

**Foundations of Cryptography**  
**Dr. Ashish Choudhury**  
**Department of Computer Science**  
**Indian Institute of Science– Bangalore**

**Lecture – 46**  
**RSA Public Key Cryptosystem**

Hello everyone. Welcome to this lecture.

**(Refer Slide Time: 00:34)**



**Roadmap**

- ❑ Generic construction of a public-key cryptosystem from any one-way trapdoor permutation
- ❑ Plain (textbook) RSA public-key cryptosystem
  - ❖ Attacks on plain RSA public-key cryptosystem
- ❑ COA(CPA)-secure RSA public-key cryptosystem
- ❑ RSA cryptosystem implementation issues



Just to recap in the last lecture, we had introduced the RSA assumption. So, we will continue our discussion with RSA assumption, specifically the road map for this lecture is as follows. We will see a generic construction of a public-key cryptosystem from any given One-Way Trapdoor Permutation. We will see how we can instantiate this framework whereby using the RSA Trapdoor Permutation to get the RSA public-key cryptosystem, which we also call as the plain RSA public-key cryptosystem. We will see several attacks on the plain RSA public-key cryptosystem. Then, we will see the COA or CPA-secure variant of RSA public-key cryptosystem.

**(Refer Slide Time: 01:18)**

## Public-key Cryptosystem from Any OWTP

<p>□ Given: A OWTP scheme <math>T = (Gen, f, Inv)</math> over <math>\mathcal{X}</math>:</p> <ul style="list-style-type: none"> <li>❖ <math>Gen() \rightarrow (pk, sk)</math> <ul style="list-style-type: none"> <li>➤ <math>pk</math>: public key</li> <li>➤ <math>sk</math>: secret key</li> </ul> </li> <li>❖ <math>f_{pk}: \mathcal{X} \rightarrow \mathcal{X}</math> <ul style="list-style-type: none"> <li>➤ <math>f_{pk}(x) = y</math></li> <li>➤ Deterministic algorithm</li> </ul> </li> <li>❖ <math>Inv_{sk}: \mathcal{X} \rightarrow \mathcal{X}</math> <ul style="list-style-type: none"> <li>➤ <math>Inv_{sk}(y) = x</math></li> <li>➤ Deterministic algorithm</li> </ul> </li> </ul> <p>□ Correctness: for every <math>(pk, sk)</math> and <math>x \in \mathcal{X}</math>:</p> $Inv_{sk}(f_{pk}(x)) = x$ <p>□ One-Wayness: <math>f_{pk}</math> is a OWF, even if an adversary knows the public key <math>pk</math></p>	<p>□ Goal: to construct a public-key cipher <math>\Pi = (KeyGen, Enc, Dec)</math> from <math>T</math> over the plaintext space <math>\mathcal{M} = \mathcal{X}</math></p> <ul style="list-style-type: none"> <li>❖ Algorithm <math>KeyGen(n)</math> <ul style="list-style-type: none"> <li>➤ <math>Gen() \rightarrow (pk, sk)</math></li> <li>➤ Set <math>pk</math> as the encryption key and <math>sk</math> as the decryption key</li> </ul> </li> <li>❖ Algorithm <math>Enc(pk, m): m \in \mathcal{X}</math> <ul style="list-style-type: none"> <li>➤ Compute <math>f_{pk}(m) = y</math></li> <li>➤ Output <math>y</math> as the ciphertext</li> </ul> </li> <li>❖ Algorithm <math>Dec(sk, c)</math> <ul style="list-style-type: none"> <li>➤ Compute <math>Inv_{sk}(c) = x</math></li> <li>➤ Output <math>x</math> as the plaintext</li> </ul> </li> </ul>
---	--

Finally, we will end the lecture with some implementation issues which we face when we implement RSA in practice. So, let us begin our discussion with a generic framework regarding how we construct a Public-Key Cryptosystem from any One-Way Trapdoor Permutation. So, just to recall what is a One-Way Trapdoor Permutation scheme is. It is a collection of 3 algorithms.

We have a Parameter Generation algorithm, which outputs a public parameter and a secret parameter, which you can call as public key and secret key, then the function  $f$  is a two input function. It takes the public key  $pk$ , and the input from the domain fancy  $X$  and it gives you an output from the set fancy  $X$  and it is always a Deterministic algorithm. On the other hand, an inverse function, it is said to input a function taking the secret key  $sk$ , and input from the co-domain, which you want to invert, and it gives you an output from the domain of the function  $f$ .

And also this is a Deterministic algorithm. We need two properties from any One-Way Trapdoor Permutation Scheme. The first property is the Correctness property, which requires that for every pair of keys output by the Parameter Generation algorithm and for every input  $x$ , if you compute the value of  $f(x)$ , and then you compute the inverse of that function with respect to the secret key  $sk$ , then you should get back the output  $x$ .

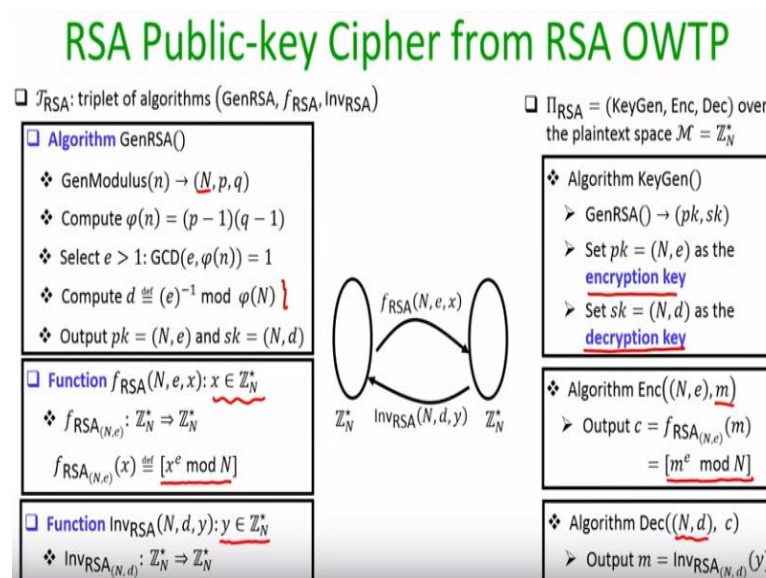
The second property which is the Security property is the one when its requirement. It demands that your function  $f$  sub  $pk$  should be a one-way function against a computationally-bounded adversary even if the adversary knows the description of the public key and steps of

your function  $f$ . Now, given such One-Way Trapdoor Permutation Scheme, our goal is to construct a Public-Key Cryptosystem, which has a Key Generation algorithm, encryption algorithm, and decryption algorithm over the plaintext space, namely the set fancy  $X$ , and this is done as follows.

So the Key Generation algorithm of your encryption process will be basically to run the Parameter Generation algorithm of your Trapdoor Permutation Scheme and obtain the public key and secret key  $pk, sk$ , and we set the  $pk$  as the encryption key, and we set  $sk$  as the decryption key. To encrypt a plain text  $m$  with respect to the public key  $pk$ , what we do is, we just compute the value of the function  $f$  with the key  $pk$  on the input  $m$ .

So, sorry for the typo here. This  $x$  should be  $m$  because we want to encrypt the plain text  $m$ . So this is a typo here, so if we want to encrypt a plain text  $m$ , then we evaluate the value of the function  $f$  using  $pk$  as the public key on the input  $m$ , and the resultant output, which I denote as  $y$  is considered as the cipher text. On the other hand, if we want to decrypt a cipher text using a secret key  $sk$ , then what we have to do is, we have to call the inverse function of the Trapdoor Permutation Scheme on the input  $c$  using the secret key  $sk$  to recover back the plaintext  $x$ .

(Refer Slide Time: 04:24)



So, let us instantiate this framework using the RSA One-Way Trapdoor Permutation. So, remember in the last lecture, we have seen that RSA Permutation can be considered as a One-Way Trapdoor Permutation Scheme and the details of the RSA Trapdoor Permutation Scheme are as follows. So the Parameter Generation algorithm for the RSA Trapdoor

Permutation is as follows. It runs the GenModulus algorithm and outputs primes  $p$  and  $q$  of size  $m$ -bits and modulus  $N$ , where  $N$  is the product of  $p$  and  $q$ .

Then it computes the value of  $\phi(N)$ , namely the size of the set  $\mathbb{Z}_N^*$  where  $\phi(N)$  will be the product of  $p-1 \times q-1$ . Then it selects  $e$ , which is greater than 1 such that  $e$  is co-prime to  $\phi(N)$  and since  $e$  is co-prime to  $\phi(N)$ , we can compute the multiplicative inverse of  $e$  modulo  $\phi(N)$ , which we denote as  $d$  and once we compute all these values, then the public key  $pk$  is said to be  $N, e$  whereas the secret key  $sk$  is said to be  $N, d$ .

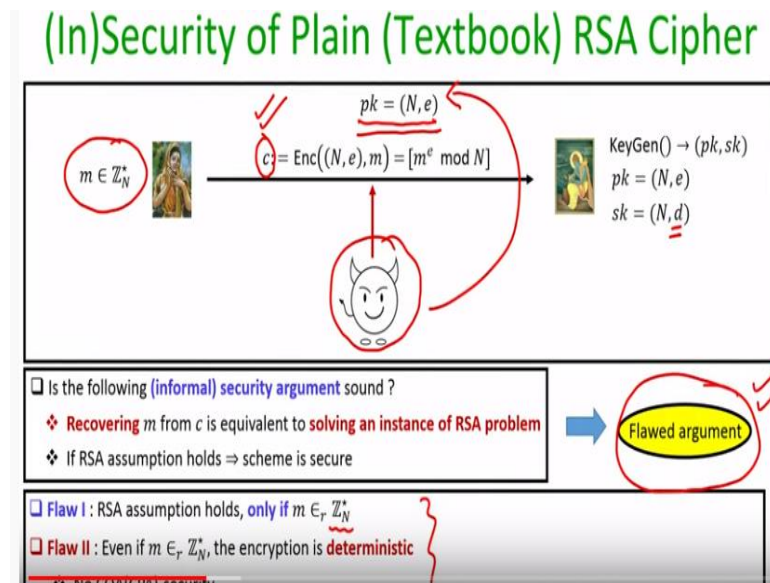
The RSA function, which takes an input  $x$  from the set  $\mathbb{Z}_N^*$  is computed as follows. To evaluate the values of the RSA function, using the public key  $N, e$ , we basically compute our output  $x$  to the power  $e$  modulo  $N$ , and  $x$  to the power  $e$  modulo  $N$  will also be an element of  $\mathbb{Z}_N^*$ . On the other hand, if you want to invert the RSA function on some input  $y$  belonging to  $\mathbb{Z}_N^*$  using the secret keys  $N, d$ , then we basically output  $y$  to the power  $d$  modulo  $N$ .

So, that is what is the RSA One-Way Trapdoor Permutation Scheme assuming the RSA problem is difficult to solve with respect to the GenRSA function, then we have proved, we had seen in the last lecture that we can use this RSA Trapdoor Permutation as a candidate One-Way Trapdoor Permutation. Let us instantiate the framework that we had seen in the last slide by using the RSA Trapdoor Permutations.

So we get what we call as RSA Public-Key Cryptosystem over the plaintext space  $\mathbb{Z}_N^*$ . So, the Key Generation algorithm for the RSA Public-Key Cryptosystem is  $UV \lambda$  GenRSA algorithm of the RSA Trapdoor Permutation, and we set  $N, e$  to be the encryption key and we set  $N, d$  as the decryption key. So the receiver will know  $N$  and  $d$  to decrypt a cipher text whereas the public key  $N, e$  will be available in the public domain.

If there is a sender, which wants to encrypt a plaintext  $m$  using the public key  $N, e$  then it has to basically compute the RSA function on the input  $m$ , which is nothing but the computing the value of  $m$  to the power  $e$  modulo  $N$ . On the other hand, if a receiver receives cipher text  $c$ , then using the secret key  $N, d$ , it can decrypt a cipher text  $c$ , it has to basically compute the inverse RSA function and output  $y$  to the power  $d$  modulo  $N$ . So, the correctness of this RSA cryptosystem follows from the correctness of the generic framework that we have discussed in the last slide.

(Refer Slide Time: 07:33)



Now, let us focus on the security of the RSA cipher that we have just constructed and imagine that we have a receiver, which runs the Key Generation algorithm of the RSA cipher that we have discussed, obtains the public parameter  $N, e$  and a secret parameters  $N, d$ , and it makes its public key  $N, e$  available in the public domain, and say there is a sender, which has a plain text  $m$  belonging to  $\mathbb{Z}_N^*$ .

Which it wants to communicate to the receiver, then as per the syntax of the RSA Encryption Scheme, it computes a cipher text, which is  $m$  to the power  $e$  modulo  $N$  and cipher text is communicated to the receiver and assume we have a polytime or computationally bounded  $(\mathcal{A})$  (08:17) the cipher text. Now, one might be wondering that whether the following security argument is sound or not.

We can say that if there is an adversary who has  $(\mathcal{A})$  (08:29) the cipher text  $c$  and its goal is to recover the underlying plain text  $m$ , which is encrypted in  $c$ , then basically it has to solve an instance of RSA problem because this adversary only knows that description of  $N, e$  and he does not know the underlying  $m$ , and he does not know the secret key  $d$ . So, recovering  $m$  from  $c$  is equivalent to solving an instance of RSA problem.

And hence if you assume that the RSA assumption holds with respect to the GenRSA algorithm that the receiver has run, then we can argue that this scheme should be secured, but it turns out that this informal argument is completely flawed here. There is intuition that

recovering the underlying plain text from the cipher text is equivalent to solving an instance of RSA problem is completely a flawed argument and there are many reasons for doing that.

There are many reasons behind this flaw. The first major flaw is that if you look closely into the RSA assumption, it holds only if the underlying  $m$ , which is encrypted in  $c$ , is uniformly randomly chosen from the set  $\mathbb{Z}_N^*$ , which may not be the case in practice. In practice, sender might have any kind of plaintext belonging to  $\mathbb{Z}_N^*$ , which might be encrypting and producing the cipher text  $c$  whereas for RSA assumption, we need that underlying  $m$  should be a random element from the  $\mathbb{Z}_N^*$ .


The second flaw here is that, even if you assume for the moment that sender is encrypting messages, which are random elements from the set  $\mathbb{Z}_N^*$ , and hence the RSA assumption hold, the whole encryption process that the sender is using now is deterministic. There is no internal randomness, which is there as part of the encryption algorithm. That means, if the same sender wants to encrypt the same message  $m$  multiple times using the same public key  $N, e$ .

Then it will end up getting the same cipher text  $c$  and throughout this course, we have regressively analyzed that how unsafe it is to use a deterministic encryption process. We can never hope that an encryption process can be CPA-secure if we are using the Deterministic Encryption process. These are the two security flaws, which are there with the so called RSA cipher that we have designed.

(Refer Slide Time: 10:51)


## More Attacks on Plain RSA Cipher


$pk = (N, e)$



$m \in \mathbb{Z}_N^*$

$c := [m^e \bmod N]$





KeyGen()  $\rightarrow (pk, sk)$

$pk = (N, e)$

$sk = (N, d)$

Assume we use plain RSA cipher for encrypting random messages from  $\mathbb{Z}_N^*$  (thus RSA assumption holds) and we aim to not achieve indistinguishability-based (semantic) security

Encrypting short messages using small encryption-exponent  $e$

- ❖ Several practical instantiations of RSA cipher set  $e = 3$ , to ensure that encryption process is fast
- ❖ Consider an application where  $m \in \mathbb{Z}_N^*$ , but  $m < N^{1/e}$ 
  - Hybrid RSA encryption:  $\|N\| \approx 1024$  bits,  $e = 3$  and  $m \in_r \{0, 1\}^{300}$
- ❖  $c := [m^e \bmod N] = m^3$  --- integer cube and not modulo  $N$  cube

It turns out that apart from this short coming that your RSA encryption process is deterministic, we can show several attacks on the Plain RSA Cipher, so assume for the moment, we are using the RSA Cipher where the sender wants to encrypt random messages from  $\mathbb{Z}_N^*$ , and we do not want a semantic security, namely, we do not aim for indistinguishability-based security. It suffice for us if adversary does not learn the entire plaintext by  $(C)$  (11:25) upon the cipher text.

That is a notion of secrecy that we are aiming for right now, but for the moment assume that. It turns out even if we go for this weaker notion of secrecy, namely all or nothing kind of secrecy, then there are several attacks which can be still launched on the Plain RSA Cipher. So, the first class of attacks is basically what we call as encrypting short messages using small encryption-exponent  $e$ .

So, it turns out that for many practical instantiation of RSA, we set the public exponent or the encryption exponent  $e$  to be 3 to ensure that our encryption process is fast because if you see the encryption, encryption is basically compute the  $e$ th power of plaintext modulo  $N$ , and if I set  $e$  to be 3, then my encryption process will be very fast. It is fine that if I set  $e$  to be 3, then my  $d$  will be very large and my decryption process running time will be slow.

But we can have some kind of tradeoff and for most of the many practical instantiation, this is a common choice, which is used to make the encryption process fast. Now, assume we are using an instantiation of RSA, where we have set  $e$  to be 3, and say we are consider an application where the underlying messages are random elements from  $\mathbb{Z}_N^*$ , but the magnitude of  $m$  is strictly less than the  $e$ th root of the modulus  $N$ .

And if you are wondering that what kind of applications encounters such kind of  $m$ , if later on we will see the Hybrid RSA encryption. Then the size of the modulus that we typically use is of size 1024 bits, and the message that we would like to encrypt to the Hybrid RSA encryption will be roughly a 300-bit uniformly random bit string and we will set  $e$  to be 3. If that is the case, then the cipher text will be  $m^3$  modulo  $N$ .

But since my magnitude of  $m$  is strictly less than the cube root of  $m$ ,  $m$  to the power  $e$  or  $m$  to the power 3 modulo  $N$  will be equivalent to the integer cube and the effect of mod  $N$  will not take place at all and if adversary is aware of the fact that we are using an application with

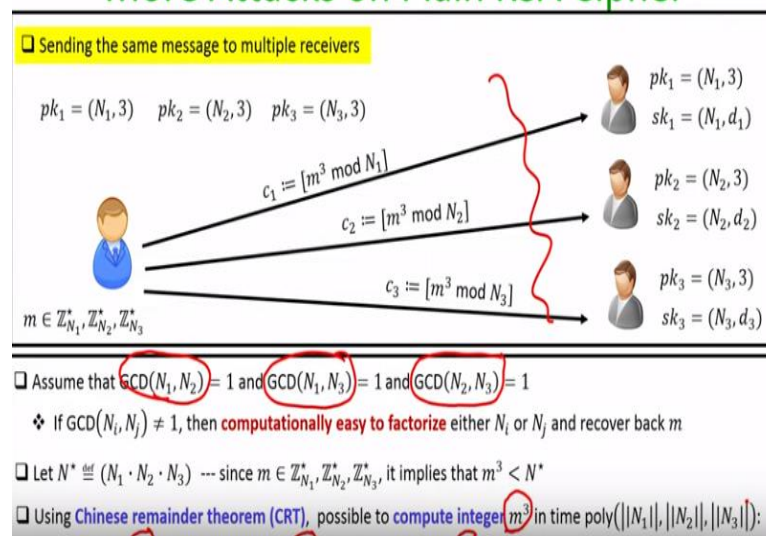


underlying plain text, its magnitude is strictly less than the cube root of modulus  $N$ , then it also will be aware that the underlying  $m$ , which has been encrypted.

Its cube is actually contained in the cipher text  $c$ , namely the integer cube not the modulo cube, and it is very easy to recover the underlying unknown  $m$  from the  $c$  by just finding the integer cube root of the cipher text  $c$ , which can be computed in poly of the size of modulus  $N$  amount of computation.

(Refer Slide Time: 14:14)

## More Attacks on Plain RSA Cipher



So that is our first class of attack, and we can have many other kinds of attack possible on Plain RSA Cipher, so imagine for the moment that we are considering an application where the same message needs to be encrypted and sent to multiple receivers. So, imagine if we say we have 3 receivers, receiver 1, 2, and 3 each of it has his own modulus  $N_1$ ,  $N_2$ , and  $N_3$  respectively.

But each of them is using a same public exponent say 3, and of course a different decryption exponent  $d_1$ ,  $d_2$ , and  $d_3$  where  $d_1$  is the multiplicative inverse of 3 modulo  $N_1$ ,  $d_2$  is the multiplicative inverse of 3 modulo  $N_2$  and so on. So, the public key, which is available in the public domain are the respective public keys of the 3 receivers and imagine that we have a sender, which has a random message belonging to  $\mathbb{Z}_{N_1}^*$ , as well as  $\mathbb{Z}_{N_2}^*$ , as well as  $\mathbb{Z}_{N_3}^*$  randomly chosen and say it wants to encrypt and send a same message to the 3 receivers.

So, it will compute  $C_1$ , which will be the  $m^3$  modulo  $N_1$ ,  $C_2$ , which will be  $m^3$  modulo  $N_2$  and so on. Now, assume that this modulus  $N_1$ ,  $N_2$ , and  $N_3$ , they are pair-wise prime. If not



suppose for instance, the GCD of  $N_i$  and  $N_j$  is not 1, they are not co-prime to each other, that means there exist a common factor of  $N_i$  and  $N_j$ , then using that common factor, it is computationally easy to factorize either the modulus  $N_i$  or  $N_j$  and say for instance if  $N_i$  is factorizable, and since  $E_i$  is also publicly known and if we know  $N_i$ 's factors.

We can compute the value of  $\phi(N_i)$  and once we know  $\phi(N_i)$  and  $E_i$ , we can compute the value of  $d_i$  in polynomial amount of time and if  $d_i$  is computable, then any encryption which is intended for the  $i$ th receiver can be decrypted by the adversary. So, it is safe to assume for the moment that pair wise, all the modulus  $N_1$ ,  $N_2$ , and  $N_3$ , they are co-prime to each other.

Now, let me define a bigger modulus  $N^*$ , which is the product of all the three modulus here, namely  $N_1$ ,  $N_2$ , and  $N_3$ , and since my underlying plaintext  $m$ , which is the sender has encrypted belongs to  $\mathbb{Z}_{N_1^*}$ , as well as  $\mathbb{Z}_{N_2^*}$ , as well as  $\mathbb{Z}_{N_3^*}$ , that means  $m$  is strictly less than  $N_1$ , it is strictly less than  $N_2$ , it is strictly less than  $N_3$ , that means the integer  $m_3$  will be strictly less than the bigger modulus  $N^*$  and now what I can do is since my modulus  $N_1$ ,  $N_2$  and  $N_3$ , and  $N_1$ ,  $N_3$  they are co-prime to each other.

I can invoke a very nice result from the Number Theory, which we call as the Chinese Remainder Theorem, which says that if your individual modulus  $N_1$ ,  $N_2$ , and  $N_3$  they are co-prime, then it is possible to compute the integer value  $m_3$  in polynomial amount of time, polynomial in the size of the respective modulus  $N_1$ ,  $N_2$ , and  $N_3$  such that the recovered  $m_3$  basically satisfies the system of following modular equations.

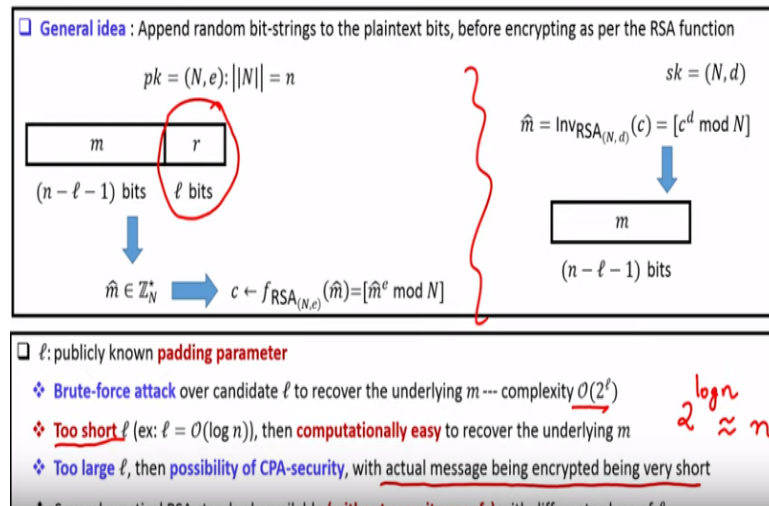
So, you are given the value  $c_1$ , which is some integer  $m_3$  modulo  $N_1$ , where  $m_3$  is not known, and you are given  $c_2$ , which is same unknown  $m_3$  modulo  $N_2$  and you are given the value of  $c_3$ , which is the same unknown  $m_3$  modulo  $N_3$ , and if your  $N_1$ ,  $N_2$ , and  $N_3$ , the respective modulus they are co-prime to each other, then what basically the Chinese Remainder Theorem says is it is possible to recover that unknown  $m_3$  in polynomial amount of computation.

Then, by applying the Chinese Remainder Theorem, an adversary who has  $(( ))$  (18:12) these three cipher text  $c_1$ ,  $c_2$ ,  $c_3$ , can apply the Chinese Remainder Theorem, and recover the unknown  $m_3$ , and once the unknown integer  $m_3$  is recovered, it can find out the exact  $m$ . So, again this is another attack, which is possible on the Plain RSA Cipher even if we assume that

a sender's message, which is a randomly chosen value from the underlying  $\mathbb{Z}_N^*$  set. It turns out that there could be several other possible attacks, which can be launched on the Plain RSA encryption process.

(Refer Slide Time: 18:48)

## Padded RSA Public-key



So, this brings us to the concept of what we call as Padded RSA public-key cryptosystem and basically the general idea here is that, we have seen already that the Plain RSA encryption process is a Deterministic Encryption process. There is no internal randomness hidden and if there is no internal randomness, then we can never hope to achieve CPS security.

So, the idea behind the Padded RSA encryption process is that we tried to append some random bit-strings to the plaintext bits, which we want to encrypt and convert everything into a group element in the set  $\mathbb{Z}_N^*$ , and then we apply the RSA function for encryption. On the other hand, the decryption end, we will chop off the random bit strings, which we have added to the plain bit strings before encryption and then that will be the recovered plaintext.

So, pictorially what we are trying to do here is the following. So, imagine that a receiver has done the public key setup. It has made its public key  $N, e$  publicly available where the size of the modulus  $N$  is little  $n$ -bits. Then, the idea here is that the Padded RSA encryption process, it will take another parameter  $\ell$  and the size of the plain text, which is Padded RSA encryption process will support will be of size  $n - \ell - 1$  bits, that means.

You can encrypt any message in the set  $0, 1$ , raise to the power  $n - \ell - 1$  bits, and the remaining  $\ell$  bits are reserved for randomness, so before encryption, imagine you have a message  $m$ , along

with that you pad little  $l$  bits of randomness, which will be uniform randomness and you will be left with 1 more bit, which we by default keep it as 0. If we do padding like that, and if we ensure that the resulted bit string, which will be of now length  $l$  bits, which we denote as  $m \text{ cap}$ , we interpret it as an element of  $\mathbb{Z}_N^*$ .

So, it might be possible that the resultant  $m$  concatenated with the randomness that we have appended, may not lead you to an element of  $\mathbb{Z}_N^*$  and if the resultant element is not an element of  $\mathbb{Z}_N^*$ , then it might look like that the RSA encryption function and RSA decryption function they need not be mutually an inverse function of each other. However, it turns out that even if the resultant  $m \text{ cap}$  is not an element of  $\mathbb{Z}_N^*$ .

But it belongs to  $\mathbb{Z}_N$ , it is suffice for us to apply the RSA function, but the encryption end and to apply the RSA decryption function at the decryption end. The Correctness property will still hold if the padded  $M$  when interpreted as a group element does not belong  $\mathbb{Z}_N^*$ , but rather belong to  $\mathbb{Z}_N$ . The Correctness property that is there with respect to the RSA forward direction function and inverse function will still hold.

We will prove that at the end of this lecture, but for the moment assume that the padded message  $N$ , which I denote by  $m \text{ cap}$  is an element of  $\mathbb{Z}_N^*$  and then once we have  $m \text{ cap}$ , we encrypt the message  $m \text{ cap}$  or the group element  $m \text{ cap}$ , we apply the RSA function, compute  $m \text{ cap}$  raise to the power  $e$  modulo  $N$ , and at the decryption end, the receiver who has the secret key  $N, d$ . It will apply that RSA inverse function, namely it will compute  $c$  to the power  $d$  modulo  $N$  and it will recover the group element  $m \text{ cap}$ .

And since it knows the value of  $l$ ,  $l$  here is a system parameter, it will be known both to the sender as well as the receiver and it will be publicly available. So, what the receiver can do is, it can parse the recovered  $m \text{ cap}$  as 0 followed by a plain text of length  $n-l-1$  bits followed by a randomness of  $l$  bits and it can simply ignore the randomness part and the remaining  $n-l-1$  bits is considered as the recovered plain text. So, as I said here,  $l$  is the publicly known public padding parameter, which is available both to the sender, receiver, and to any third party.

Now, it turns out that an adversary who is aware of the value  $l$  can launch a Brute-force attack over the amount of randomness or over the actual randomness, which has been padded

at the sender's end before encrypting the message and complexity of the Brute-force attack is basically order  $2$  to the power  $O$ ,  $2$  to the power  $l$  because there could be  $2$  to the power  $l$  number of candidate values of  $r$ , and overall those candidate randomness adversary has to perform a computation of order  $2$  to the power  $l$ .

That automatically implies that if your  $l$  is too short, that means the amount of randomness slot that is available in your version of padded RSA is too short for instance, it is of order  $\log$  of  $l$ , then it is computationally easy to recover the underlying  $m$  because a Brute-Force of the order  $2$  to the power  $\log n$  is equivalent to a computation of order  $n$ , which is polynomial in the security parameters.

So too short size of  $l$  is dangerous. On the other hand, if you reserve a huge amount of slot for the randomness, but little slot for the actual plain text, which you want to encrypt, then you can hope for a possible CPS security for the resultant instantiation of the padded CRSA, but the disadvantage will be that the actual message that we are going to encrypt, namely the actual bit string of length  $n-l-1$  will be very short.

So, we have a kind of trade-off here and it turns out that there several practical RSA standards, which are available in the literature with different values of  $l$ , but unfortunately most of them do not have any kind of security proofs. However, we will use this blue print and we will later return to the CCS-secure versions of RSA public-key cryptosystem, where we will retain this blue print and they are also the idea will be that we will take the actual plain text, which is a bit string appended with some random pad.

Then convert everything either as an element of  $\mathbb{Z}_N^*$ , or an element  $\mathbb{Z}_N$ , and encrypt it as per the RSA function, and the decryption end, we do the reverse operation. The kind of padding that we use that will ensure that we get a CCA-secure version of RSA public-key cryptosystem.

**(Refer Slide Time: 25:18)**

## Fermat's Little Theorem : RSA Message Space $\mathbb{Z}_N$

□ If  $p$  is a **prime**, then for every integer  $a$ , such that  $[a \bmod p] \neq 0$ , we have:

$$[a^{p-1} \bmod p] = 1$$

□ **Theorem:** Let  $N = p \cdot q$ , where  $p, q$  are **distinct primes** (hence  $\phi(N) = (p-1) \cdot (q-1)$ ).

Let  $e, d$  be integers, such that  $[ed \bmod \phi(N)] = 1$ . Then **for all**  $x \in \mathbb{Z}_N$ :

$$[x^{ed} \bmod N] = x \quad \approx \quad [x^{ed} - x] \text{ divisible by } N$$

❖ **Case I:** Let  $[x \bmod p] = 0$

$$[x^{ed} - x] \text{ divisible by } p$$

$x^{ed} - x$  divisible by  
distinct primes  $p, q$

❖ **Case I:** Let  $[x \bmod q] = 0$

$$[x^{ed} - x] \text{ divisible by } q$$

❖ **Case II:** Let  $[x \bmod p] \neq 0$

$$[x^{p-1} \bmod p] = 1$$

❖ **Case II:** Let  $[x \bmod q] \neq 0$

$$[x^{q-1} \bmod q] = 1$$

Finally, let me end this lecture with something related to the message space of  $\mathbb{Z}_N$  and for that let me first state a property from the well-known theorem from Number Theory, which I will not prove, which we also call as Fermat's Little Theorem, and what Fermat's Little theorem basically says that if  $p$  is a prime, then for every integer  $a$ , which is not divisible by  $p$ , namely for every integer  $a$  such that  $a \bmod p$  is not 0, then  $a$  to the power  $p-1$  modulo  $p$  is 1. This holds for every integer  $a$ , which is not divisible by the prime  $p$ .

Now, what we are going to prove using this Fermat's Little theorem is that imagine if you have a modulus  $N$ , which is the product of two distinct primes  $p$  and  $q$ , that means you are  $\phi(N)$  is nothing but the product of  $p-1$  and  $q-1$  and say you have two integers  $e, d$  such that  $e$  and  $d$  are multiplicative inverse of each other modulo  $\phi(N)$ . That means,  $ed$  modulo  $\phi(N)$  is 1.

Then what we are going to show is that for every  $x$  in the set  $\mathbb{Z}_N$ ,  $x$  to the power  $ed$  modulo  $N$  is going to give you  $x$ , equivalently this means that  $x$  to the power  $ed$  minus  $x$  is completely divisible by  $n$ . That is what we are going to prove. It is easy to that these two conditions are equivalent. If indeed,  $x$  to the power  $ed$  modulo  $N$  is  $x$ , that means, when I divide  $x$  to the power  $ed/n$ , I get the remainder  $x$ .

That means, if I subtract the remainder  $x$  from  $x$  to the power  $ed$ , then the resultant number will be completely divisible  $y$ . Before I go into the proof of this theorem, what exactly is the significance of this theorem. The significance here is the RSA function and its corresponding

inverse function will work even if I have an  $x$ , which is not a member of  $\mathbb{Z}_N^*$ , but rather a member of  $\mathbb{Z}_N$ .

That means if you go and see the padded RSA where we are padding the bit string, which we want to encrypt with a random pad and trying to interpret it as an element of  $\mathbb{Z}_N^*$ , I said that it may not be an element of  $\mathbb{Z}_N^*$ , because to be an element of  $\mathbb{Z}_N^*$ , the resultant element should be co-prime to your modulus  $N$ , but that need not be the case here. Your  $m$  cap need not be your co-prime to  $N$ , but that is fine.

This theorem says that even if you encrypt such  $m$  cap using the RSA function and try to decrypt it using the RSA function, you will get back the right  $m$  cap. Of course, remember that we have reserved the first bit in the padded RSA to be 0, which automatically ensures that  $m$  cap is definitely less than the modulus  $N$  and hence it is an element of  $\mathbb{Z}_N$ . So, let us proceed to prove this theorem.

So we take case 1, so what basically we are going to do in this proof is we are going to prove certain properties with respect to  $x$  modulo  $p$ , and symmetrically we are going to prove similar properties with respect to  $x$  modulo  $q$ , and then we will combine these two properties to arrive at the proof of this theorem. So, let us first consider case 1, where we are going to see the properties of  $x$  modulo  $p$ .

And we can have two subcases here, if  $x$  modulo  $p$  is 0, that means if  $x$  is completely divisible by  $p$ , then so is  $x$  to the power  $ed$ , and if  $x$  to the power  $ed$  is divisible by  $p$  and if  $x$  is also divisible by  $p$ , then it implies automatically that  $x$  to the power  $ed$  minus  $x$  is also divisible by  $p$ . So, that is sub case 1 and sub case 2 here is when  $x$  modulo  $p$  is not zero, that means  $x$  is not completely divisible by 0.

And in this case, I can invoke my Fermat's Little theorem, and I can say that  $x$  to the power  $p-1$  modulo  $p$  is 1, and now what I am going to do is, I am going to use the fact that  $ed$  modulo  $\phi(N)$  is 1. Remember, my  $ed$  modulo  $\phi(N)$  is 1, and also my  $\phi(N)$  is the product of  $p-1$  and  $q-1$  and that means, I can rewrite my  $e$  times  $d$  as some multiple of  $p-1$  times  $q-1$  namely some  $k$  times  $(p-1)(q-1) + 1$ .

Because  $ed$  gives the remainder 1 when divided by  $\phi(N)$ , and now what I can do is if I want to find out the value of  $x$  to the power  $ed$  modulo  $p$ , I know that  $ed$  is nothing but  $K$  times  $p-1$   $x$   $q^{-1} + 1$ . So, I can rewrite  $x$  to the power  $ed$ , modulo  $p$  as  $x$  to the power  $p-1$  whole raise to the power  $K$  times  $q^{-1}$ , and this  $+1$  will contribute another  $x$  modulo  $p$ , so that is what  $x$  to the power  $e$  modulo  $p$  will be and I know that  $x$  to the power  $p-1$  modulo  $p$  is 1.

That means this thing is nothing but 1, and 1 raise to the power  $K$  times  $q^{-1}$  is going to give me 1 only. That means, this entire first bracket is going to give me 1, so that means I can say that  $x$  to the power  $ed$  modulo  $p$  is nothing but  $x$  modulo  $p$ . That means with respect to  $x$  modulo  $p$  in subcase 1, if  $x$  is already divisible by  $p$ , then I can say  $x$  to the power  $ed$  minus  $x$  is completely divisible by  $p$ .

And in the second sub case also, I am establishing that even if  $x$  modulo  $p$  is not 0, I have established a  $x$  to the power  $ed$  modulo  $p$ , is same as  $x$  modulo  $p$ . So, that means both  $x$  to the power  $ed$  and as well as  $x$  gives us the same remainder on divided by  $p$ , and as a result I can say that their difference, namely  $x$  to the power  $ed$  minus  $x$  is completely divisible by  $p$ . It does not matter whether  $x$  is divisible by  $p$  or not, I have established here that  $x$  to the power  $ed$  minus  $x$  is completely divisible by  $p$ .

And symmetrically, I can do the same argument for  $x$  modulo  $q$  as well. So with respect to  $x$  and  $q$ , I have 2 subcases. If  $x$  is already divisible by  $q$ , then so is  $x$  to the power  $ed$ , and hence I can easily conclude that  $x$  to the power  $ed$  minus  $x$  is completely divisible by  $q$ . On the other hand, for the case when  $x$  is not divisible by  $q$ , I can apply Fermat's Little Theorem here, and I can say that  $x$  to the power  $q-1$  modulo  $q$  is 1.

And then using the similar argument that I have used for the case of module  $x$  and  $p$ , namely I can use the fact that  $ed$  is  $K$  times  $(p-1)(q-1) + 1$ , and then I can rewrite  $x$  to the power  $ed$  as  $x$  to the power  $q-1$  whole raise to the power  $k$  times  $p-1$ , multiplied by  $x$  modulo  $q$ . I know that since  $x$  to the power  $q-1$ , I know that overall it turns out to only  $x$  modulo  $q$ , that means that  $x$  to the power  $ed$ , as well as  $x$  gives me the same remainder on divided by  $q$ .

And hence I can say that  $x$  to the power  $ed$  minus  $x$  is completely divisible by  $q$ . So these are the properties that I have established now, that means I have shown that  $x$  to the power  $ed$  minus  $x$  is individually divisible by prime  $p$  as well as by prime  $q$ . Since my primes  $p$  and  $q$



are distinct, it automatically implies that  $x$  to the power  $e$  minus  $x$  is also going to be divisible by  $n$ , because  $n$  is my product of  $p$  and  $q$  and that establishes this theorem.

(Refer Slide Time: 33:01)

## Using Chinese Remainder Theorem (CRT) for Fast RSA Encryption and Decryption

- ❑ Both RSA encryption and decryption requires modular exponentiation
 
$$f_{\text{RSA}_{(N,e)}}(x) \stackrel{\text{def}}{=} [x^e \bmod N] \quad \text{Inv}_{\text{RSA}_{(N,d)}}(y) \stackrel{\text{def}}{=} [y^d \bmod N] \quad \left. \vphantom{\begin{matrix} f_{\text{RSA}_{(N,e)}}(x) \\ \text{Inv}_{\text{RSA}_{(N,d)}}(y) \end{matrix}} \right\} c \cdot n^3, \text{ where } |N| = n$$
- ❑ Time complexity for computing modular exponentiation modulo an  $\ell$ -bit integer  $\sim c \cdot \ell^3$
- ❑ (Chinese Remainder Theorem): Let  $N = p \cdot q$ , where  $p$  and  $q$  are primes

$[y^d \bmod N] \leftrightarrow (y_p, y_q)$

- ❑ (Number Theory):  $\text{GCD}(y, p) = \text{GCD}(y, q) = 1$ 
  - ❖  $[y^d \bmod p] = [y^{[d \bmod (p-1)]} \bmod p] = y_p$
  - ❖  $[y^d \bmod q] = [y^{[d \bmod (q-1)]} \bmod q] = y_q$
- ❑ Using CRT,  $y^d \bmod N$  can be computed in  $\frac{c \cdot n^3}{8} + \frac{c \cdot n^3}{8}$

*Handwritten notes on the right side of the slide:*  
 $|N| \approx \frac{n}{2}$   
 $N = p \cdot q$   
 $|N| = n$

Now, let us see how we can apply the Chinese Remainder Theorem for fast RSA Encryption and Decryption because this is a common crypt, which we use during the real-world instantiation of RSA function, so if you see the RSA encryption function and decryption function, then both of them requires modular exponentiation. To encrypt, we need to perform a compute  $x$  to the power  $e$  modulo  $n$ , and to decrypt we need to perform cipher text raise to the power  $d$  modulo  $n$ .

Now even though we have not yet discussed the best known algorithms for computing modular exponentiation, if time permits, we will discuss one of such algorithms in our subsequent lecture, it turns out the best known algorithm for performing modular exponentiation, modulo  $\ell$ -bit integer that requires amount of time, which is  $c$  times  $\ell$  cube, where  $c$  is some constant.

That means, if my modulus  $N$  is of size  $\ell$  bits, then to perform both RSA encryption as well as decryption function, I need to perform  $c$  times  $n^3$  operation. Now, what Chinese Remainder theorem says is since  $\ell$  is a product of 2 primes  $p$  and  $q$ , where the two factors  $p$  and  $q$  are co-prime to each other, then basically the Chinese Remainder Theorem gives you a bijection namely a one-to-one on two mapping from the set  $\mathbb{Z}_N^*$  to the Cartesian product of the set  $\mathbb{Z}_p^*$  and  $\mathbb{Z}_q^*$ .

Remember  $\mathbb{Z}_N^*$  is basically the set of all integers in the range 1 to  $N-1$ , which are co-prime to  $N$ , in the same way  $\mathbb{Z}_p^*$  is basically the set 1 to  $p-1$ . Basically, the set of integers in the range 1 to  $p-1$  which are co-prime to  $p$ , but since  $p$  is prime, the set  $\mathbb{Z}_p^*$  is nothing but the entire set 1 to  $p-1$  and in the same way, the set  $\mathbb{Z}_q^*$  is the entire set 1 to  $q-1$ . So what a Chinese Remainder Theorem does is, it defines a very nice bijection from the set  $\mathbb{Z}_N^*$  to the Cartesian product of  $\mathbb{Z}_p^*$  and  $\mathbb{Z}_q^*$ , where any element  $a$ , belonging to the set  $\mathbb{Z}_N^*$ .

It is mapped to the following pair of elements. You take the remainder of  $a$  modulo  $p$ , and the remainder of  $a$  modulo  $q$ . That will be the representation of the element  $a$  belonging to  $\mathbb{Z}_N^*$  in the set  $\mathbb{Z}_p^*$ , and the set  $\mathbb{Z}_q^*$  respectively, and not only that what Chinese Remainder Theorem basically shows is, tells you that if you are performing some computation in the set  $\mathbb{Z}_N^*$ , say if you are evaluating the value of  $f(a)$  modulo  $N$ .

Then the same computation you can carry over individually  $\mathbb{Z}_p^*$  and  $\mathbb{Z}_q^*$  and you will get a representation of the result of  $f(a)$  modulo  $N$ . That means instead of performing  $f(a)$  modulo  $N$ , you can perform  $f(a)$  modulo  $p$  and  $f(a)$  modulo  $q$ , and that resultant pair of elements can be considered as the representation of your result  $f(a)$  modulo  $N$ . So, that is how you can interpret this Chinese Remainder Theorem bijection.

That means, if I consider a decryption function for the moment, I am assuming that my public exponent  $e$  is 3, that takes care of the encryption part of the RSA function. RSA encryption process will be very fast, if I set my  $e$  to be 3, but my problem will be my decryption. I want to speed up my decryption process. Since, my decryption function requires me to compute  $y$  to the power  $d$  modulo  $N$ , by applying the Chinese Remainder Theorem.

The element  $y$  to the power  $d$  modulo  $N$ , which is an element of  $\mathbb{Z}_N^*$  can be interpreted as a pair of elements, one from  $\mathbb{Z}_p^*$  and another from  $\mathbb{Z}_q^*$ , where the representation from  $\mathbb{Z}_p^*$  will be  $y$  to the power  $d$  modulo  $p$  and representation from  $\mathbb{Z}_q^*$  will be  $y$  to the power  $d$  modulo  $q$ . Now, since  $y$  is relatively prime to  $p$ , as well as relatively prime to  $q$ , and if indeed that is the case, it turns out that we can prove that  $y$  to the power  $d$  modulo  $p$  is same as  $y$  to the power  $d$  modulo  $p-1$  modulo  $p$ .

That means, in the exponent, I can reduce my exponent,  $d$  to  $d$  modulo  $p-1$ , and I call this value to be  $y \text{ sub } p$ , and the same holds for  $y$  to the power  $d$  modulo  $q$  as well. That is, in the

exponent, I can reduce the exponent  $e$  from  $d$  to  $d$  modulo  $q-1$  and let me call this value to be  $y_q$ . That means, this  $y$  to the power  $d$  modulo  $N$  can be written as or expressed as the pair of elements  $y_{\text{sub } p}$ ,  $y_{\text{sub } q}$  as for the Chinese Remainder Theorem.

That means, if you know how to compute  $y_{\text{sub } p}$  and  $y_{\text{sub } q}$ , then using the Chinese Remainder Theorem, you can obtain the result  $y$  to the power  $d$  modulo  $N$ . That is what Chinese Remainder Theorem ensures for you. Now let us try to analyse how fast it is to compute  $y_{\text{sub } p}$  and  $y_{\text{sub } q}$ . Before going into that, let me tell you that since  $d$  is known to the receiver who is going to run the decryption algorithm, and  $p-1$  is also known to the receiver.

Because it knows the factors  $p$  and  $q$ , so  $d$  modulo  $p-1$  can be pre-computed by the receiver and can be stored once for all, and same holds for  $d$  modulo  $q-1$  as well. So  $d$  and  $q$  are also known to the receiver or to the person who is going to run the decryption algorithm and hence  $d$  modulo  $q-1$  can be pre-computed in advance by the receiver. Now, it turns out that using the Chinese Remainder Theorem, computing  $y$  to the power  $d$  modulo  $N$  requires you to perform two times  $c$  and  $q/8$  or  $n^{3/4}$  times computation.

This is because, while  $N$  is the product of two primes  $p$  and  $q$ , and my size of  $N$  is roughly of  $n$  bits, since  $n$  is the product of  $p$  and  $q$ , that means the size of prime factors  $p$  and  $q$  that we are using here is roughly of size  $n/2$  bits each. That means, to compute  $y$  to the power  $d$  modulo  $p-1$  modulo  $p$  or the value  $y_p$ , I need to perform a modular exponentiation, where the size of the modulus is  $n$  over two bits.

And by using the best known algorithm that will require me to perform computations of order  $c$  times  $n^{3/8}$  and similarly to compute  $y_{\text{sub } q}$ , I need to perform computation of order  $c$  and  $q/8$ , and if I sum these two things. I get that the total computation that I need to perform to compute  $y_{\text{sub } p}$  and  $y_{\text{sub } q}$  will be two times  $c$  and  $q/8$ , which is basically  $c$  times  $n^{3/8}$ , and this is simply 25% saving compared to the naïve way of performing or calculating  $y$  to the power  $d$  modulo  $N$  directly.

If instead of computing  $y$  to the power  $d$  modulo  $N$  directly, we use this indirect approach where we compute  $y_{\text{sub } p}$ ,  $y_{\text{sub } q}$ ,  $ZP^*$ , and  $ZQ^*$ . Then combine it to obtain the result  $y$  to

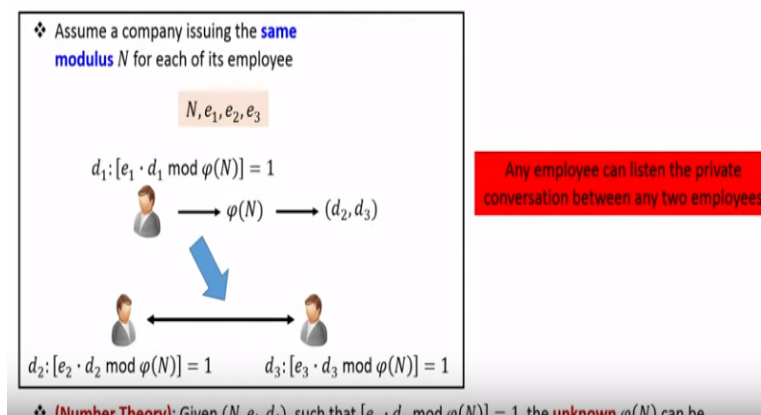
the power  $d$  modulo  $N$ , basically end up saving 25% of computation and this is a very common thing that is used in the practical instantiations of the RSA decryption algorithm.

(Refer Slide Time: 40:25)

## Dependent Public Keys Attack on RSA

❑ Sharing RSA public parameters across multiple users is extremely unsafe

❑ Common modulus attack



Now, let me end this lecture by showing you some more attacks on RSA, namely I want to show you that how dangerous it could be to share public parameters across multiple users in the context of RSA cryptosystem. So, I am going to show you one of the simplest possible attack, which we call as common modulus attack, there are other sophisticated attacks, which are also possible.

But I am not going to discuss them, and this is kind of very different compared to El Gamal encryption scheme, where we have seen in the context of El Gamal encryption scheme, sharing public parameters, namely sharing the description of the group, description of the generator across multiple receivers, that means it is fine. If multiple receivers use the same cyclic group to instantiate their El Gamal encryption scheme, the same generator to instantiate your El Gamal encryption scheme and so on, but when it comes to RSA.

It might be extremely unsafe to share public parameters across multiple users. So, the attack here is as follows. Assume a company, which is using the same modulus  $N$  for each of its employee. That means, every time a new employee joins the company, you can imagine that the company retains the same modulus  $N$  for the employee, but what it does is, it generates a fresh independent public exponent  $e_i$  for that user, corresponding decryption  $d_i$  for that user such that  $e_i$  and  $d_i$  are co-prime modulo  $N$ .

So for the moment, assume we have 3 employees in the organization, the first employee has a secret decryption key  $d_1$ . The second employee has its secret decryption key  $d_2$ , and in the same way, the third employee has a secret decryption key  $d_3$ , and we know that property wise  $e_i$  and  $d_i$ , they are multiplicative inverse of each other modulo  $\phi(N)$ . Now, it turns out that again by using a well-known fact from Number Theory, we can prove that, if we are given the modulus  $N$ , and  $e_i, d_i$  such that  $e_i$  and  $d_i$  are multiplicative inverse of each other.

So I beg your pardon here, it should not be  $e_1$  times  $d_1$  here, it should be  $e_i$  times  $d_i$ , that is a typo here. So, if you know the modulus  $N$ , if you know the value of  $e_i$ , and we know the value of  $d_i$  such that  $e_i$  and  $d_i$  are multiplicative inverse of each other, modulo  $\phi(N)$  where  $\phi(N)$  is not known to us, then we can compute a value of  $\phi(N)$  in poly of size of modulus  $N$  time. That means, for instance employee 1 is considered here.

Since it knows its public exponent  $e_1$ , as well as decryption exponent  $d_1$ , but it does not know the unknown value of  $\phi(N)$ , by using this fact from the Number Theory, and using that algorithm, it can compute in polynomial amount of time, the value of  $\phi(N)$ , and once  $\phi(N)$  is computed by the employee 1. Since it knows the value of  $e_2$ , namely the public exponent public key of the second employee, and it knows the modulus  $N$ , then by using the same result from Number Theory, it can compute  $d_2$ .

And in the same way it can compute the value of the decryption exponent of the third employee as well, and once it knows the value of  $d_2$  and  $d_3$ , then any private communication, which is happening between the second and the third employee using RSA encryption scheme. Even if it is a padded RSA encryption scheme, which is randomized for the moment assume that, since the value of  $d_2$  and  $d_3$  is known completely to the employee 1.

It can completely find out what exactly is happening between employee 2 and 3. So, that shows that how unsafe it might be if we end up having multiple users having the same modulus  $N$ . It is highly, highly dangerous. So, that brings me to the end of this lecture. Just to summarize, in this lecture, we have seen that how we can instantiate a public-key encryption scheme from any One-Way Trapdoor Permutation.

And we have shown that how we can instantiate using the RSA Trapdoor Permutation, and get what we call as Plain RSA Cipher, but Plain RSA Cipher cannot be used in practice

because first of all it is not randomized, and secondly we cannot directly reduce its security to the RSA problem. We have seen how we can make RSA randomized encryption process by doing padding, and we have seen that how we can speed up the RSA decryption function using Chinese Remainder Theorem, Thank you.