.
That is, as we found ideals as F or (0), so Kernel of f is also F and {0}

Now let's consider the first case:
When Kernel (f) is {0}. : In this Case Homomorphism is One to one or injective.

ie : Kernel of a homomorphism is {0} if only if the Homomorphism is one-one.

Proof : Suppose Homomorphism 'f' is not one-one.
Then $f(r) = f(s)$ or $f(r-s) = 0$
which implies $r - s \in Ker(f)$ [acc. to def" of Ker(f)]
and $r - s = 0$, thus $Ker(f) = \{0\}$

Or Suppose 'f' is one-one: Then for $a \in Ker(f)$ and $a \neq 0$ then $f(a), f(0) \to 0$
That means 'f' can't be one-one.

Hence Proved.

Now let's consider the second Case:
When Kernel (f) is F itself.

Scanned by TapScanner

Page No. :
Date :

In this Case Homomorphism of is Zero map.

Proof :- Let's understand the meaning of Kernel being F.

According to definition of Kernel :

$$Ker(f) = f^{-1}(0) = \{ x \in R \mid f(x) = 0 \}$$

ie : Kernel Consists of all those elements which were mapping to 0 [$f(x)=0$]

And if Kernel is given as F, that means all elements of F mapped to 0, [$f(x)=0$ for all $x \in F$]

Hence it shows that Homomorphism function f is a takes each element into 0 or a Zero map.

Hence proved that Homomorphism of a field is either a monomorphism or takes each element into zero.

Scanned by TapScanner

Page No.:
Date:

Ques - 11) Construct the Galois field of 16 elements, $GF(2^4)$ .....

Solution - 11) We have to use polynomial $f(x) = x^4 + x + 1$ to Generate $GF(2^4)$.

As we know in order to Generate all non-zero elements of $GF(2^4)$, we have to use a primitive element α of this finite field GF. As Exponents of this primitive element α gives us all the elements of the field. Such as :

$$\{ \alpha^0 = 1 , \alpha, \alpha^2, \cdots, \alpha^{16-2}, \alpha^{16-1} = 1 \}.$$

Also every element of the field $GF(2^4)$ can be represented as a polynomial :

$$a(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$$

where m is 4 in our case, and polynomial Coefficients are binary, $a_i \in \{0, 1\}$.
So if we make a vector of all these coefficients : $a = (a_0\ a_1\ a_2 \cdots a_{m-1})$

for each field element, we obtain it's equivalent binary representation, using m bits (In our case $m = 4$).

Now a primitive polynomial $p(x)$ of degree 'm' is used to obtain these representations & establish a connection between them.

Scanned by TapScanner

As we know Primitive element is a zero/root of the primitive polynomial so let's put α in $p(x)$.

Our primitive polynomial = $x^4 + x + 1 = p(x)$

So $p(\alpha) = 0 \Rightarrow \alpha^4 + \alpha + 1 = 0$

$\Rightarrow \alpha^4 = 1 + \alpha$ -①

Using relation ①, we can now obtain the polynomial representation of each field element.

$\alpha^5 = \alpha \cdot \alpha^4 = \alpha \cdot (1+\alpha) = \alpha + \alpha^2$

$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3$

$\alpha^7 = \alpha \cdot \alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4$

$= \alpha^3 + 1 + \alpha$

Obtained Table of all elements is shown below:

Now, let's verify $\alpha^{15} = 1$:

$\alpha^{15} = \alpha \cdot \alpha^{14} = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = 1$

α^i	polynomial	$(a_0 a_1 a_2 a_3)$	integer	order
0	0	0 0 0 0	0	-
α^0	1	1 0 0 0	1	1
α^1	α	0 1 0 0	2	15
α^2	α^2	0 0 1 0	4	15
α^3	α^3	0 0 0 1	8	5
α^4	$\alpha+1$	1 1 0 0	3	15
α^5	$\alpha^2+\alpha$	0 1 1 0	6	3
α^6	$\alpha^3+\alpha^2$	0 0 1 1	12	5
α^7	$\alpha^3+\alpha+1$	1 1 0 1	11	15
α^8	α^2+1	1 0 1 0	5	15
α^9	$\alpha^3+\alpha$	0 1 0 1	10	5

Scanned by TapScanner

α^{10}	$\alpha^2+\alpha+1$	1110	7	3
α^{11}	$\alpha^3+\alpha^2+\alpha$	0111	14	15
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111	15	5
α^{13}	$\alpha^3+\alpha^2+1$	1011	13	15
α^{14}	α^3+1	1001	9	15

Scanned by TapScanner

Page No. :
Date :

Ques-12) Suppose there are two Hash f^ns h & h'

Sol-12) A hash function is any function that can be used to map data of arbitrary length to fixed size values. The values returned by a Hash function are called Hash Values.
And Hash function is said to be Pre-Image resistant if for a Given element in the range of a Hash f^n, it is Computationally to find an input that maps to that element.

* Second Pre-Image Resistant : Hash f^n is second Pre image resistant if for a given input m_1, it is difficult to find another input m_2 s.t. $m_1 \neq m_2$ & $hash(m_1) = hash(m_2)$. But point to be noted is : the attacker is handed a fixed m_1 that means attacker can not freely choose m_1 & m_2.

* Collision-Resistant : A Hash f^n is Collision Resistant if it is difficult to find two different messages m_1, m_2 s.t. Hash (m_1) = Hash (m_2) ~~and~~ when attacker is allowed to freely choose m_1.

Scanned by TapScanner

So we can say that Collision resistance implies second - pre image resistance.

Now Acc. to Ques, h' is defined as :

$$h'(x) = \begin{cases} 0 \| x & x \in \{0,1\}^n \\ 1 \| h(x) & \text{otherwise} \end{cases}$$

where $\|$ is a Concatenation operator.

First ~~we~~ I will proove that h' is not pre-image resistant.

Proof : From hash value y, if we are able to get pre-image x st: $h(x) = y$, then hash f^n is not pre-image resistant.
In our Case, for any Hash Value y of form $0 \| x$, we get pre-image x easily. but not possible if Hash Value of the form : $1 \| h(x)$.
Hence we are able to find pre image for atleast Half of all Hash values. Hence h' is not pre-image resistant.

Now Let's proove that h' is second preimage & Collision resistant.

Proof : If h' is not Collision resistant then : for some $x_0 \neq x_1$, $h'(x_0) = h'(x_1)$
that means we are able to find two Hash Values such that they are equal.

Scanned by TapScanner

Page No. :
Date :

Now two Cases arises :-
first Case - 1 :- If $h'(x_0) = h'(x_1)$, and first bit of $h'(x_0)$ is 0. That means $0 \| x$ is used as a hash functions. Which implies if first bit is 0 then $x_0 = x_1$. But we assumed $x_0 \neq x_1$. Hence a Contradiction.

Second Case - 2 :- $h'(x_0) = h'(x_1)$ and first bit of $h'(x_0)$ is 1. That means $1 \| h(x)$ is used as a hash function. Which implies after the first bit, $h(x_0) = h(x_1)$ but as in ques, it's given that h is Collision resistant & Second pre-image resistant. Thus $h(x_0) = h(x_1)$ is not possible. Hence again a Contradiction.
Thus h' is also second pre-image & Collision resistant.

Hence Proved that h' is not pre-image resistant but second pre-image & Collision resistant.

Scanned by TapScanner

Page No.:
Date:

Ques- 13) What is the Minimum size of the linear feedback shift register, which can generate first ~~time~~ 'nine .....

Solution-13) Linear feedback shift Register is a shift Register whose input bit is a linear function of it's previous state.

Generally this function is Boolean Exclusive OR, and the bits that affect the state of in the other bits are called as taps. These are used for pseudo-random number Generation.

An LFSR with 'n' register bits will only sequence through $(2^n - 1)$ values & not 2^n unique values because LSFR's With XOR feedback paths will not sequence through the value where all the bits are 0.

So as 9 bit Output '100000001' is given, in order to get this Output, we need to have Minimum 4 registers.

Because if were having 3 registers then this sequence would have repeated after 7th bit but it's not. Hence Min. 4 registers are required.

Scanned by TapScanner

Page No.:
Date:

Ques-5) Let G be finite Group of order n.....

Sol-5) Group G is of order 'n' ie :- $|G| = n$

& n is coprime to 3 that means $GCD(3,n) = 1$
Now using Euclidean Algorithm, we can write / replace $G(3,n)$ by $3x+ny=1$ for some $x,y \in Z$. using Bezout's Theorem, as 3 & n both are non-zero.

Now $a,b \in G$ & $a*b \in G$,
so we can write $ab = ab^{(3x+ny)}$ because $3x+ny=1$
and $(ab)^n = e$, we can write : $ab = ab^{(3x+ny)} = (ab)^{3x}$
{as $(ab)^n = e$}

so, $(ab)^{3x} = (a^3b^3)^x = \underbrace{a^3b^3a^3b^3.....a^3b^3}_{x \text{ times}}$

$\Rightarrow a^3 \underbrace{(b^3a^3)(b^3a^3)..(b^3a^3)}_{x-1 \text{ times}} b^3$

$\Rightarrow a^3 (b^3a^3)^{x-1} b^3$
$\Rightarrow a^3 (ba)^{3x-3} b^3$
$\Rightarrow a^3 (ba)^{3x} (ba)^{-3} b^3$
$\Rightarrow a^3 (ba)^{3x} (ba)^{ny} (ba)^{-3} b^3$
$\Rightarrow a^3 (ba)^{3x+ny} (ba)^{-3} b^3$ [$\because (ba)^n = e$]
$\Rightarrow a^3 (ba) (ba)^{-3} b^3$
$\Rightarrow a^3 (ba)^{-3} (ba) b^3$
$\Rightarrow a^3 a^{-3} b^{-3} (ba) b^3$
$\Rightarrow b^{-2} a b^3 = b^{-2} a^{-2} a^3 b^3$
$\Rightarrow (b^{-2}a^{-2})(ab)^3$

Now $(b^{-2}a^{-2})(ab)^3 = (ab)^{-2}(ab)^3 = ab$

Thus we get $ab = b^{-2}a^{-2}(ab)^3$

Scanned by TapScanner

Page No. :
Date :

Now if we Multiply left by a^2 & b^2 & right by $(ab)^{-1}$, we get :

$a^2b^2 = (ab)^2$ ie : $a^2b^2 = abab$

Now Multiply right by b^{-1} & left by a^{-1}, we get $ab = ba$ for all $a, b \in G_7$.

Hence Proved that G_7 is Commutative / Abelian.

Scanned by TapScanner