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

Lecture – 33
Rabin Cryptosystem

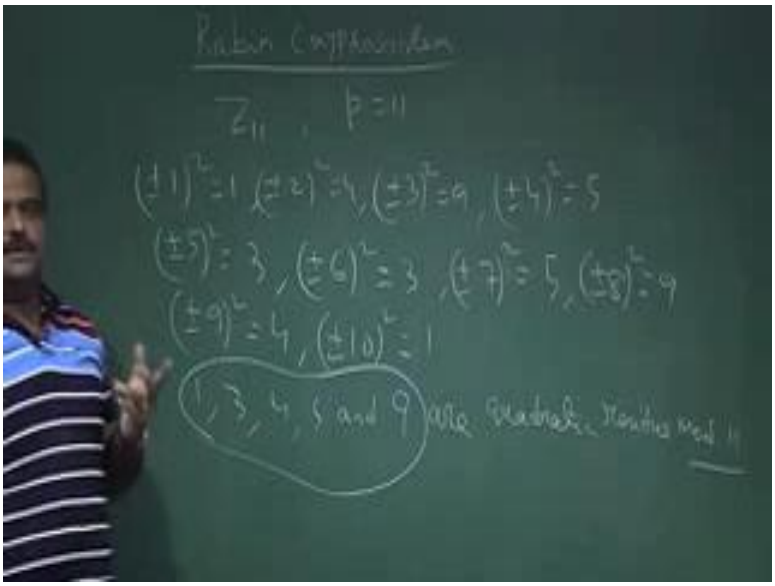
We will talk about Rabin cryptosystem. So, we have seen the Chinese remainder theorem and it also use what is called quadratic residue.

(Refer Slide Time: 00:29)

We will just recap what is the quadratic residue, what do you mean by quadratic residue mod, some prime, modulo P. So, this you know let P where P is a prime, typically odd prime and a is an integer then the definition is a, a is called a quadratic residue, called a quadratic residue; residue mod P if and only if this modular equation y square equal to a mod P has a solution in Z p.

That means, if there exists a y in Z p such that y square is congruent to a mod P so; that means, a should have a square root. So, basically we can write y is basically the root over of a something like that I mean here root over means this sense quadratic residue. So, this is the definition of quadratic residue we have seen this and now. So, let us take an example suppose P is equal to 11, then what are the integers with the quadratic residue mod 11?

(Refer Slide Time: 02:15)



Suppose we are talking about Z 11. So, P is 11, so, then so, y must belong to Z p. So, we will take the possible wise. So, let us take plus minus 1 square is 1 plus minus 2 square is 4 6 squared is 9 plus minus 4 square is basically 16, but it is under mod 11. So, it is basically 5 then plus minus 5 square is basically 3 plus minus 6 square is 36 in mod 11, it will give us 3 again and then plus minus 7 square.

These are possible wise basically is 5 plus minus a square is basically 9 and plus minus 9 square is basically 4 plus minus 10 square is basically 1. So, basically so, these are all possible wise. So, these are the number which are having this is our a I mean this is having self square root for 4, this there are 2 square roots plus 2 minus 2. So, plus 2 is basically 2 and minus 2 is basically this 9. So, this way so, these are the number. So, 1 3 4 5 and 9 are basically quadratic residue modulo mod 11.

Quadratic residue mod 11 so, under Z 11, these are the having the square root. So, now, in general how we can check whether a is a quadratic residue or not. So, we have seen this is by Euler criteria. So, we have given a prime number P and we have given a; a and how to check a is a quadratic residue or not? So, this is by the Euler.

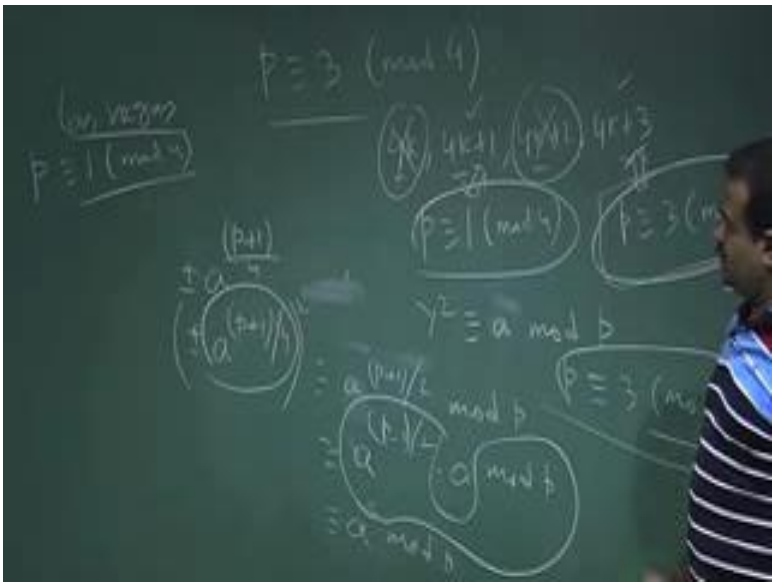
(Refer Slide Time: 04:48)

Euler criteria to check the quadratic residue, so, P again; the same thing, P is a prime, let P be a prime and a is an integer and we know this theorem that a is a quadratic residue; quadratic residue mod P if and only if a to the power P minus 1 by 2 is congruent to 1 mod P.

This theorem is by Euler's and we have seen the proof in our mathematical background portion. So, this is by Euler. So, this is to check if this condition satisfy, if this is satisfied then a is a quadratic residue. So, this will tell us whether is a quadratic residue or not, but this will not give us the square root. So, to get the square root, so, this will only tell us whether a is quadratic residue or not, yes or no.

Now, if it is no there is no question go further, but if it is yes then how to get those how to get the y such that y square is congruent to x mod P. So, how to get the square root of x? Basically so, how to get those solutions y, so that is another questions that we require for our Rabin cryptosystem. So, in general it is hard.

(Refer Slide Time: 07:00)



But if we if P is of the form 3 mod 4. So, P is an integer P, we are choosing as a prime, P is an integer basically. So any integer can be written as if this is mod 4, any integer can be written as either 4 k, 4 k plus 1, 4 k plus 2, 4 k plus 3. So, any integer will be either of this form, either it is 4 k form; k is another integer or 4 k plus 1 from, or 4 k plus 2 or 4 k plus 3.

Now, P is a prime. So, these 2 are odd numbers. So, this is not prime, so, this is automatically cancelled. So, we have to choose P as a prime. So, this is 4 k and 4 k plus 2 we cannot choose. So, we have only to options these 2. So, this means P is congruent to one mod 4 and this means P is congruent to 3 mod 4. So, we will basically consider this for our Rabin cryptosystem why because for this the square root; getting square root is easy, there is the deterministic polynomial time; deterministic algorithm to find the square root, suppose we have equation like this y square equal to x mod P.

Now, we have to find square root of x I mean suppose x is a quadratic residue. So, we have to find the solution y. So, that if P is of this form, then we know the solution then the solution will be of the form of this is basically solution will be like this P to the power. So, this is basically y. So, suppose anyway, this is suppose let could be a. So, if it is a then we know that solution is basically plus minus a to the power P plus 1 by 4, here we write very carefully plus minus a to the power P plus 1 by 4 y, this is this to the mod p.

So, this is the solution for this when P is equal to of this form y, this is a solution because if you take the square of it provided a is a quadratic residue; that means, provided that Euler criteria satisfied. So, if you take the square of it. So, this is basically y, we are suspecting if you take the square of this. So, this will give us what this will give us? This is y to the power. So, P plus 1 by 2 sorry, 1 by 2 mod P, now this is basically sorry, a to the power this is the basically a to the power P minus 1 by 2 into a mod P.

Now, this by Euler criteria this is basically 1. So, this will give us e mod P. So, this a mod P so; that means, these 2 is the solution for this system of this modular equation provided P is of this form, now if P is not of this form, if P is of this form then there is no polynomial time deterministic algorithm to solve this, but there is a algorithm which is polynomial time, but non deterministic that is Las Vegas; Las Vegas algorithm when P is, but that is not determine non deterministic P is 1 mod 4, but for getting solution in a polynomial time deterministic way, we need to assume this. So, this is the assumption, we will make for our Rabin cryptosystem in order to get the square root of this a. So, we will come to Rabin cryptosystem.

So, this is a public key cryptosystem and this is invented before RSA, but this cryptosystem is having ambiguity besides a cipher text is ambiguous

(Refer Slide Time: 12:13)

This is a public key cryptosystem. So, Rabin cryptosystem, so it is a public key cryptosystem and it was invented much before r s a, but this is having some drawbacks

we will come to that. So, since this is a public key cryptosystem. So, we have to get the public key private key pair for the receiver.

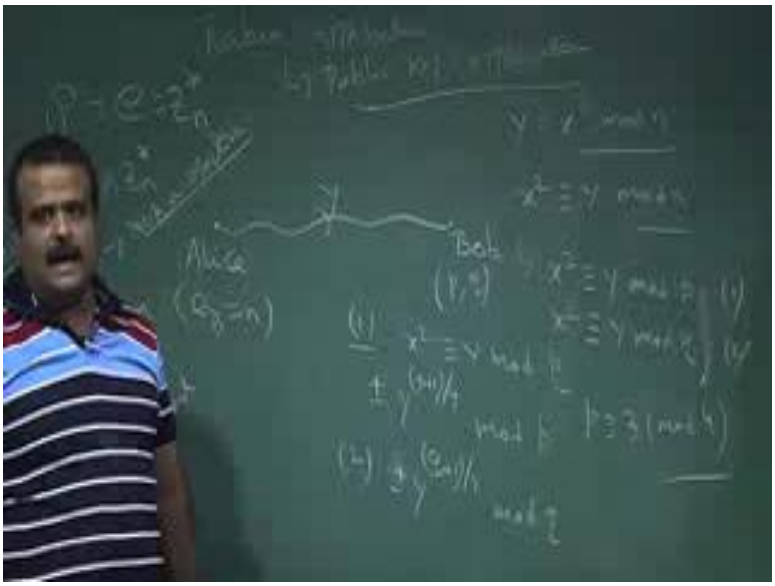
Now, suppose Alice wants to send a message to Bob in a public key setup so; that means, Alice need to get Bob public key sorry this is Alice need to get Bob public key and Alice will encrypt this using the Bob public key encrypt the message Alice will choose a message and Alice will encrypt the message using Bob public key and Bob is having Bob a this is the encryption public key encryption and Bob is having Bob secret key. So, what Bob will do Bob will decrypt y using Bob secret key and this is basically d b of e b of m. So, this should give us m back. So, this is decryption this is encryption this is the public key setup.

Now, the question is. So, Bob is the receiver. So, Bob has to generate this public key private key pair and then Bob has to announce this is my public key then only Alice can send a message to Bob. So, this is this public key private key pair setup this is the key generation algorithm key generation. So, this key has to generate by the Bob. So, this is the setup phase which has to done by the Bob because Bob is the receiver Alice is sending message to Bob.

So, at the setup phase what Bob will do? So, Bob will choose 2 prime P and q 2 prime such that both are congruent to 3 mod 4 this is we have seen in order to have the square root I mean we will come to that where we need this to get the solution for the I mean quadratic residue. So, the square root, so, this is the condition and this is one of the restrictions of Rabin cryptosystem, but if we have if we choose congruent because these are prime. So, if we choose congruent to 1 mod 4 then we have to apply the Las Vegas algorithm which is not deterministic.

Anyway, so this is the setup. So, choose this and then Bob compute P into Q and this is the key of Bob. So, this n P Q, so, this is the key space of Bob and this is the public key of Bob e b which is basically n this is the public key of Bob and these 2 is d b which is the secret key of Bob or the private key this is the public key of Bob and this is the private key or the secret key Bob P and q both. So, Bob keep P Q to himself and Bob make this n published public. So, Alice will be knowing this n Bob public key.

(Refer Slide Time: 16:13)



Now the plaintext, cipher text space is basically Z n star. So, Alice will choose a plaintext from Z n star, suppose x is the plaintext. So, Alice is choosing a plaintext from Z n star and Alice is having Bob public key. So, what is the encryption? Encryption is basically e k of. So, e k of this is above public key the key x is basically x square mod n. So, Alice will just do the square root of it and then take the mod and this is the y in the cipher text and this cipher text Alice will send to Bob y.

Now this is Alice can you just make the square root, square it and take the mod n and send it to Bob. So, this is the encryption this is Rabin encryption. So, now Bob, how Bob will decrypt it? So, Bob has to get back x Bob is getting y, so, the first of all, so that is why it is. So, there could be many many x which is mapping to y. So, that is why, this is not an injective function, this is not a injective function that is 1 of the drawback of this cryptosystem. So, Bob will be getting many x for which the y is the cipher text. So, Bob will be confused which x is the plaintext was chosen by the Alice.

Now what is the decryption? How Bob will decrypt it? So, Bob is having P Q is the Bob public key. So, now, this is basically we have. So, Bob is getting y. So, y is basically what y is basically some x square mod n now Bob need to get back x. So, now, how Bob will get back x so; that means, x square is equal to y mod n now by Chinese remainder theorem so, this can be breaking into 2 part, So, x square is equal to y mod P and x square is congruent to y mod Q. So, this 2 system if this if this 2 system has a solution

and that solution is basically this x square equal to, so, this is just a Z mod n. So, this is coming from Chinese remainder theorem.

Now, the question is how to solve this, now we know that. So, for this is equation 1, this is equation 2. So, let us deal with. So, this is the decryption process Bob is doing, let us the deal with equation 1. So, from equation 1 x square is congruent to y mod P, now here we assume P is 3 mod 4, in order to get the solution for these equations. So, then what is the solution? We know the solution is basically a plus minus y to the power P plus one by 4 mod p. So, we have 2 solutions from here for this is the solution for this and from equation 2 also we have 2 solutions plus minus y to the power Q plus 1 by 4 mod Q.

Basically you have 4 solutions and these are the possible plaintext and from here. So, that is why it is the cipher text is not it ambiguous, it is not unambiguous, it is ambiguous because we have 4x which is mapping to that y the cipher text. So, the Bob will be confused among this 4 which 1 is Alice was chosen. So, that is why this cryptosystem is having the ambiguity. So, which one is Alice has chosen. So, let us take an example, so, basically these 4, so, plus this minus this mod P plus this minus this mod Q, so, these 4 at the possible plaintext.

Now, Bob has to think which 1 is the plaintext Alice was chosen. So, let us take an example of this cryptosystem.

(Refer Slide Time: 21:56)

Example of Rabin cryptosystem, example of Rabin cryptosystem, so, now, Alice wants to send a message to Bob. So, Bob has to generate this key generation phase or this setup phase Bob has this is the key generation phase, these has to be done by Bob because Bob is the receiver. So, if I want to send a message to Bob in a public key setup I need to get Bob's public key. So, this key generation has been done by Bob. So, once Bob complete this key generation. So, then Bob will be having Bob public key, private key pair, excuse me, then Bob will make Bob's public key as public in a public domain or can announce in a. So, the setup phase we know we have to choose 2 prime, but they must be congruent to 3 mod 4.

Let us take 2 prime P is equal to say seven and Q is equal to say 11 and Bob compute this Bob's public key which is basically P into Q which is 77. So, this is basically e b of Bob; Bob public key and this Bob make public. So, e b of Bob is basically 77. So, this is the setup phase and it is done.

Now, so the key's key space under cipher text space is basically Z star 77, Z star 77 means it is the all integer less than 77 which are relatively prime to 77 and the cardinality of this number is 5 77. So, this is basically cardinality of this number is 5 77 and this is basically phi this is phi P Q. So, this is basically P minus 1 into P minus 1 and this is how many elements are there this is 6 and this is 10. So, 60 elements are there in the plaintext space and all the elements basically Z n star are this is basically set all the elements all the integer all the positive integer less than seventy seven which are relatively prime to 77.

So, this is the star. So, all the all the elements which are less than seventy seven, but it must be relatively prime. So, Alice has to choose a plaintext from this or the message has to be coming from Z 77, suppose message is x, Alice is chosen a message and then what is the encryption? Encryption is basically e k is basically. So, k is this e k of x is basically x square mod seventy seven and this is the y and y is the cipher text Alice is sending to Bob. So, what Bob will do Bob has to decrypt for decryption using the secret key Bob. So, this is basically square root of this. So, square root means we have to perform those ah solution for this quadratic residue equations.

Let us take an example suppose y is 23. So, Alice choose a message x and for which this is coming to be 23, now 23 is the cipher text. So, 23 is going to Bob. So, how Bob will

decrypt it? So, that is the and there will be some ambiguity will be there. So, to decrypt it, so, Bob has to get the solution so, by Chinese remainder theorem, so x Bob has to find x square a x such that x square is congruent to actually x square is congruent to 27, 23 mod 27, but this from here we can say this is by Chinese remainder theorem x square is congruent to 23 mod 7, this is 1 equation an x square is congruent to 23 mod 11. So, we have to solve these 2 separately and then the solution will give us the solution for this.

If we take this equation, if this is equation 1, equation 2 did not onto here. So, this is basically from equation 1 we can say that 23 to the power P plus 1 by 4 plus minus. So, this will give us mod7. So, this n plus minus 23 to the power 11 plus 1 by 4 mod 11 so, these 2 will give us the solution the solution plus minus 10 and plus minus 32 mod 77. Basically possible x is 10, 32 then minus 10 which is basically 67 and minus 32 which is basically 45, 45 and 67. So, these are the possible plaintext corresponding to this cipher text 23, these are possible plaintext, Bob is getting possible plaintext corresponding to the cipher text corresponding to the cipher text 23. So, Bob is getting all these plaintext.

Now, Bob will be confused which 1 is the correct plaintext. So, that is why this system is not unambiguous, this is the ambiguous system. So, Bob has no way to know how to what is the plaintext used by the Alice among this. So, Bob is getting four plaintexts from this cipher text 23. So, Bob will be confused. So, now, Bob has to somehow guess which 1 could be the plaintext if it is a age of Alice then maybe 10 is not possible, 67 is not possible, 40, 45 maybe not possible. So, maybe 32, so some type of guess is required. So, that is why this cryptosystem is become not popular because of this ambiguity.

Thank you.