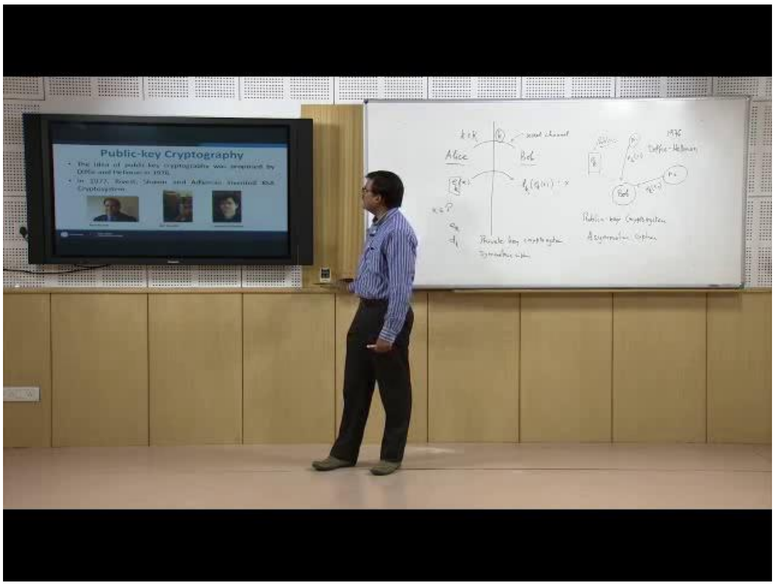
Introduction to Cryptology
Dr. Sugata Gangopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology, Roorkee

Lecture – 11
Public Key Cryptology Introduction, RSA Cryptosystem

Hello, welcome to Week 3, Lecture - 11. In this week, we will introduce public key cryptosystems or asymmetric ciphers. Of course, the first question that comes to mind is that what are the public key cryptosystems? And what is symmetry and asymmetry in a cipher? Now, for that let us think of what we have done already. Now, we have been looking at situations where Alice, the sender wants to send a message to Bob.

(Refer Slide Time: 01:02)



Public-key Cryptography

- The idea of public key cryptography was proposed by Diffie and Hellman in 1976.
- In 1977, Rivest, Shamir and Adleman invented RSA Cryptosystem.

Now, what Alice does is that she chooses a key from the key space and transmits to Bob by a secret channel, and once this key exchange takes place after that Alice uses the encryption function to encrypt the messages or plain text and sends to Bob. Bob uses decryption function corresponding to the key on the encryption function applied on the message to get back x.

So, this is what happens. Now, we look little more closely we will see that in a way there is a symmetry of the knowledge or a symmetry on the knowledge that is shared by Alice and Bob. The secret that they shared together has a symmetric property in the sense that they know the same thing essentially because of course, they have to exchange a secret key which is not known to all, only Alice and Bob knows. Now, suppose instead of giving Alice the key, suppose Bob kept the key to himself and gave Alice only this encryption function, but then the type of ciphers that we have seen so far they are the knowledge of encryption function will let Alice know the decryption function without any difficulty.

For example, if Alice and Bob are using shift cipher then of course, I mean it is just the key is something between 1 and 20, 25 and we have just take minus of that key and reduce modulo 26 and then Alice will know the decryption function and it similarly for affine functions and for other functions and then we will see the block ciphers that we have studied there also the keys encryption key and decryption keys are kind of interchangeable in the sense that if somebody knows the encryption key, he will be able to know the decryption key and vice verse.

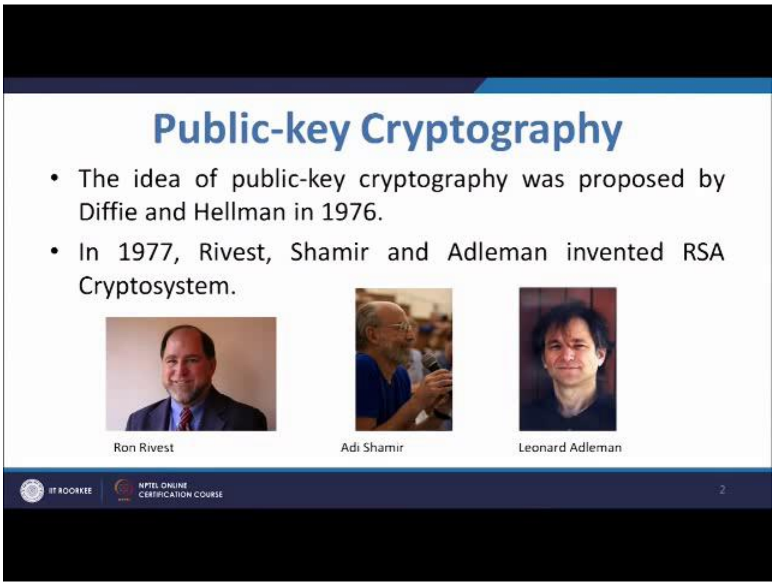
So, that is a symmetry that we have in symmetric cipher. So, these are called private key cryptosystems or symmetric ciphers. Now, there is a problem with symmetric ciphers it is like this, suppose that Bob has to communicate to several people and those need not have had secret channel with Bob. So, that they could have communicated the keys, the secret key then what will Bob do? So, it was proposed somewhere around 1976 by Diffie and Hellman that something can be done here that probably Bob can publish a key or let us say, an encryption function into public, such that anybody who would like to communicate to Bob will use this encryption function and send in the message like someone.

Let us say, this is a 1 then let us say a 2, he is sending a message like this, let us say a 2 is sending x 2 and like that, but this encryption function will be such that knowledge of encryption function does not let the person with that knowledge the ability to compute the decryption function.

Then if he knows the encryption function the whole construction should be such that the computation of the decryption function becomes infeasible, if that happens then we will have something that will be called a public key cryptosystem or asymmetric cryptosystem, where the asymmetry is with respect to the knowledge of the sender and the receiver that is the sender does not, I mean even if the sender knows the encryption function she is unable to know the decryption function.

So, there is an asymmetry although the receiver knows the both, because of course, the encryption function is publicly available and the decryption function is a special knowledge that receiver has. So, it is called private public key cryptosystem or asymmetric ciphers. Then the question occurred to people is that well an idea it is good, but are they are efficient and algorithms which for a public key crypto systems and that was designed just 1 year after the publication of Diffie-Hellman's idea in 1977 by Rivest, Shamir Adleman and they designed something which is called the Rivest, Shamir Adleman's cryptosystem or RSA cryptosystem in short and this is what it is.

(Refer Slide Time: 08:29)

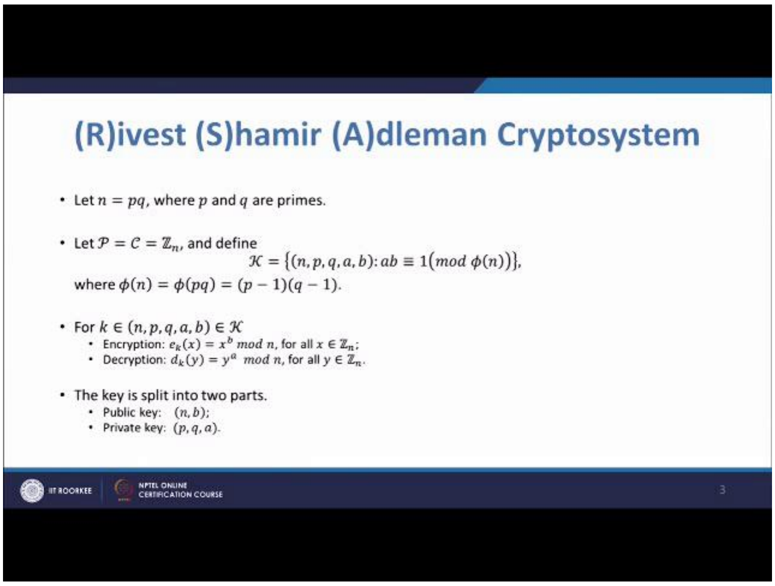


Public-key Cryptography

- The idea of public-key cryptography was proposed by Diffie and Hellman in 1976.
- In 1977, Rivest, Shamir and Adleman invented RSA Cryptosystem.

So, the idea of public key cryptography was proposed by Diffie and Hellman in 1976 by the way, although it is known today that these was known possibly in late sixties by the British and American intelligence agencies, but it was kept confidential, but in academics the idea of public cryptography was proposed by Diffie and Hellman and just 1 year after that Rivest, Shamir and Adleman proposed RSA cryptosystem which is a practical implementation of the idea. Now, we will move on to RSA cryptosystem and these are the details of RSA cryptosystem.

(Refer Slide Time: 09:29)

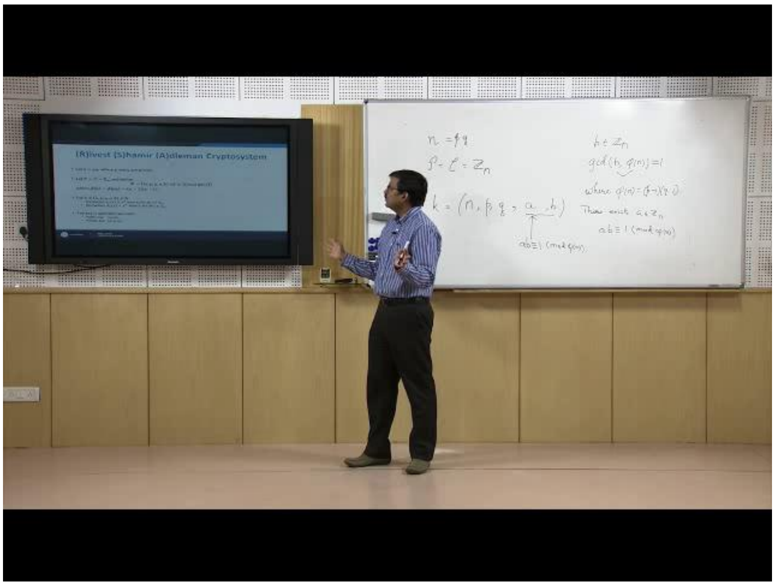


(R)ivest (S)hamir (A)dleman Cryptosystem

- Let $n = pq$, where p and q are primes.
- Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and define $$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1(mod\ \phi(n))\},$$ where $\phi(n) = \phi(pq) = (p-1)(q-1)$.
- For $k \in (n, p, q, a, b) \in \mathcal{K}$
  - Encryption: $e_k(x) = x^b\ mod\ n$, for all $x \in \mathbb{Z}_n$;
  - Decryption: $d_k(y) = y^a\ mod\ n$, for all $y \in \mathbb{Z}_n$.
- The key is split into two parts.
  - Public key: (n, b);
  - Private key: (p, q, a).

Now, let us explain this cryptosystem stepwise. In the first step we need 2 large primes.

(Refer Slide Time: 09:52)



$n = pq$
$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
$k = (n, p, q, \underline{a}, b)$
$ab \equiv 1 \pmod{\phi(n)}$
$b \in \mathbb{Z}_n$
$\gcd(b, \phi(n)) = 1$
where $\phi(n) = (p-1)(q-1)$
There exist $a \in \mathbb{Z}_n$
$ab \equiv 1 \pmod{\phi(n)}$

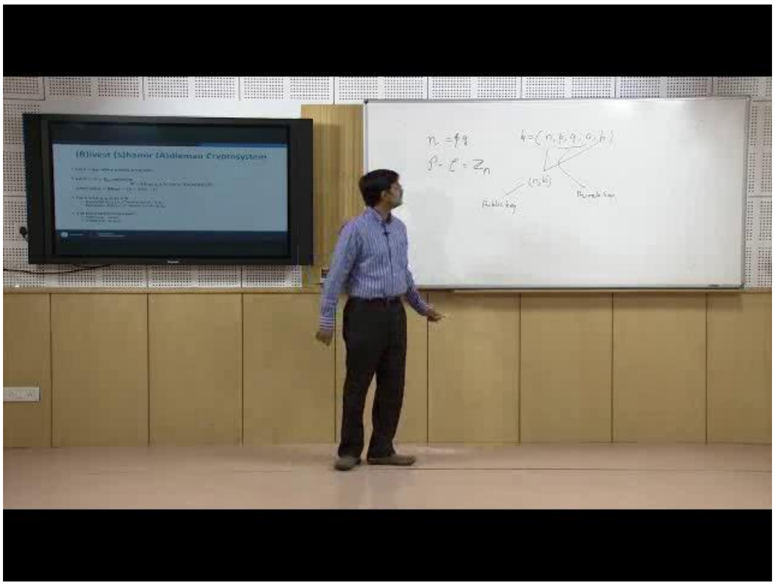
So, let us call the primes p and q and then we will take the product of these 2 primes and we will get a number which is n. So, that is what I have written in the first line and now of course, we are talking about crypto systems. So, the question is what is the set of plain text? What is the set of cipher text? And what is the set of keys? The set of plain text, script p and the set of cipher text, script c both are same and equal to z, sub n that is the integers modulo n.

So, we have p, we have c which is equal to z sub n, where n is equal to p and q and now we come to keys. Now, interestingly here the key consists of n which is a product of 2 primes and the primes themselves. So, a single key for this cipher will consist of this n and the primes which make up this key make up this n and after that there are some other numbers. So, one number is b and b is chosen at random from z's of n with the property that GCD of b and phi n is equal to 1, where phi n is equal to p minus 1 into q minus 1.

Just little afterwards, we will be talking about 5 more details and we will say that what really phi n is, but right now we are not doing that. So, just remember that phi n is p minus 1 into q minus 1 and then we also know from our previous lectures that on modular arithmetic that, if b is co prime to phi n that is GCD is 1 then is possible to find a that is there exist a belonging to z sub n such that a times b is congruent to 1 modulo phi n and this is the last component of the key.

So, they together have to follow this condition a into b is 1 mod phi n. We will look at the computational issue soon, not now. Let us say we can do this now. So, once we have this key, this key is split up into 2 parts; one part is called the private key the other part is called public key. Now, let us remove some of the writings from the board and write the key at a top. So, I have a key.

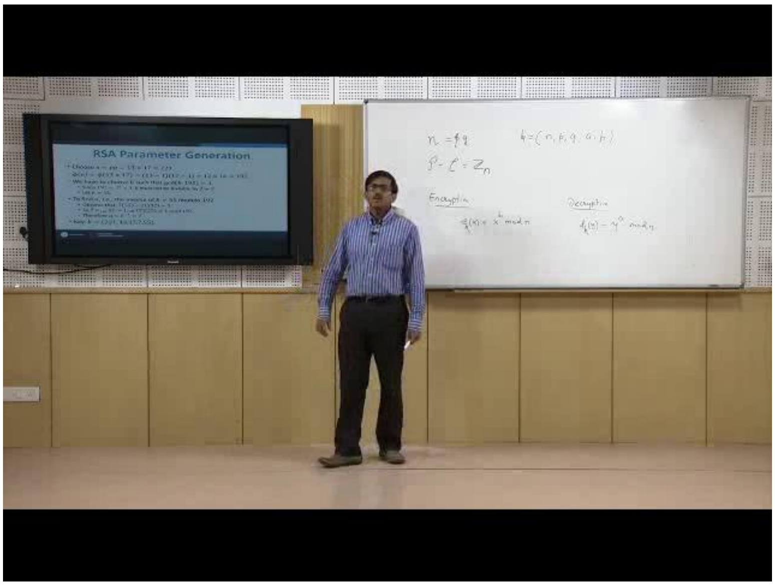
(Refer Slide Time: 14:11)



Like this it is a total key. So, this is n, p, q, a and b and these 2 elements make up the public key and the rest p, q and a make up the private key. What is claimed and what has not been disproved so far is that if someone knows n and b, and if p and q are very large primes possibly having a representation of more than 600 bits long then knowing n and b does not let anyone to compute the factorization and hence the inverse modulo phi n in a f e with a infeasible time in reasonable time.

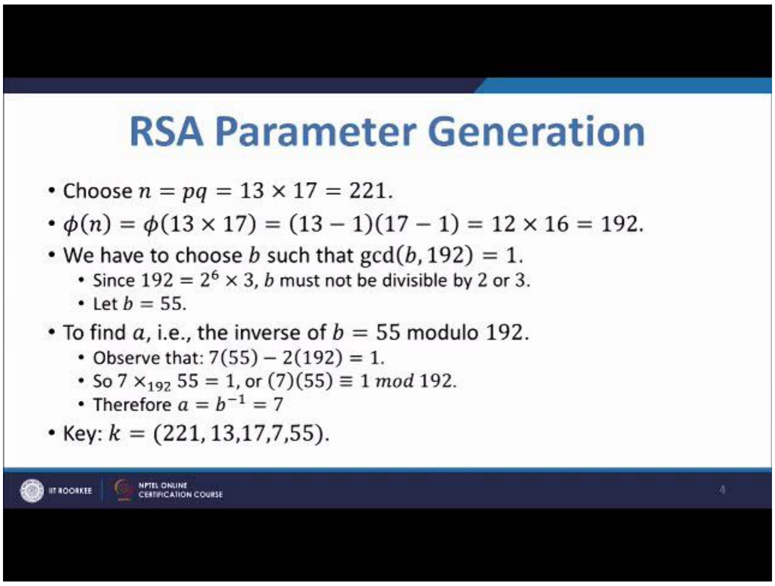
So, it is computationally infeasible for anyone to compute a given b and n without the knowledge of p, q or phi n. So, this is something a claim on which RSA to system rests and the security of RSA crypto system depends and nobody has been able to disprove this claim. So, now we come to the encryption and decryption of RSA, the encryption of RSA is done by using the public key, which is n and b.

(Refer Slide Time: 16:57)



So, the encryption function e, k, x is equal to x to power b mod n and the decryption function is d, k, y is equal to y raise to the power a mod n. Now, let us look at a small example of RSA of course, in practice it is not secure at which. So, small parameters but let us check that what happens. So, what we are going to do now is to choose p and q as particular primes. So, suppose p is 13 and q is 17, both are primes and therefore let me modify my writings here.

(Refer Slide Time: 18:39)



RSA Parameter Generation

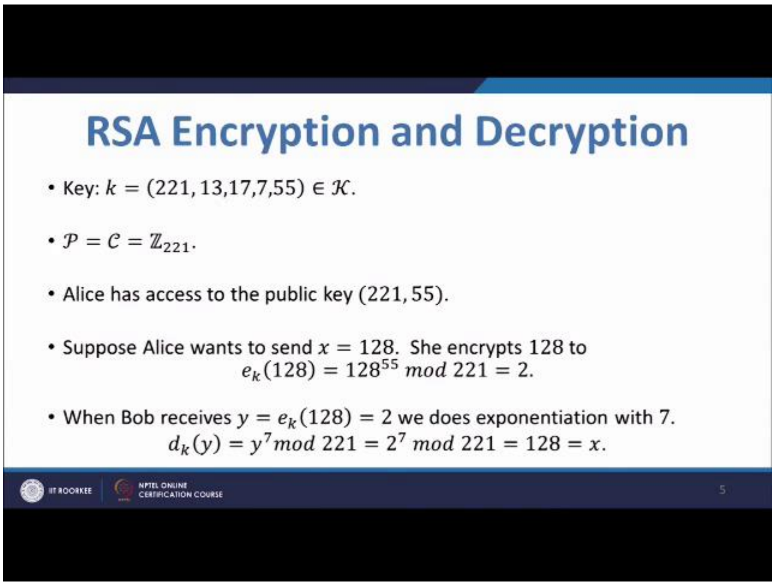
- Choose $n = pq = 13 \times 17 = 221$.
- $\phi(n) = \phi(13 \times 17) = (13 - 1)(17 - 1) = 12 \times 16 = 192$.
- We have to choose b such that $\gcd(b, 192) = 1$.
  - Since $192 = 2^6 \times 3$, b must not be divisible by 2 or 3.
  - Let $b = 55$.
- To find a, i.e., the inverse of $b = 55$ modulo 192.
  - Observe that: $7(55) - 2(192) = 1$.
  - So $7 \times_{192} 55 = 1$, or $(7)(55) \equiv 1 \ mod \ 192$.
  - Therefore $a = b^{-1} = 7$
- Key: $k = (221, 13,17,7,55)$.

IIT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE 4

So, p is 13 and q is 17 and therefore, the product is 221 and phi n is equal to 13 minus 1 17 minus 1 and if it is equal to 192, we can check this and now we have to choose b which is co prime to 192 a note of question b is co prime to phi n and not n. So, if we choose b, in that way b equal to 55 will work and once we have b equal to 55, we can essentially use the technique that we have discussed again in our previous lectures from big one onward that I can compute a inverse of p modulo 192 and for that I do not have to do such thing I can use Euclidean algorithm in back and forth and get the inverse. I have discussed that and in this case this inverse is going to be 7.

So, we can check that 7 into 55 are equal to 1 or congruent to 1 mod 192. We have this and now we have a set up over here and so we know that b is phi and if b is phi, a is going to be 7 and therefore, we have the key that is going to be as you see here 221, 13, 17, 7 and 55. So, this is RSA parameter generation and once we have generated the parameter we can do the encryption. So, for that let us take an example of a plain text. We have told that plain text is z's up to 21. So, plain text in this case can be any number from 0 to 220. So, we choose a number 128.

(Refer Slide Time: 21:25)



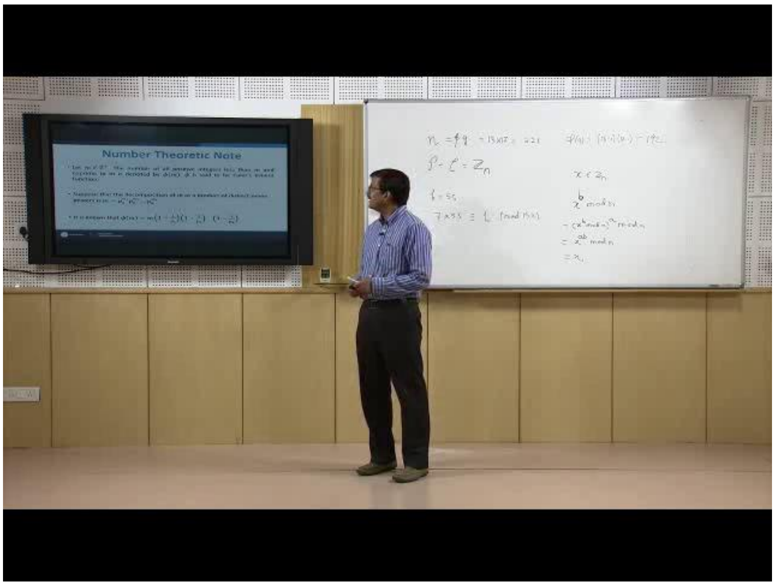
RSA Encryption and Decryption

- Key: $k = (221, 13, 17, 7, 55) \in \mathcal{K}$.
- $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{221}$.
- Alice has access to the public key $(221, 55)$.
- Suppose Alice wants to send $x = 128$. She encrypts 128 to
  $$e_k(128) = 128^{55} \, mod \; 221 = 2.$$
- When Bob receives $y = e_k(128) = 2$ we does exponentiation with 7.
  $$d_k(y) = y^7 mod \; 221 = 2^7 \; mod \; 221 = 128 = x.$$

I am deliberately choosing 128 because I want to show that it need not be this, the number that we choose need not be co prime to n and it is something different what I want to just show is that the number that we choose, it need not be co prime to phi n. It can be any number, if we take any number in z sub to 221. So, in this case x equal to 128 and we raise it to the power 55 and then we will see we can do it by calculator so far. So, will see that modular 21 is going to be 2.

So, that is my encrypted value and if on the other hand we take the encrypted value and raise it to the power a then reduce modular 221, it is trivial to check that we are going to a at 128 because 2 raise to the power 7 is 128. So, at least for 1 instance we see that the encryption and decryption works. Now, we have a question that will encryption and decryption for RSA work for all instances for that we have to show that given any x inside z 7.

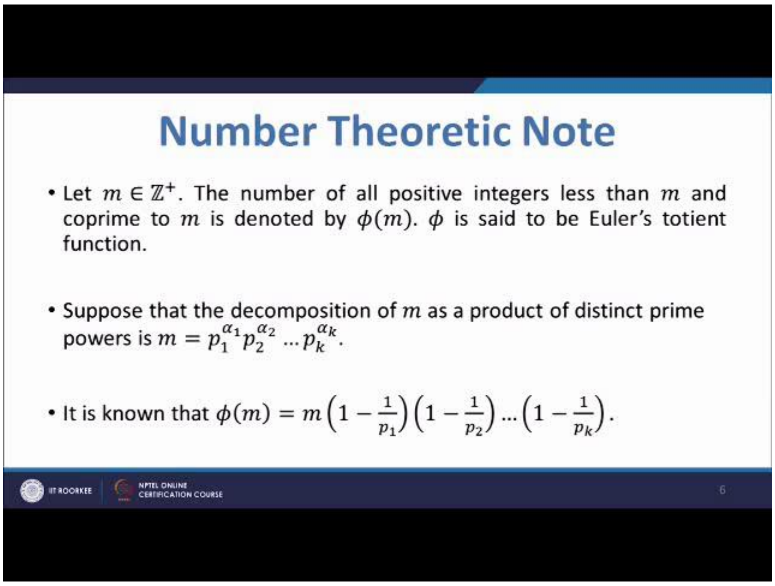
(Refer Slide Time: 23:11)



If I raise it to the power a, I am sorry, first raise it to the power b and I take mod n all right and then I raise it to the power a x to the power b mod n, raise it to the power a then again take mod n. This is going to be x to the power a into b mod n and I want to show that it is equal to x always I have to show we need to show this to show that the RSA is indeed valid cryptosystem of course, it is a valid cryptosystem, in order to prove that we have to know little more about phi n.

Now, phi n essentially is a number of positive integers starting from 1 to m minus 1 which are co prime to m. So, we have written the definition of phi n at the first point and then the question occurs, how to compute phi n? At this point, we cannot discuss the details of the proof of the expression for phi n, but it is not difficult to remember. We will remember that phi n is equal to m times 1 minus 1 by p 1 into 1 minus 1 by p 2 and so on up to 1 minus 1 by p n, where pi's are the prime factors of m.

(Refer Slide Time: 25:02)



Number Theoretic Note

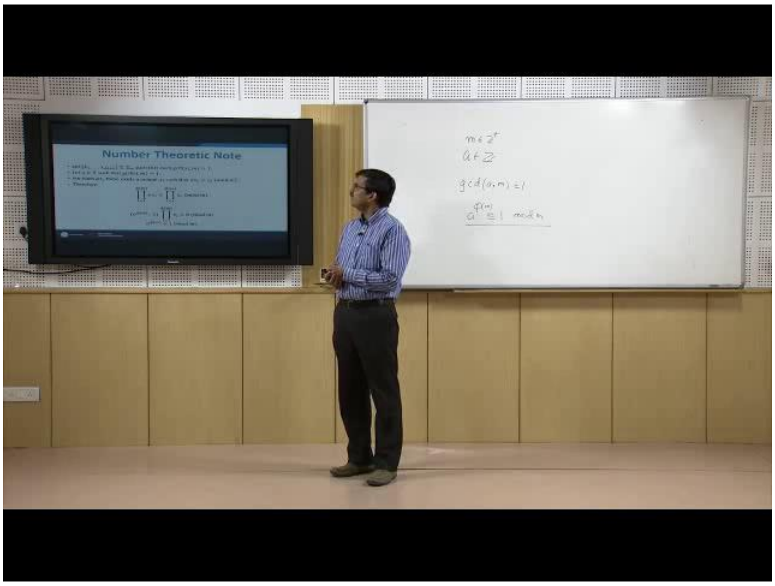
- Let $m \in \mathbb{Z}^+$. The number of all positive integers less than m and coprime to m is denoted by $\phi(m)$. ϕ is said to be Euler's totient function.
- Suppose that the decomposition of m as a product of distinct prime powers is $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
- It is known that $\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$.

IIT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

6

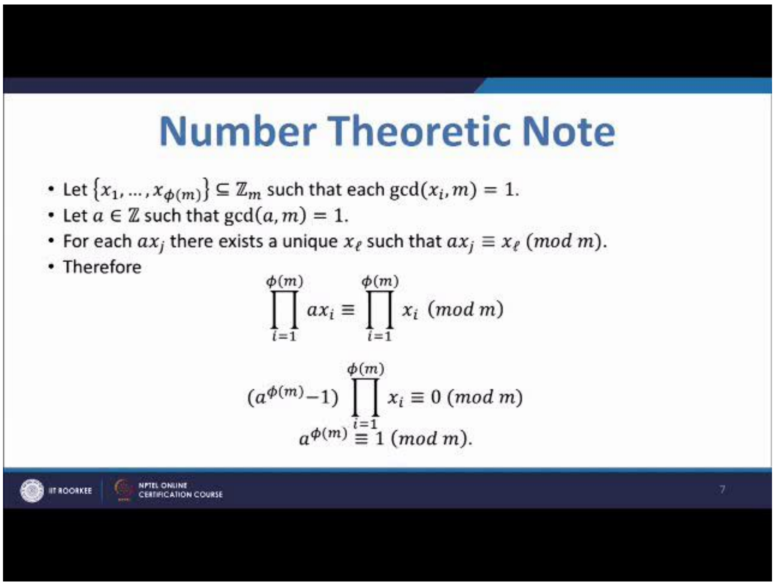
Once we remember this, we move forward, we come over here eventually what we would like to prove here and that is what we have to remember is this let me write it down separately.

(Refer Slide Time: 25:20)



Give me any number, any integer such that the greatest common divisor of a and m, where m is a positive integer. This should be 1 then a raise to the power phi m is congruent to 1 mod m. Now, this a general rule, I have written outline of the prove here to go through the outline it is mainly like this that I can list down all the positive integers in z m, which are co-prime to m like this x 1 up to x m.

(Refer Slide Time: 26:38)



Number Theoretic Note

- Let $\{x_1, \ldots, x_{\phi(m)}\} \subseteq \mathbb{Z}_m$ such that each $\gcd(x_i, m) = 1$.
- Let $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$.
- For each ax_j there exists a unique x_ℓ such that $ax_j \equiv x_\ell \ (mod\ m)$.
- Therefore

$$\prod_{i=1}^{\phi(m)} ax_i \equiv \prod_{i=1}^{\phi(m)} x_i \ (mod\ m)$$

$$(a^{\phi(m)}-1) \prod_{i=1}^{\phi(m)} x_i \equiv 0 \ (mod\ m)$$

$$a^{\phi(m)} \equiv 1 \ (mod\ m).$$

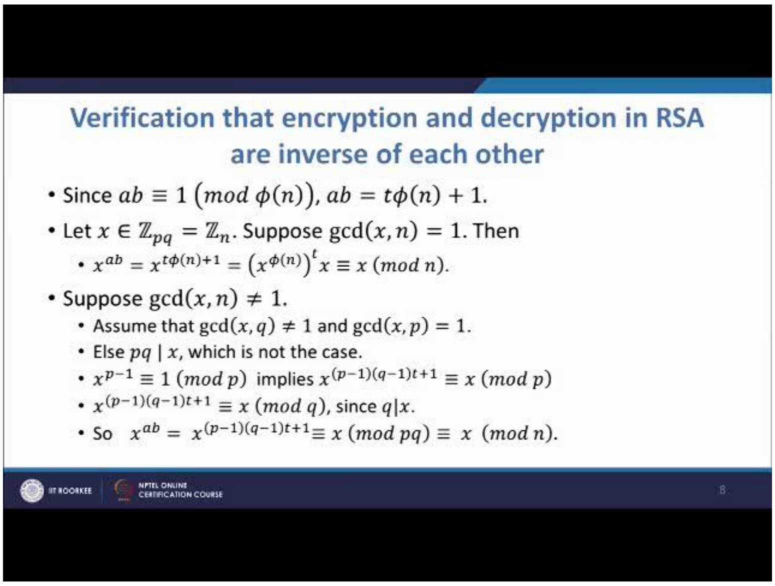
IIT ROORKEE NPTEL ONLINE CERTIFICATION COURSE 7

Then if I take an integer co prime to m and multiply all this x is by that integer a and then reduce modular m, then I will be getting all the distinct xi's 1 by 1 in certain order. So, essentially is not difficult to see that we will be getting all of them, all the distinct one, even if we multiply them by a and reduce modulo m. We do that and since a and all the xi's are eventually co prime to m. If I take the product they are going to be equal modular m, if I do after that, the left hand side can be transport to the right hand side and a raise to the power phi m minus 1 factor out.

We have a raise to the power phi m minus 1 in one side product with the product of all xi's and that is going to be 0 mod m and we are started with the assumption that xi's are co prime to m. So, their product is not going to be divisible by m therefore, a raise to the power phi m minus 1 is going to be divisible by m and therefore, we have this ultimate thing and we are not to forget this m.

Now, particularly this is a special case, if m is equal to p a prime when a raise to the power p minus 1 is congruent to 1 mod p because phi p is equal to 1 minus is equal to p minus 1 if p is a prime. So, we have this, now we are in position to verify the invertability of encryption and decryption function of RSA. So, we have come over here. In the first line, let us see that a, b are inverse of each other modulo phi n. So, I can write a b equal to t times phi n plus 1 and then I choose x inside z sub n or z's of p q such that in the beginning x is co prime to n.

(Refer Slide Time: 29:27)



Verification that encryption and decryption in RSA are inverse of each other

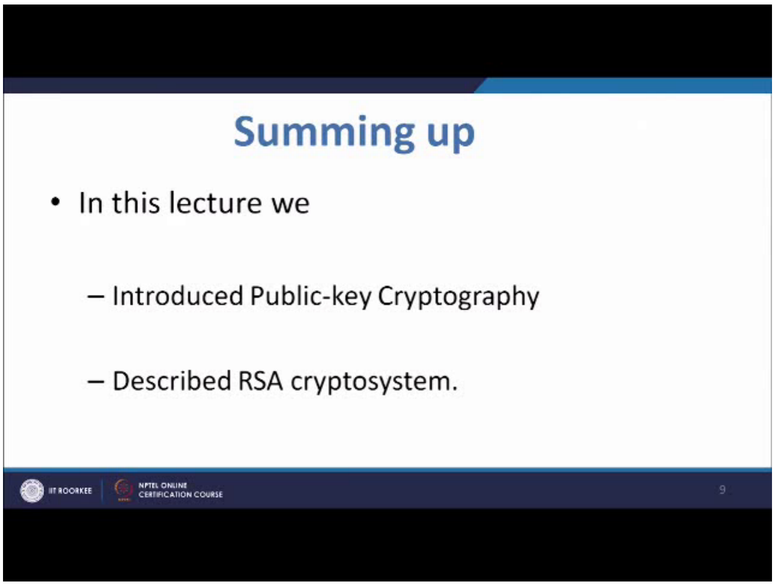
- Since $ab \equiv 1 \left(mod\ \phi(n)\right)$, $ab = t\phi(n) + 1$.
- Let $x \in \mathbb{Z}_{pq} = \mathbb{Z}_n$. Suppose $\gcd(x, n) = 1$. Then
  - $x^{ab} = x^{t\phi(n)+1} = \left(x^{\phi(n)}\right)^t x \equiv x\ (mod\ n)$.
- Suppose $\gcd(x, n) \neq 1$.
  - Assume that $\gcd(x, q) \neq 1$ and $\gcd(x, p) = 1$.
  - Else $pq \mid x$, which is not the case.
  - $x^{p-1} \equiv 1\ (mod\ p)$ implies $x^{(p-1)(q-1)t+1} \equiv x\ (mod\ p)$
  - $x^{(p-1)(q-1)t+1} \equiv x\ (mod\ q)$, since $q|x$.
  - So $x^{ab} = x^{(p-1)(q-1)t+1} \equiv x\ (mod\ pq) \equiv x\ (mod\ n)$.

Now, if x is co prime to n then we know that x raise to the power a b is equal to x raise to the power t times phi n plus 1 is equal to x raise to the power phi n raise to the power t into x. Now, since x is co prime to n x raise to the power phi n is going to be equal to 1 mod n and therefore, this portion is 1 and then I will going to get x mod n. So, at least if x is co prime to n we have proved that the encryption and decryption are inverse of each other, we have the last portion here, suppose x is not co-prime to n then what is going to happen?

Now, it is not difficult to see that since x is between 1 and p, p q minus 1 x cannot be divisible by both p and q. So, either x is divisible by p or x is divisible by q. We assume that x is divisible by q and not divisible by p and q is prime therefore, greatest common divisor of x and q not equal to 1 and x divisible by q they are same things. So, we have got this and x is not divisible by p, since x is not divisible by p, we know that x raise to the power p minus 1 is congruent to 1 mod p which implies that x raise to the power p minus 1 into q minus 1 into t plus 1 is congruent to x mod p, and well once I have here we have already assume that x is divisible by q and therefore, both these sides are divisible by q therefore, I can I have got this condition free of cost.

So, I have got x raise to the power p minus 1 into q minus 1 into t plus 1 is congruent to x mod q and now, we have a scenario where p divides something minus x and q divides something minus x the same thing and p q are primes, therefore, p q divides that, therefore, we can ultimately write that x to the power a b, which is equal to x to the power p minus 1 into q minus 1 into t plus 1 is congruent to x mod p q, which is equal to x mod n. So, this verifies the RSA algorithm.

(Refer Slide Time: 32:44)



Summing up

- In this lecture we
  - Introduced Public-key Cryptography
  - Described RSA cryptosystem.

IIT ROORKEE | NPTEL ONLINE CERTIFICATION COURSE

9

So, we can sum up. Now, we have introduced the idea of public key cryptography, public key cryptosystems and we have described the RSA algorithm. So, that is end of today’s lecture.

Thank you.