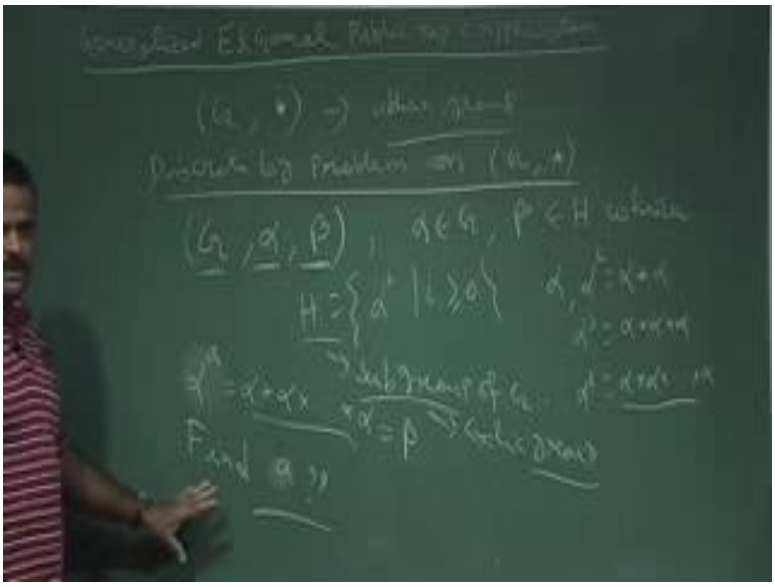
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture – 31
Generalised El Gamal Public Key Cryptosystem

We talk about generalized version of the El Gamal cryptosystem, we have seen the El Gamal cryptosystem of a Z p, but this can be over any group G. So not only we restrict ourselves on Z p so, will talk about generalized version of the El Gamal cryptosystem. So, for that we need to discuss the discrete log problem also in that group.

(Refer Slide Time: 00:50)

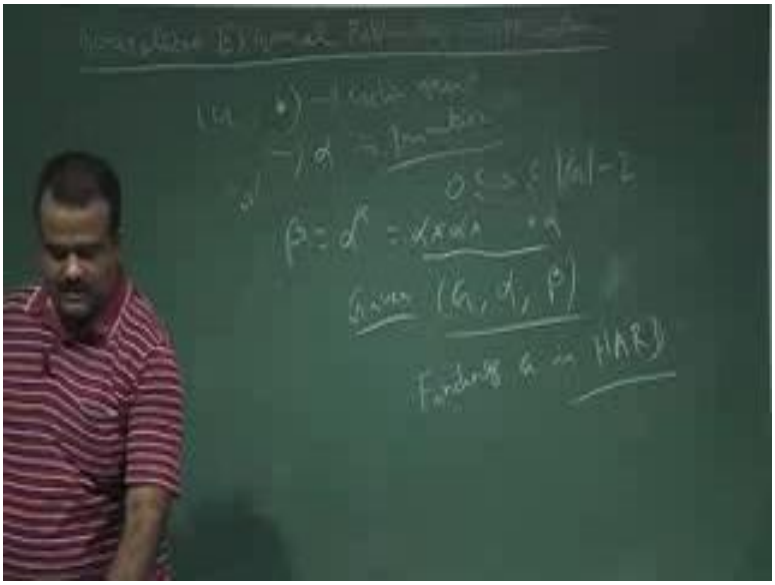


Suppose we have a group G and we have operation star in that group. So, this is Abelian group, now we define the discrete log problem over this group, on this group this is the generalized version of the discrete log problem. So, the problem is we have given a; we have given G alpha beta where G is a finite group and this is the operator on this group and this alpha beta such that we have given that the alpha belongs to G and beta belongs to H where H is basically is the subgroup generated by this alpha. So, this is alpha to the power i, i is greater than equal to 0. So, it is basically a subgroup generated by alpha. So, alpha; that means, alpha; this is alpha square, alpha square means alpha times alpha. So, alpha cube is basically alpha times alpha times alpha, like this. So, alpha to the power i is basically alpha you are operating alpha i times like this. So, this is the group; subgroup

generated by this alpha. So, this is a cyclic group, this is H is the subgroup of G and this subgroup is a cyclic group.

Now, we define this beta so, beta is basically we choose a, we choose a, and we calculate alpha to the power a so; that means, alpha a times so, this is we say beta this is the beta. So, we have given G group, we have given the generator and we have given beta and it is hard to find, the question is to find alpha, sorry, question is to find a. So, that is the discrete log problem. So, if it is hard then we can think of a think of a El Gamal cryptosystem based on this. So, for the simplicity we are taking, so, this is the problem of this is discrete log problem. So, for the simplicity we are taking our group to be a cyclic group. So, this is the general case, but supposes you have a group cyclic group.

(Refer Slide Time: 04:27)

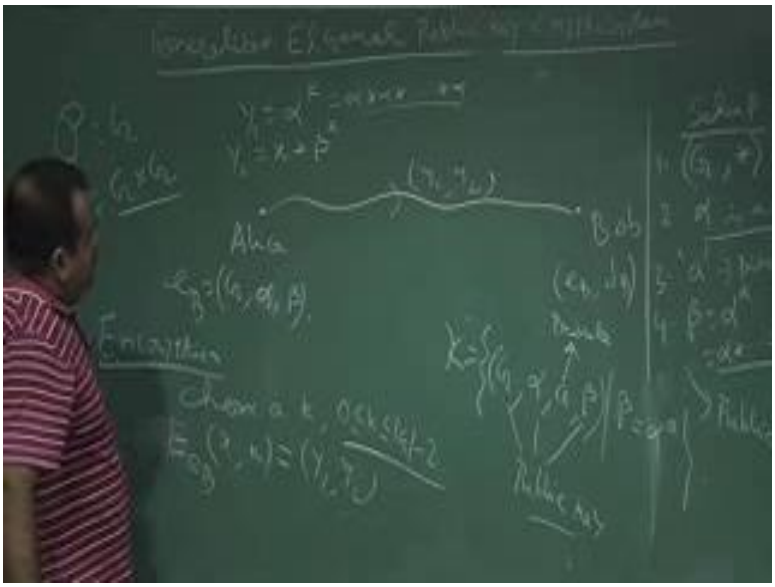


Suppose G is a cyclic group and say alpha is a generator of this group, alpha is a primitive element. So, it can work out on the subgroup also, if you take any alpha then it will generate a subgroup generated by alpha that is H, but for the simplicity we are taking G as a our whole group is a cyclic group and alpha is a generator and we choose a which is which is between 0 a less than equal to the size of the group minus 2 and we compute beta, beta is equal to basically alpha to the power a which is basically alpha cross alpha times and a times alpha.

Now the discrete log problem is basically given this group along with this generator and the beta which is basically alpha to the power a, finding a is hard, finding a is hard, this

is the finding a is the this called discrete log problem and this is if this is hard in this group then we can have a El Gamal cryptosystem based on this group. So, how, then let us talk about that generalize El Gamal cryptosystem based on this group.

(Refer Slide Time: 06:17)



Alice and Bob, Alice also sends a message to Bob. So, Bob has to get Bob's public key and private key. So, this is the setup phase Bob has to run. So, Bob choose a group that generalized group along with this operation and alpha is a primitive element is a generator if this is cyclic group. So, we take a cyclic group is the generator of this group and then Bob choose a which is basically secret to the Bob this is the private key and then Bob compute beta which is basically alpha to the power a which is alpha times a times alpha.

Now, so this is a times alpha and now Bob publish this. So, this is also this beta is public and in this group; the discrete log problem should be hard. So, now, what is the plaintext space? So, plaintext space is basically G and the cipher text is basically G plus G and the key space is basically this is the key space. So, key has this component G alpha a beta such that beta is equal to alpha to the power a and only this is private or secret key and remaining this key is public key of Bob public key. So, Bob made this public. So, this is e B, e B is basically the group G alpha and beta.

Now, Alice wants to send a message to Bob. So, what Alice will do? This is the El Gamal cryptosystem. So, Alice will choose a secret. So, this is a encryption and as we

remember in El Gamal encryption as a G plus G. So, y 1 and y 2 has 2 parts. So, before that Alice has to choose a random number a, Alice choose a k a and then what Alice is doing? Alice is encrypting using this using the Bob. So, this is the encryption using the Bob public key on the message. So, message is coming from along with this random number k and this is y 1 y 2 basically and or sending to sending this y 1, y 2.

So, what is y 1? Y 1 is basically alpha to the power k and y 2 is basically x masking beta to the power k. So, alpha to the power k means alpha time k and so, this k is coming from 0 less than k less than G minus 2. So, this is the random number Alice is choose in then alpha times this G, this star, this group operation, a times, k times on this alpha, this is basically alpha; alpha k times. So, this is alpha to the power k then this is k times beta then followed by this x masking and sends it to Bob.

Now, how Bob will decrypt it? So, this is the encryption process and for decryption so, upon receiving the cipher text y 1, y 2.

(Refer Slide Time: 10:48)

This is the decryption made by Bob. So, upon receiving the cipher text y 1, y 2, what Bob will do? Bob will just compute y 2 into means this operation y 1 to the power. So, Bob is having secret a y 1 to the power a inverse and this should give us basically x. So, this is the description for generalize El Gamal cryptosystem. So, if we have a group if we can get a group G which is having a generator and so, if we can get a cyclic group G which is having a generator then we can think of a of an El Gamal cryptosystem. So, this

is the generalized version of El Gamal cryptosystem. So, based on this idea, we can have what is called El Gamal cryptosystem of our elliptic curve points. So, let us talk about that, but the idea is this. So, if we can have a group from anywhere I mean maybe from elliptic curve points. So, that Z p you know Z p was a group Z p star. So, for that we have a elliptical much for that we have El Gamal version.

(Refer Slide Time: 12:31)

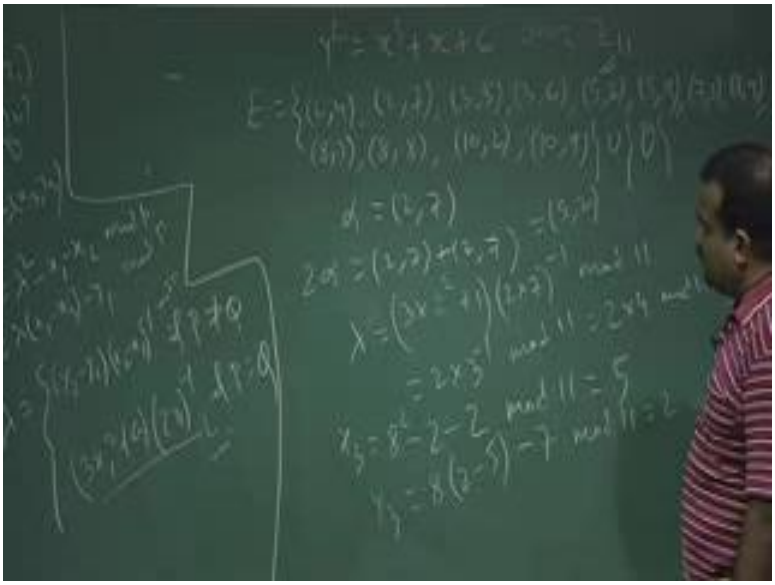
Now we know the elliptic curve points over Z P. So, now, we talk about El Gamal cryptosystem; cryptosystem over elliptic curve points. So, we have seen suppose we take this elliptic curve for example, over Z P. So, this is say x y and x y is coming from Z P cross Z P, Z P cross Z P such that our P is a prime, y square is congruent to x cube plus a x plus b mod P and a b are coming from Z P and we have this non singularity conditioned 27 b square is not congruent to 0 mod P then we know this along with this theta this form a this is the elliptical points and this will form a group Abelian group under the addition operation and this addition operation is defined as like this.

So, if you take any 2 points P Q from this, if you take any 2 point P Q. So, say P is equal to x 1 y 1, Q is equal to x 2 y 2 and if we know the if Q is equal to minus P, this is the point at infinity, now if Q is not equal to minus P then P plus P is basically R which is x 3 y 3 and we know the formula for this. So, basically x 3 is so, x 3 is basically lambda square minus x 1 minus x 2 mod P and y 3 is basically lambda into x 1 minus x 3 minus y 1 and the lambda is. So, this will use for elliptic curve y 2 minus y 1 into x 2 minus x 1

inverse if P not equal to Q is P not equal to Q and it is basically 3 x 1 square plus a 2 y 1 inverse if P is equal to Q. So, this is the formula for addition.

Now this, under this addition you will form a group. So, will use that group to have a ellipse to have a El Gamal cryptosystem. So, will take an example, so, suppose our P is 11 and we take a curve under Z 11 sorry.

(Refer Slide Time: 16:22)



Suppose we take this curve y star equal to this you have seen last class x plus 6 and this is over Z 11. So, our points are coming from Z 11 or P is 11 and we have seen the points are basically. So, E is basically we have seen these points like 2 comma 4. 2 comma 7, let me just write it again, 3 comma 5, 3 comma 6. So, 5 comma 2, 5 comma 9 and then excuse me 7 comma 2, 7 comma 9 and we have 8 comma 3, 8 comma 8 and 10 comma 2, and 10 comma 9. So, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, this along with the point at infinity so, this will form a group over elliptic curve point, these are the elliptic curve points and this will form a group over Z p.

Now, we need to choose a primitive element. So, this is a finite group and 13 elements. So, we need to choose a primitive element. So, let us try to get a primitive element. So, that we can construct the El Gamal cryptosystem, let us choose alpha is say 2 comma 7, we can just verify whether this is a generator of that group or not. So, how to verify this? So, if we take this now how to calculate 2 alpha, 2 alpha is basically plus 2 comma 7.

So, now, this is the addition, this addition formula is written over here. So, this is the case when P is equal to Q P is equal to Q. So, we have to use this formula x 3 using. So, everything under mod P this is also under mod P this is also under mod p. So, we just simply use this formula x 3 we calculate lambda. So, lambda square will be coming from this formula in P is equal to Q. So, this is under mod P. So, you just calculate this value and we got lambda and so lambda is basically coming from this formula 3 into x square x 1 square is 2 square plus 1 into, so, a is 1, this is the curve 2 y 1. So, y, this is basically 7. So, 2 into 7 inverse mod 11, so, this is basically coming out to a 2 into 3 inverse mod 11.

This is basically 2 into 4 mod 11, this is 8. So, lambda is coming out to be 8. So, once you have the lambda, once we have a lambda. So, we can use this formula to get this x 3 and y 3. So, the sum, so, basically then x 3 will be so, lambda square 8 square minus y 1 minus y 2, here y 1 y 2 is same which is basically 2, 2 minus mod 11. So, it is giving us basically 5 and y 3 is basically. So, y 3 is basically this formula. So, 8 into 8 into 2 minus 5 minus y 1, so, minus 7 mod 11, this is coming out to be 2; that means, 2 alpha is basically 5 comma 2. So, we got this 5 comma 2.

So, similarly we have to calculate 3 alpha. So, this is in additive sense. So, this operation is additive sense operation. So, it is it has this 2 alpha 3 alpha. So, 2 alpha means alpha times alpha, alpha we operate and 3 alpha means alpha operate alpha operate alpha. So, like this; this is additive same.

(Refer Slide Time: 21:54)

How to calculate 3 alpha? So, we got 2 alpha then to calculate 3 alpha. So, 3 alpha is basically 2 alpha plus alpha, now 2 alpha we know just now we have calculated and alpha is this, now for this also we have to use the formula, but here P Q are not same. So, we have to find this addition P plus Q. So, this is x 1, y 1; x 2, y 2. So, P Q are not same. So, if P Q are not same this is the lambda. So, if we use the same formula will be getting this as a say 8 comma 3, 8 comma 3, this one. So, similar way if we continue. So, 4 alpha will be 10 comma 2 5 alpha will be 3 comma 6, 6 alpha will be 7 comma 9 and 7 alpha is 7 comma 2, 8 alpha is basically. So, these you have to calculate. So, 3 comma 5, so you have to calculate based on this addition rule 3 comma 5, 9 alpha is basically 10 comma 9 and then 10 alpha is basically 8 comma 8 and 11 alpha is basically 5 comma 9, like this we continue 12 alpha is basically 2 comma 4. So, if we just check we are getting all the points. So, alpha is basically a primitive element. So, alpha is equal to 2 comma 7 is a generator of this group is a primitive element. So, we got the primitive element. So, we can use this to have a El Gamal cryptosystem.

How we can do that? So, basically, so this is this setup is done by Bob. So, Alice wants to send a message to Bob and they are going to use this elliptic curve point. So, Alice wants to send in message to Bob and they have decided to go for El Gamal cryptosystem over the elliptic curve points. And discrete log problem is quite hard here because to calculate itself this addition is expensive. So, you have to calculate lambda, you have to calculate this x 3, y 3 like this. So, the discrete log problem over this elliptic curve point is hard. So, if we assume that then we have El Gamal cryptosystem over this.

So, the Bob chosen this alpha, this is the setup phase. So, both this is the elliptic curve. So, the primitive element is 2 comma 5, this is Bob and then Bob choose a, which is 7 say and then Bob calculate beta. So, this is 7 alpha which is basically 7 alpha is basically 7 comma 2, 7 comma 2.

Now the encryption; so, then Bob make this public, this is public, this is public and the elliptical points of public, only this k now suppose Alice wants to send a message x which is coming from the elliptic curve point E. So, this is Alice wants to encrypt. So, Alice has to choose also a k which is the random number. So, Alice will encrypt using this Bob public key. So, Bob public key is basically e B is basically alpha beta and; obviously, the elliptic curve. So, encryption of x comma k using e B is basically y 1 y 2 here y 1 is basically so, y 1 is basically what? Y 1 is basically k times alpha and y 2 is

basically x plus, this is masking. So, our operation is addition operation, this is plus k times 7 comma 2, this is the beta. So, beta to the power k, so, this is the additive self, so k plus beta.

So, this is basically and the so, this is basically encryption and the decryption is. So, the decryption is description means Bob is receiving y 1 and y 2. So, Bob will just calculate apply this using this Bob secret key d B on this y 1 and y 2 is basically y 2 minus 7 1 1. So, this is an additive sense. So, basically it is y 1 to the power 7. So, additive sense 7 y 1 then inverse; inverse is basically minus.

Bob will calculate this, now suppose let us take an example, suppose x is the messages say 10 comma 9. So, Alice choose this message to send and Alice chooses k is equal to say 3. So, then Alice will calculate this y 1, y 1 is basically 3 into this. So, this is basically 8 comma 3. So, 3 alpha 8 comma 3 and x plus this, so this is basically x is 10 comma 9 plus k is 3 and 7 comma 2. So, this if we calculate, this is 10 comma 9 and this will be 3 comma 5 and this is basically 10 comma 2. So, this is y 1 and y 2. So, this y 1 y 2 it send it to Bob and after receiving this y 1 y 2, how Bob will get back. So, Bob is receiving this 8 comma 3 and 10 comma 2, this is y, this is the cipher text y 1 y 2. So, what Bob will do? Bob will simply do this, y 2 minus 7, 8 comma 3. So, this will be basically 10 comma 2 minus 3 comma 5. So, minus 3 comma 5 is basically plus 3 comma 6. So, this is basically 10 comma 9, which is the message sent by Alice. So, this is the El Gamal Hershel over the elliptic curve points.

So, if we can have a group typically if it is have a cyclic group then it has a generator and then we can construct El Gamal version over that group. So, this is over the elliptic curve points.

Thank you.