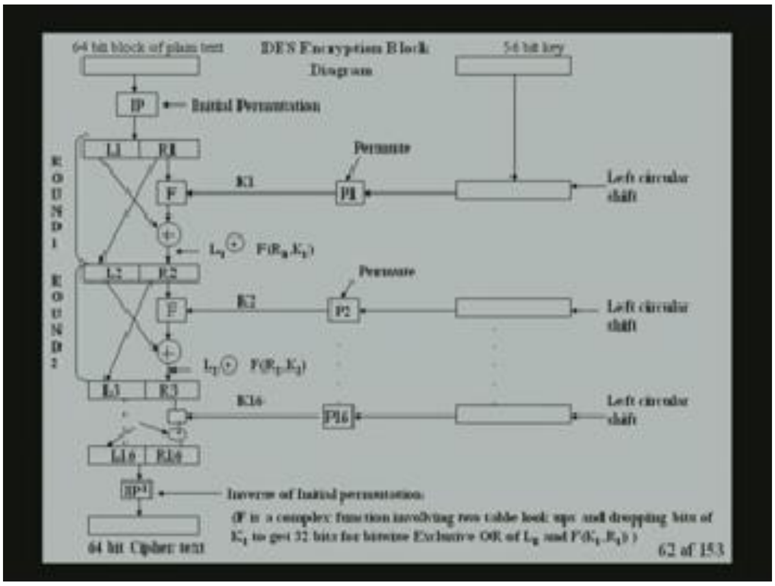
System Analysis And Design
Prof. V. Rajaraman
Department of Super Computer Education & Research
Indian institute of Science , Bangalore

Lecture - 35

Thus, encryption and I put down this transparency, which effectively gives the block diagram of the steps in encryption.

(Refer Slide Time: 01:23)

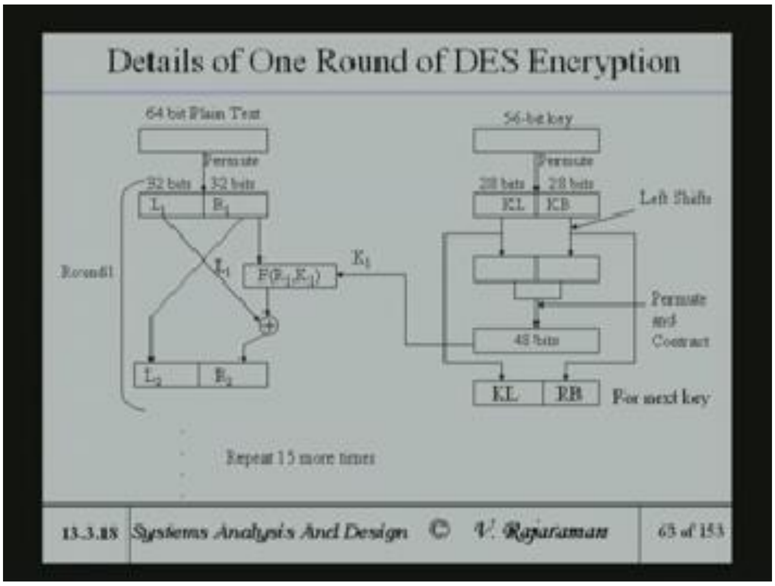


DES Encryption Block Diagram

(F is a complex function involving two table look ups and dropping bits of K_1 to get 32 bits for bitwise Exclusive OR of L_0 and $F(K_1, R_0)$)

And this being a very long figure does not happen to fit into a screen. And so, what I will do is, I will take one stage of it one top most stage and explain what exactly happens in the disencryption.

(Refer Slide Time: 01:46)



Details of One Round of DES Encryption

13-3.18 Systems Analysis And Design © V. Rajaraman 63 of 153

Now, you take 64 bit plain text it means as I pointed out the plain text by plain text. You mean unencrypted text. So, the text you take and out it up into 64 bit chunks and each 64 bit chunk is separately disencoded. So, you got a 64 bit plain text. Then you permute it. There is a initial permutation that is what the block shown there, it will have it will again become too long.

But, there is a permutation operation; that means, permutation operation. I explained in other words there will jumbling of the bits in some specific order determined by some kind of a key. And then, the 64 bit text is put into two parts L1 and R1. There are two parts and we will deal with each of the parts separately. So that is as far as this is concerned.

Let us then go the, where the key? The key which is used is 56 bit key. It is not a 64 bit key, but it is a 56 bit key. You might ask why 56, why not 64, why not 48, why not 32. Whatever it is the reason why 56 has been chosen is that. They found that it is a reasonable key size. And for this dealt encryption in terms of the prevailing technology in the 1970s as I pointed out DES was invented in 1970s at that time a 56 bit key was considered sufficient.

So, once again the key is permuted with some permutation operation. Then, it is divided into two parts. And some bits are dropped again permutation contraction operation takes place and then 48 bits come again. You drop some bits, because here R1 is a 32 bit number. And K1 which will come here will be again a 32 bit number. Because, you will take some function R1 K1 which is somewhat like the transposition, which you looked at they had two steps is not it.

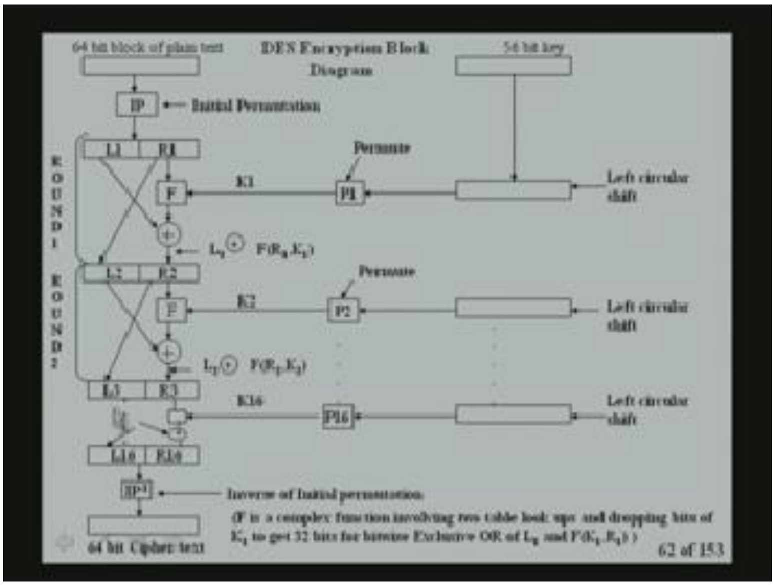
So here, the table you look at the F will be a very complex function of R1 K1, where it can it looks at some table lookup, where R1 is involved and also some exclusive or operations and so on. The reason, why I am not going to go through this full details of that is because, it is not rather than to this course that the entire courses are there in cryptography.

In cryptographic courses, they give theoretical background of why 56 bits is scripted. And how do you determine this strength of the key and how do you drop this. And what kind of a table is used and why the table is used, all that is given in a cryptography book. In fact, there is a book by schmider. And another book by skillings schmiders book effectively deals with cryptography the whole book.

And skillings book has both security and as a part of security it is cryptography is dealt with and that book also does deal with this in far amount of detail. So those, who are interested may kind of go and look at that book. Now, here this ((Refer Time: 01:46)). This 48 bit is selectively reduced to 32 some dropping is takes place. And a key which is essentially involved in some table look up and so on is used. And this function operation is carried out.

And then, you take the left half 32 bits exclusive or bit this result of this operation. This function application of R1 and K1and then that becomes R2 were as L1. After this work it goes to R2 and R1 becomes L2. There is no nothing which happens here, this is one step. And there is again one step here and this is repeated 15 more times that is, what is show showed in the earlier slide.

(Refer Slide Time: 06:31)



DES Encryption Block Diagram

64 bit block of plain text

56 bit key

IP ← Initial Permutation

ROUND 1

ROUND 2

L1 R1

F

K1

Permute

P1

Left circular shift

$L_0 \oplus F(R_0, K_1)$

L2 R2

K2

P2

$L_1 \oplus F(R_1, K_2)$

L3 R3

K16

P16

L16 R16

IP^{-1} ← Inverse of Initial permutation

64 bit Cipher text

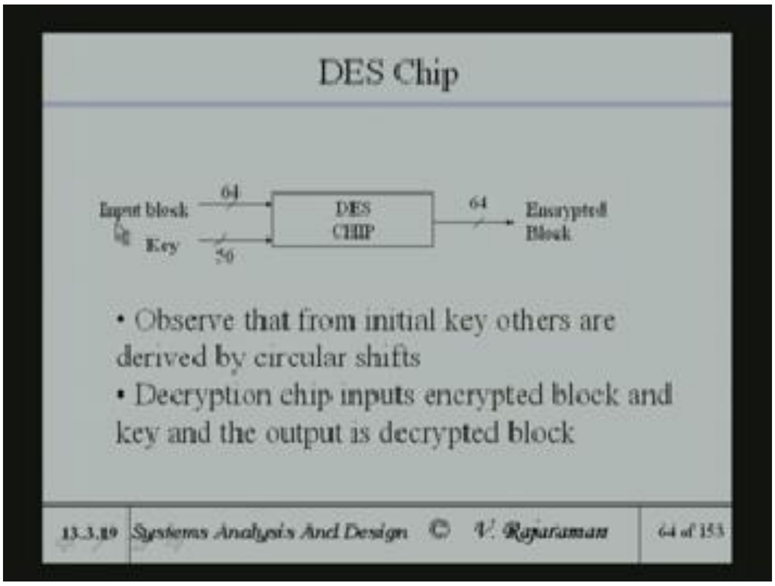
(F is a complex function involving two table look ups and dropping bits of K_1 to get 32 bits for bitwise Exclusive OR of L_0 and $F(K_1, R_0)$)

62 of 153

Now here, this is one step and there are number of steps and it goes on to till 16K. 16 is 16th time it happens. And then, inverse permutation of IP inverse that is initial permutation. The inverse permutation is done and you will get a 64 bit cipher text at the end of this.

((Refer Time: 01:46)) So, effectively you if it have this kind of a step. So, 15 more times and then the reverse inverse permutation, the inverse of this is done. And at these step also as you say the key now the 28 bits are taken and made into the next the next key is effectively. The same key the same thing except after permutation. And more again this key is used. And we go through the whole process again for the next 15 steps. This is the primarily the way in which the DES encryption works.

(Refer Slide Time: 07:35)



DES Chip

- Observe that from initial key others are derived by circular shifts
- Decryption chip inputs encrypted block and key and the output is decrypted block

13.3.19 Systems Analysis And Design © V. Rajaraman 64 of 153

And now, the advantage of DES encryption and why it is been very popular is that. You have a chip that is VLSI chip in which the entire all those can be incorporate. Because, the all those consists of primarily shifting and SARI. And some terms of some bits you might table and so on. So, this kind of not difficult to make a chip, it is not if as long as the volume of this is very high.

The semi conductor manufacturers will find it very quite profitable to come up with the same chip which is at alienable cost. And the advantage from the users point of view is he just has to put this chip in front of a PC. And then the entire thing will be encrypted before. In other words at the, you can look at it in other point of view. That is at the output which is going from the company to the recipient, you put this chip.

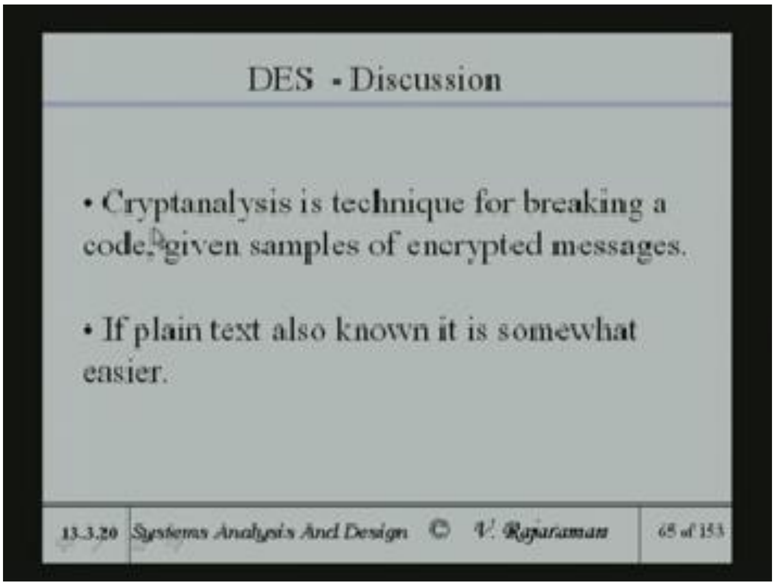
And to which you feed the input blocks a 64 bits and give the key of 56 bits. And then, encrypted block comes out. At the other end what you really have to do is to use same key and do the reverse of whatever is done the entire DES encryption method is symmetric. That is the point really is decryption chip inputs encrypted block and key.

And output the decryption block, whether it is the same DES chip is used again, where you give the encrypted block as input. And then the key is also another input and out comes the decrypted block. So, it is effectively it is a symmetric algorithm that is one of the reasons, why it is used very effectively. Because, the same chip can be used for both encryption and decryption as in all these algorithms the algorithm itself is made public.

The only thing which is not public made public is the key. So, the secrecy lies in the key. So, you should not reveal the key to anybody, if you reveal the key the entire game is lost. So, the key is the leapt to be the most important part of any encryption. So, two points is that. Two points I want to make is that the entire security lies in the key number 1, number 2 the entire disencryption is simple enough to import into your chip. Number 3 is that it is a symmetric encryption.

In other words, the same block which can be used in encryption. The either way is applied with the encrypted one then the outcomes the decrypted output that is decrypted thing.

(Refer Slide Time: 10:54)



DES - Discussion

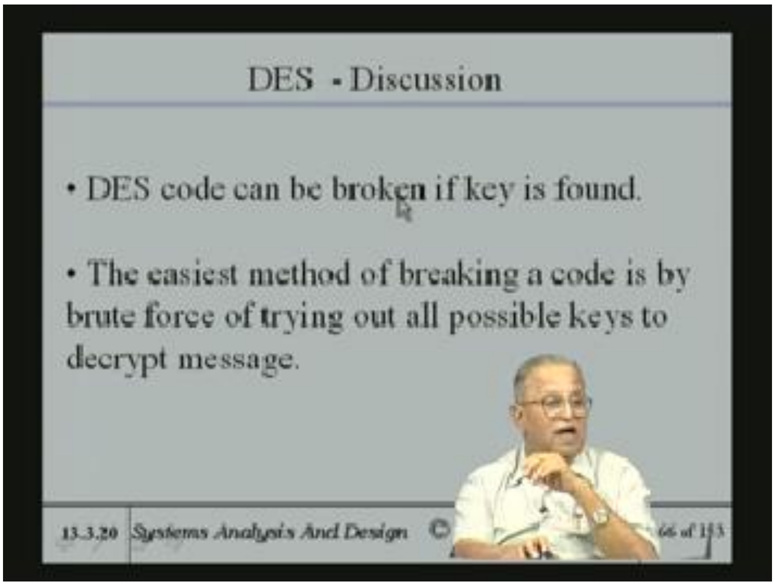
- Cryptanalysis is technique for breaking a code, given samples of encrypted messages.
- If plain text also known it is somewhat easier.

13-3.20 Systems Analysis And Design © V. Rajaraman 65 of 153

Now, cryptanalysis is a technique for breaking a code given samples of encrypted messages. As I said all in all whenever encryption is done, there are professionals who are trying to find and locate how to break the code. Particularly, Norton and all that and also suppose your companies secretes are also found out by a competitor. He they may employ some people to whose main job is to guess, what the key ought to be.

And the tracing of that is done, suppose there are lot of samples of plain text and encrypted text. So, they got input and output and they got to guess, what the function is what the encryption function is.

(Refer Slide Time: 11:48)



DES - Discussion

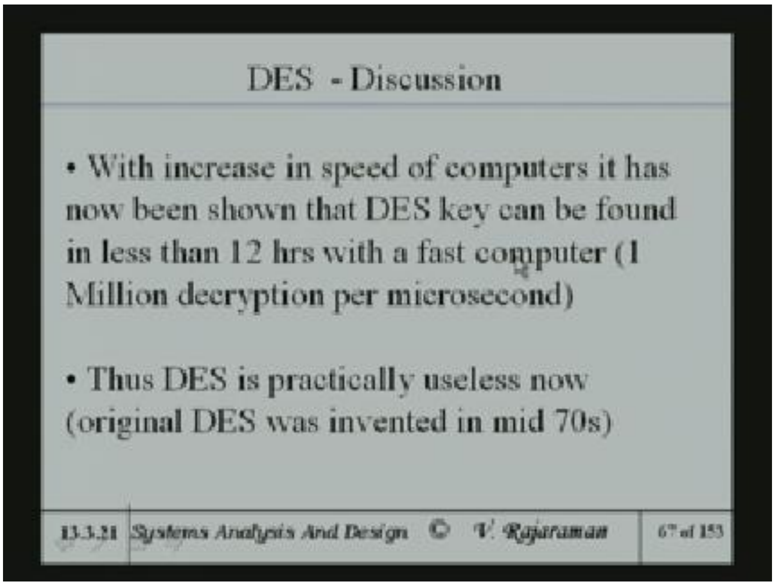
- DES code can be broken if key is found.
- The easiest method of breaking a code is by brute force of trying out all possible keys to decrypt message.

13.3.20 Systems Analysis And Design © 66 of 153

And this of course, is not easy the easiest the, what I would say the brute force technique is to try out all possible keys. See there are 56 bit key, so there are there are two to the 56 possible ways in which you can change the key. And of course, there are tables and permutations so on. So, there are; obviously, quite a large number of trials that we have a to do.

But then, nowadays computers are becoming very fast. So, we have got enough samples of plain text. We have got and encrypted text, you can be just trying with a whole lot of these. And of course, the parallel machine work works wonderfully for this. Because, each of the processors can be looking at one different key and all of them can be run in the same algorithm. So, if it is a parallel machine with 500 process sites effectively 500 key had been tested in 1 cycle.

(Refer Slide Time: 13:05)



DES - Discussion

- With increase in speed of computers it has now been shown that DES key can be found in less than 12 hrs with a fast computer (1 Million decryption per microsecond)

- Thus DES is practically useless now (original DES was invented in mid 70s)

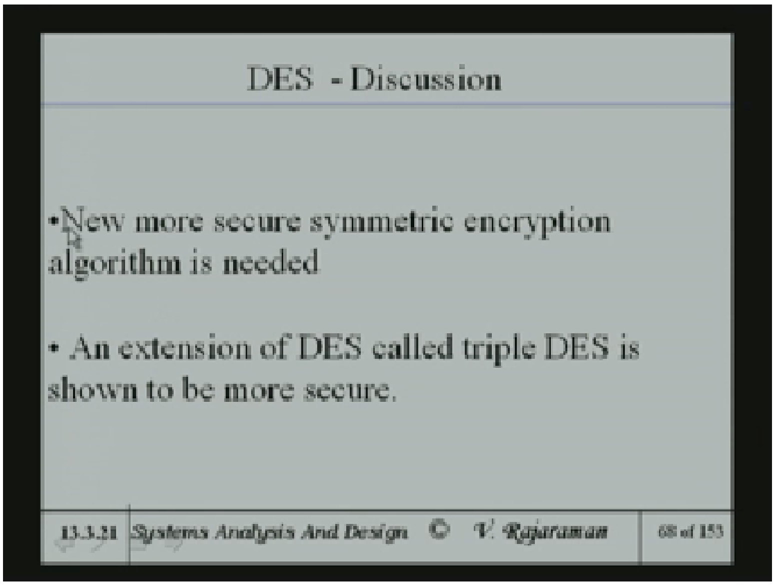
13.3.21 Systems Analysis And Design © V. Rajaraman 67 of 153

So, with all this modern technology it has been found that with increasing speed of computers DES key can be found in less than 12 hours with a with a fast computer may be a parallel computer. And I find if one million decryptions per microsecond if ad visible then in 12 hours, you can actually brute force to find out the key.

Thus, DES is practically useless now. Because, this current machines are having finally, this kind of a speed, because machines that are of this range are now available. And so, it is one is to access to that slot machine. Even if, you do not got access, you have got huge lot PC's ideal PC's. You can make all of them work simultaneously and get effectively speed up.

And each PC is reasonably fast nowadays, because with something like 2 Giga hertz servers and so on or even 1.5 Giga hertz desktop. You get a company has got 500 desktops is very common. You can able to can use the ideal secure cycles and able to decrypt. That is the reason why DES is considered practically useless. Because, very recently I said it was invented in 1970s.

(Refer Slide Time: 14:24)



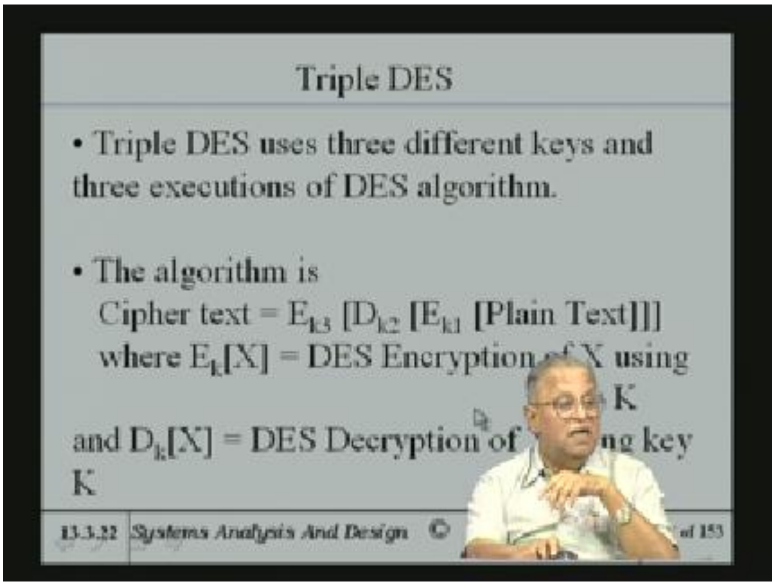
DES - Discussion

- New more secure symmetric encryption algorithm is needed
- An extension of DES called triple DES is shown to be more secure.

13.3.21 Systems Analysis And Design © V. Rajaraman 68 of 153

So, one is to find new methods. So, new more secure symmetric encryptions have in some needed. An extension of DES called triple DES is shown to be more secure. In fact, triple DES is what is currently doing used formally extensively.

(Refer Slide Time: 14:41)



Triple DES

- Triple DES uses three different keys and three executions of DES algorithm.
- The algorithm is
  Cipher text = E_{k3} [D_{k2} [E_{k1} [Plain Text]]]
  where E_k[X] = DES Encryption of X using [illegible] K

and D_k[X] = DES Decryption of [illegible]ng key K

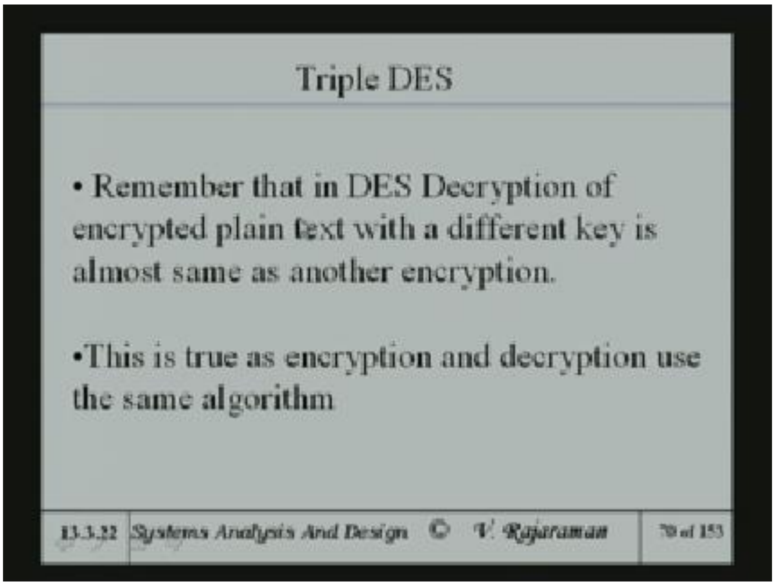
13.3.22 Systems Analysis And Design © [illegible] of 153

And let us look at what is triple DES? Triple DES as the name implies applies DES three times over. The algorithm is taking the plain text. Apply DES encryption once. And having applied DES encryption once with one key K1 pick another key and do decryption. See as I pointed out the decryption method different key will not get back the plain text, because unless this and this are equal.

The decryption will effectively here of only if the two are equal. Decryption will get back give back the plain text. In this case, it is useless. So, the two different keys are used and so, this will decrypt. And decryption is nothing but encryption. Because, the same algorithm is used with a different key and then you encrypt again with third key K3.

And one number, why I am using E D and E. The simple reason is it is kind of symmetric applying only on the other way which we will see again very quickly. So, it is a very simple way of having a symmetric encryption and decryption is to effectively apply it in reverse, so the triple DES effectively.

(Refer Slide Time: 16:14)



Triple DES

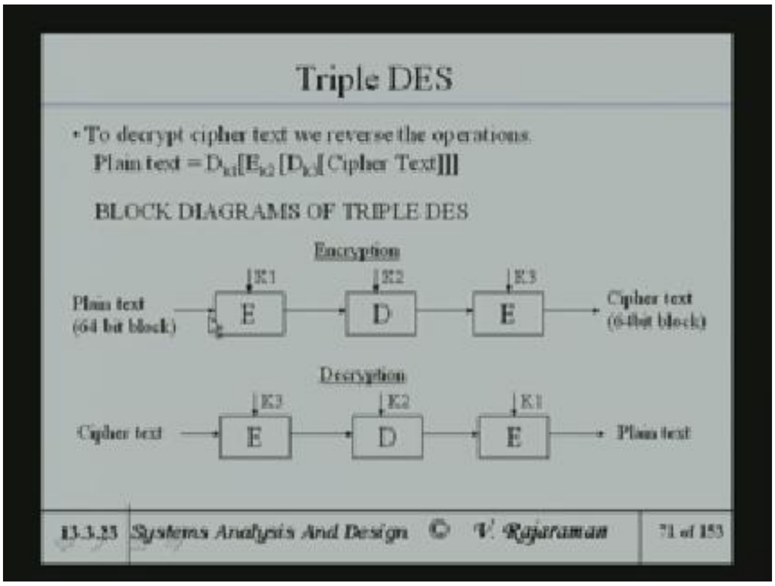
- Remember that in DES Decryption of encrypted plain text with a different key is almost same as another encryption.

- This is true as encryption and decryption use the same algorithm

13.3.22 Systems Analysis And Design © V. Rajaraman 70 of 153

Say I said remember decryptions of encrypted plain text with a different key is almost same as another encryption. This same as encryption and decryption use the same algorithm.

(Refer Slide Time: 16:27)



Triple DES

- To decrypt cipher text we reverse the operations.
  Plain text = $D_{k1}[E_{k2}[D_{k3}[\text{Cipher Text}]]]$

BLOCK DIAGRAMS OF TRIPLE DES

Encryption

Plain text (64 bit block) → E (K1) → D (K2) → E (K3) → Cipher text (64-bit block)

Decryption

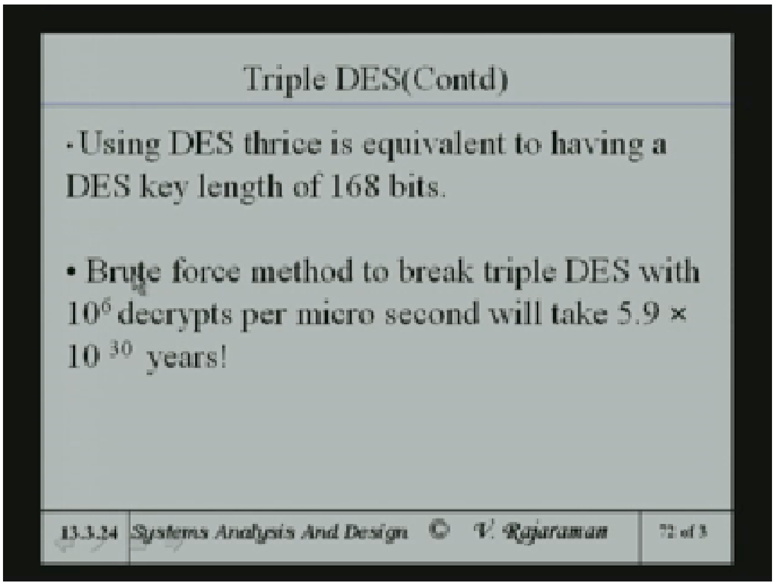
Cipher text → E (K3) → D (K2) → E (K1) → Plain text

13.3.35 Systems Analysis And Design © V. Rajaraman 71 of 153

So, now you take a plain text. And apply you see the plain text K1 you applied will be encrypted with K2 you decrypt which is again going for another encryption. And with K3 you encrypt you get a cipher text. Now there are three different keys were being used and three different encryptions texts initiated them. Use a 15 bit key and of course, encoded block is a 64 bit block.

At decryption in the reverse that is you apply K3 first encrypted. And then apply K2 and then apply K1 in reverse and you get back plain text. So, you can see the symmetry between this and this. And that is the reason, why this kind of a three step process with of course, the in between being a decryption step is being done in triple DES.

(Refer Slide Time: 17:25)



Triple DES(Contd)

- Using DES thrice is equivalent to having a DES key length of 168 bits.

- Brute force method to break triple DES with 10^6 decrypts per micro second will take 5.9×10^{30} years!

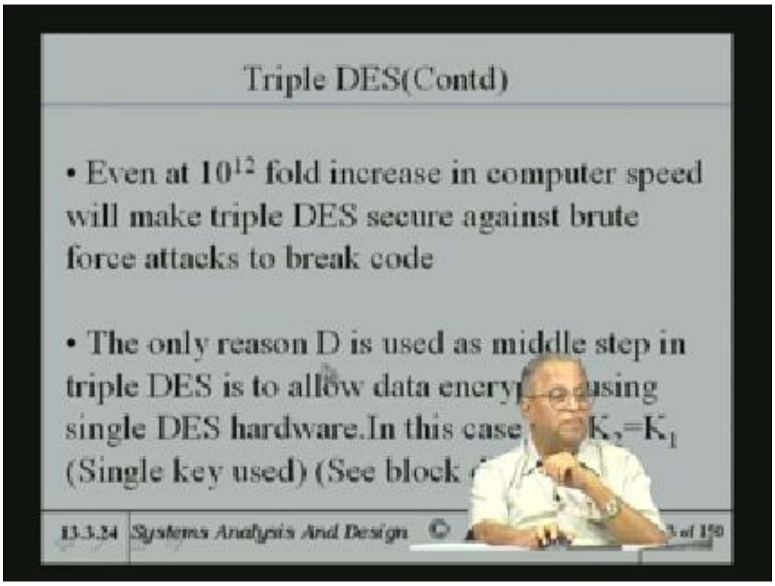
13.3.24 Systems Analysis And Design © V. Rajaraman 72 of 3

Using DES thrice is equivalent to having a key DES key length of 168 bits. In other words, three different keys of 56 bit each 3 times of 56 168. So, this tends to encryption in other words the time required to decrypt it now it becomes very very large. Send brute force method to break a triple DES with 10 to 6 decrypts per micro second will take in this case people have calculated 5.9 times 10 to the 30 years. That of course is a, you cannot even imagine 10 to the power of 30 years.

So even if, suppose you have to increase the speed of 10 to the 12e in possibly the future. Then, the number of years would come down to 30 minus 12 which is 18 which is 10 to the 18 years which is again still a lot of time. So, brute force cannot be applied on triple DES. So, people are quite satisfied with triple DES a symmetric encryption scheme. And of course, it is it is the same old chip can be used except that.

You go through use through different keys and you got to have a problem of distributing three different keys to the person who is going to receive it. So that is the major problem with every symmetric encryption.

(Refer Slide Time: 18:51)



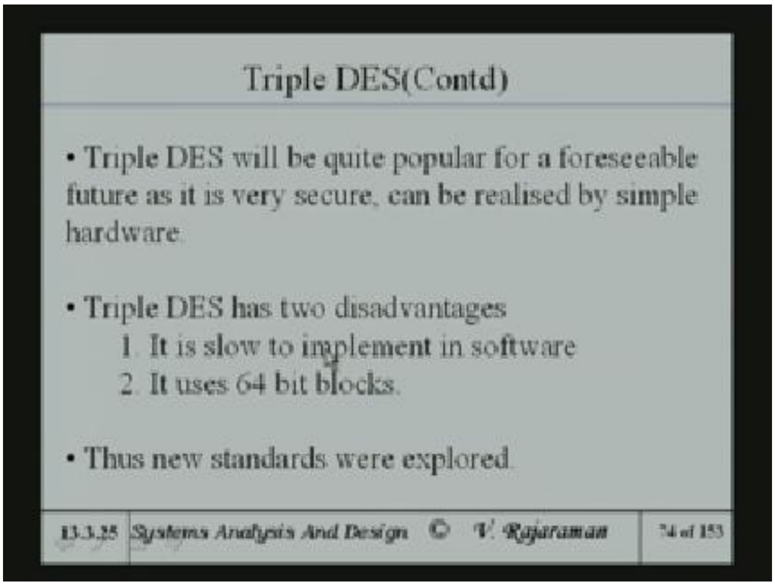
Triple DES(Contd)

- Even at 10^{12} fold increase in computer speed will make triple DES secure against brute force attacks to break code
- The only reason D is used as middle step in triple DES is to allow data encry[illegible]using single DES hardware.In this case [illegible] K_2=K_1 (Single key used) (See block [illegible]

13.3.24 Systems Analysis And Design © [illegible] 3 of 150

What is a key distribution problem? Is that even at 10 to the power 12 fold increase in computer speed will make triple DES code secure because brute force. The only reason D is used as middle step is triple DES is to allow data encryption using single DES hardware.

(Refer Slide Time: 19:10)



Triple DES(Contd)

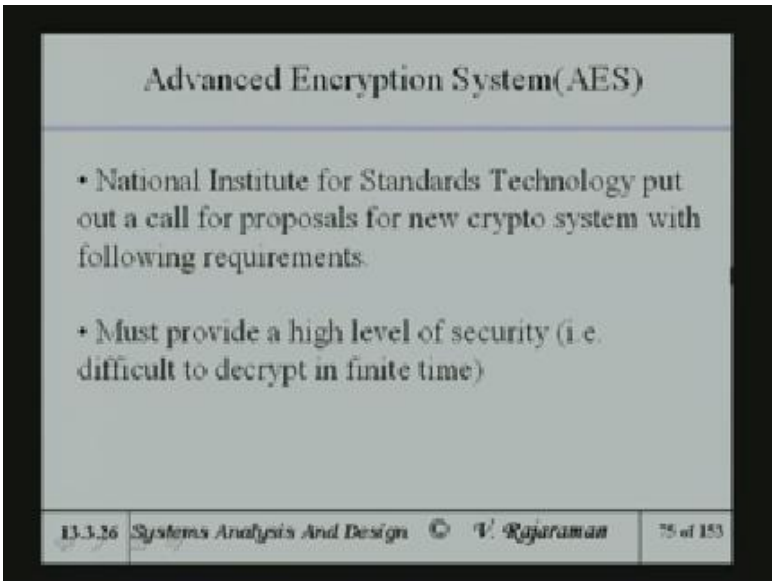
- Triple DES will be quite popular for a foreseeable future as it is very secure, can be realised by simple hardware.
- Triple DES has two disadvantages
  1. It is slow to implement in software
  2. It uses 64 bit blocks.
- Thus new standards were explored.

13.3.25 Systems Analysis And Design © V. Rajaraman 74 of 153

And single say it will be popular in the next four sided feature. And triple DES as of course, has got two disadvantages. It cannot be implemented in software easily. Because, all these steps I pointed out changing things around and dropping bits and permutations and so on. And 64 steps for each encryption step and decryption step.

And three such steps if you want to program it is going to take to program it is going to take a long time to be able to do the encryption were as a chip will do it very fast. So, the disadvantage software cannot be used. You had to only use only hardware. So, hardware is of course, is sometimes considered more expensive. Because, particularly small companies cannot be just going you know going go and buy these things.

(Refer Slide Time: 20:17)



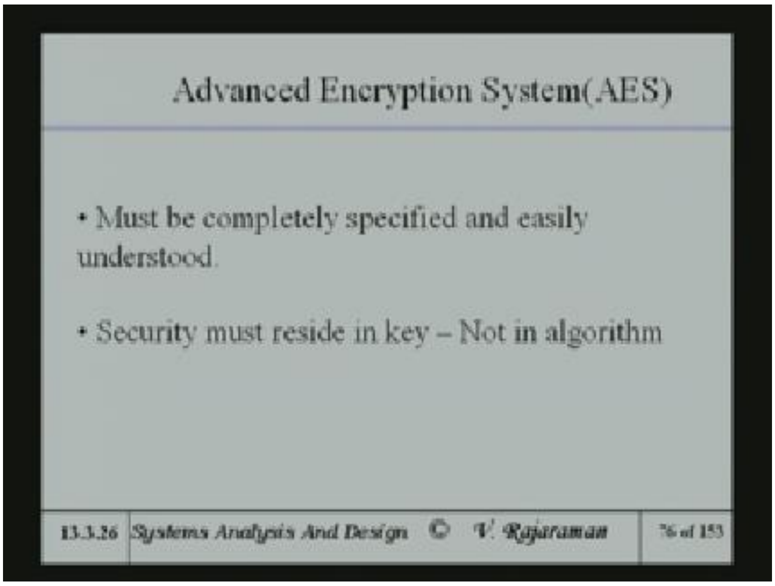
Advanced Encryption System(AES)

- National Institute for Standards Technology put out a call for proposals for new crypto system with following requirements
- Must provide a high level of security (i.e. difficult to decrypt in finite time)

13.3.26 Systems Analysis And Design © V. Rajaraman 75 of 153

And so, new standard was explored now onwards is there. Any other method of encryption which is more modern and so the national institute of standards of USA. Put out a call for the proposals for new crypto system called advanced encryption system with the requirements. That it must provide high level of security that is difficult to decrypt. Decrypt in a finite time. That is in other words it should be at least as strong as the triple DES is dealt with in 8 years to decrypt using brute force.

(Refer Slide Time: 20:53)



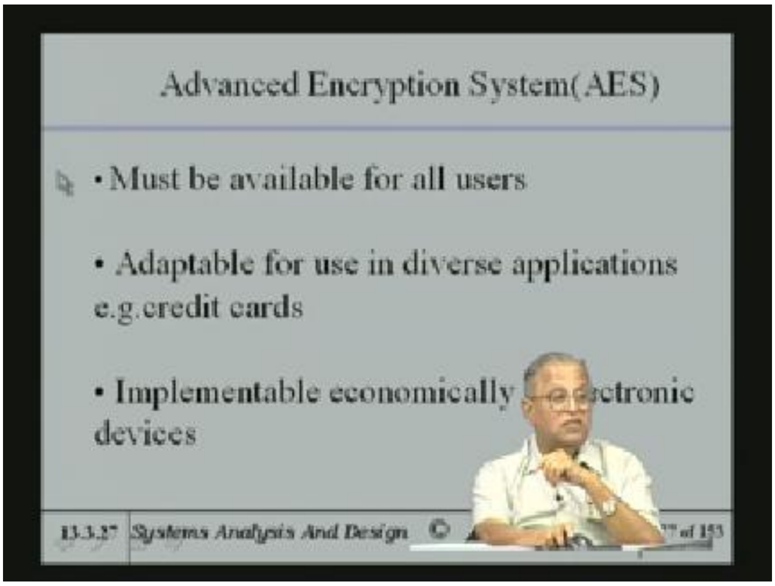
Advanced Encryption System(AES)

- Must be completely specified and easily understood.
- Security must reside in key – Not in algorithm

13.3.26 Systems Analysis And Design © V. Rajaraman 76 of 153

Must me completely specified and easily understood. Whenever the algorithm must be completely specified, it should be easily understood by people. And security must reside in key not in the algorithm as usual. Because, all the algorithms are made public, only the key is not made public.

(Refer Slide Time: 20:53)



Advanced Encryption System(AES)

- Must be available for all users
- Adaptable for use in diverse applications e.g.credit cards
- Implementable economically ... ctronic devices

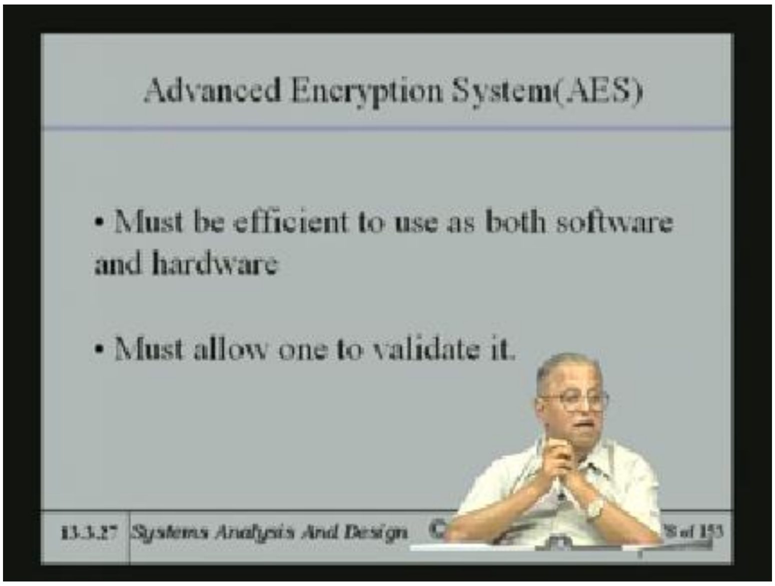
13.3.27 Systems Analysis And Design © ... 77 of 153

Must be available to all users, so there should be not be any kind of restriction on the kind of use. Because, what happened was with DES and all that, the American government put a restriction on the use of DES and some what they have strong encryption methods outside of America. And also if what if you are considered their friend then you are considered their enemy and the enemy is not allowed to use this.

And they had export controls on that report like for instance India was under that export control and watch list for number of years. Now of course, there is little bit of a warm relationship by and large. The government should not have the power to deny technology outside of a country. So that, report as a requirement.

Adaptable for use in diverse applications that is not only on computer, but even on credit cards to ensure security; that means, either them must be a very enough at the same time easy enough to be put into a chip which can be incorporated in a in a credit card. Implemented economically in a electronic device; that means, we can use a chip for doing it.

(Refer Slide Time: 22:26)

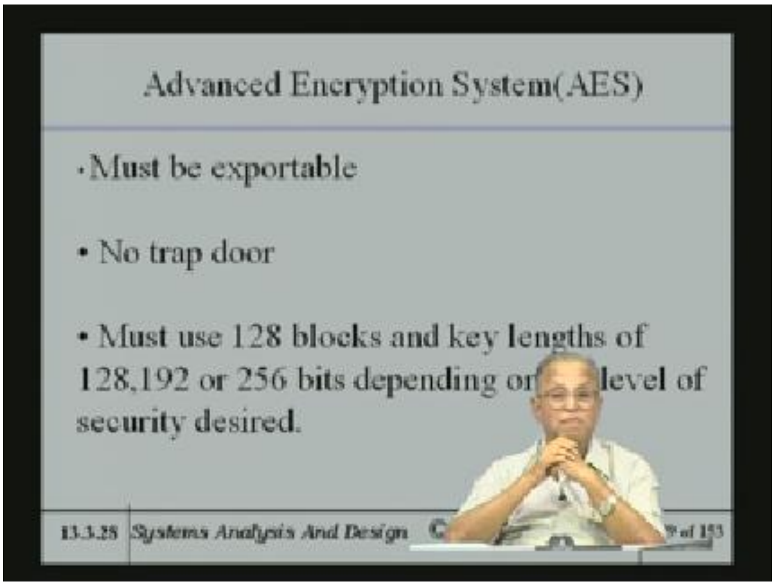


Advanced Encryption System(AES)

- Must be efficient to use as both software and hardware
- Must allow one to validate it.

Must be efficient to use both as software and hardware, so unless this they want day years to be easily put in software’s also. So because, one does not have to invest in hardware. Must allow one to validate it that is one the algorithm must be validated by transpositions.

(Refer Slide Time: 22:53)



Advanced Encryption System(AES)

- Must be exportable
- No trap door
- Must use 128 blocks and key lengths of 128,192 or 256 bits depending on level of security desired.

13.3.28 Systems Analysis And Design ©

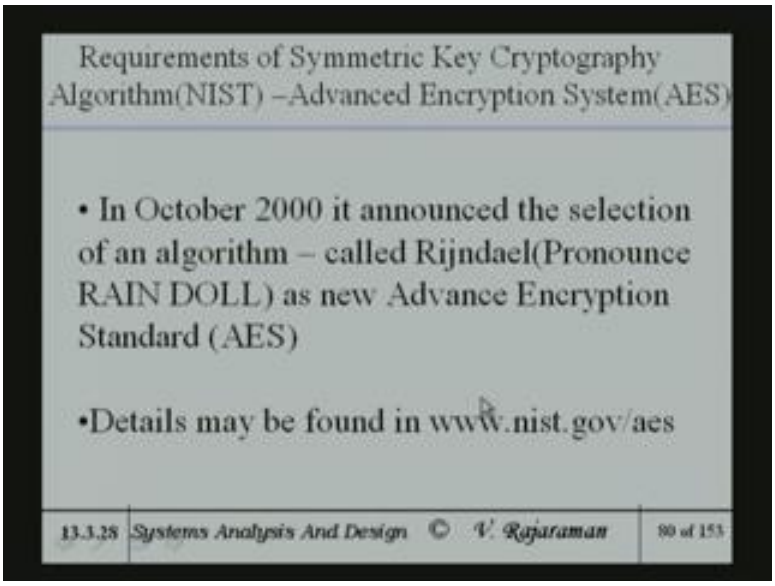
9 of 153

To find out, how much time we have taken to kind of decrypt, must be exportable; that means, we said the country cannot put restriction on export.

No trap door, trap door a secret method of actually which the government try o keep to try to kind of break the code. And this trap door, these are all used particularly if suppose government does has monopoly on say best type chip. Then, they can intentionally put a trap door to be able to kind of break the code. By safely kind of getting some values of key by snooping inside and with some technology they may have. That is a very dangerous thing that should not be allowed.

I must use 128 see instead of 64 bit blocks 128 bit blocks or 192 or 256 blocks. So, large blocks should be useable. So, the security becomes higher.

(Refer Slide Time: 23:58)



Requirements of Symmetric Key Cryptography Algorithm(NIST) –Advanced Encryption System(AES)

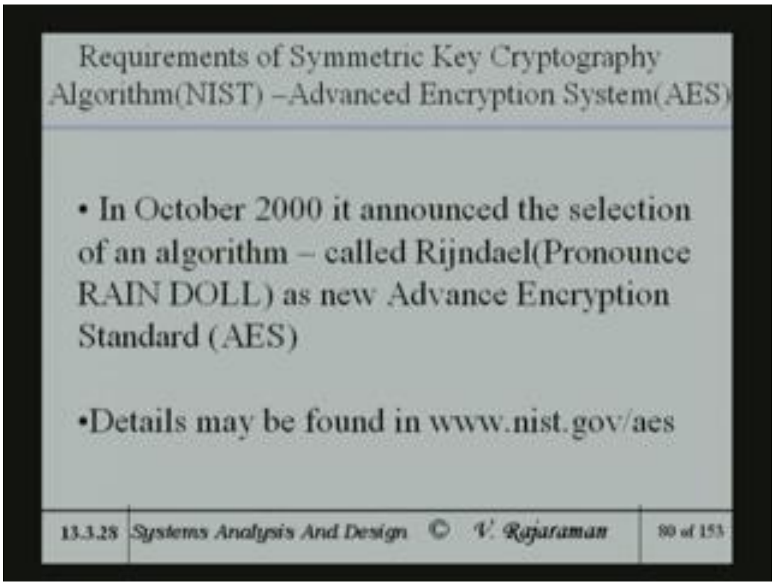
- In October 2000 it announced the selection of an algorithm – called Rijndael(Pronounce RAIN DOLL) as new Advance Encryption Standard (AES)
- Details may be found in www.nist.gov/aes

13.3.28 Systems Analysis And Design © V. Rajaraman 80 of 153

So, in october (Refer Slide Time: 23:59)

(Refer Slide Time: 22:53) The blocks in this was only 64 bits were as in the advanced encryption standard the blocks can be 128 192 or key lengths you might say. The blocks are at key length; because the block size and the key length are equal must be 128 192 or 256 depending on the level of security designed.

(Refer Slide Time: 25:15)



Requirements of Symmetric Key Cryptography Algorithm(NIST) –Advanced Encryption System(AES)

- In October 2000 it announced the selection of an algorithm – called Rijndael(Pronounce RAIN DOLL) as new Advance Encryption Standard (AES)
- Details may be found in www.nist.gov/aes

13.3.28 Systems Analysis And Design © V. Rajaraman 80 of 153

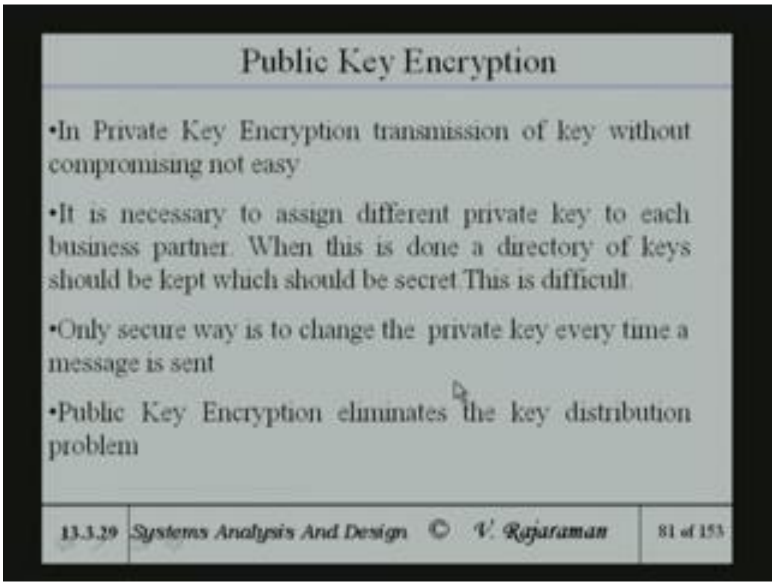
In October 2000, they kind of you mean they put out this advertisement for many groups in the world to compete for this proposing the advanced encryption standard. After considering a number of different entries which have came from all over the world. They finally, decided on picking something which is proposed by do two Dutch mathematicians. And it is the two peoples name was Rijndael (Pronounce RAINDOLL).

That is the pronunciation in the correct pronunciation. So, the actual word is Ri j j n d a e l and pronounced Rijndael RAIN DOLL is the new advanced encryption standard algorithm. And this algorithm is now available for people to implement and some people have started implementing chips for this and inspected. That this will be a very very secure standard which will be much better than the DES type standard for long time to come.

The detail the algorithm is found to be complicated. So, those who are interested can look at this website n i s t. Because, n i s t is the one which a put out the adds for this and then they are the ones who had sponsored the whole thing. So, n i s t dot g o v, because it is a government organization slash a e s advanced encryption standard. This website gives the complete detail of the algorithm.

So, I am not going to go beyond that except to say that this is a new type of an algorithm which is in the horizon which is going to replace the triple DES.

(Refer Slide Time: 26:32)



Public Key Encryption

•In Private Key Encryption transmission of key without compromising not easy

•It is necessary to assign different private key to each business partner. When this is done a directory of keys should be kept which should be secret This is difficult

•Only secure way is to change the private key every time a message is sent

•Public Key Encryption eliminates the key distribution problem

13.3.29 Systems Analysis And Design © V. Rajaraman 81 of 153

Now, the public key encryption is somewhat different from the so far, what we have talked about is called a private key encryption. Because, the key is private to the crypto parties that is why I who de encrypt have a key and I had to make that key known to the recipient for them to able to decrypt. Transmission of the key without compromising the key that is without the key getting public is difficult.

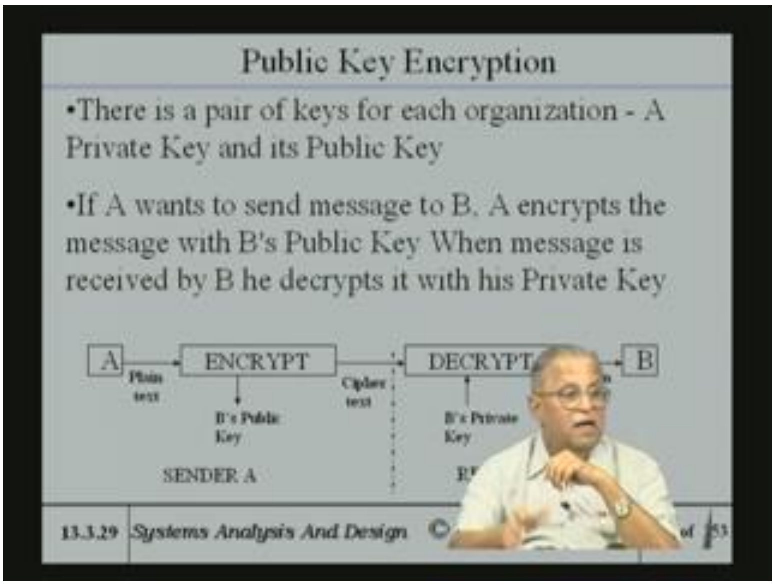
Because, if we send by e mail definitely somebody is going to get heard of it and so probably you should send it by some other mails by post or whatever. The other problem is for each partner you must have a different key. And so, you had to have a database of all your partners and all their keys and that can be called a horrendous thing. Suppose, you are having a huge number of partners to with whom you want to correspond.

Then the number of keys you had to maintain it can become very large. And it should not you cannot confuse one with the other. That should be extremely safely kept if that becomes public everybody is compromised. So, only way to make it absolutely secure is for every transmission use a different private key. And that can still be horrendous because every time use a different key.

The recipient should also know what key you are going to be using for what transmission. So, these are all the points with private key encryption. So, people were looking for newer methods which are somewhat which will eliminate this key distribution problem. It is a major impediment to the use of symmetric key encryption. And they came up they in fact to be (Refer Time: 28:32) of looking at this question for a lot of time. That is almost 56 years people have been searching for a solution.

To this key distribution problem and finding out some method of encryption, where key distribution is made unnecessary. And that there finally back around 80s, a method came out called the public key encryption method, which eliminates the key distribution problem.

(Refer Slide Time: 29:07)



Public Key Encryption

- There is a pair of keys for each organization - A Private Key and its Public Key
- If A wants to send message to B. A encrypts the message with B's Public Key When message is received by B he decrypts it with his Private Key

13.3.29 *Systems Analysis And Design* © … of 53

That is a tremendous advance in the area of cryptography. Now in the case of public key encryption, there is a pair of keys for each organization is each organization has only two keys. You do not have to maintain anything about anything like a table of keys. So, every organization has got only two keys; one they call the private key which they keep secret as it implies. The other is called the public key, public key is publicized to everybody where everyone knows their public key.

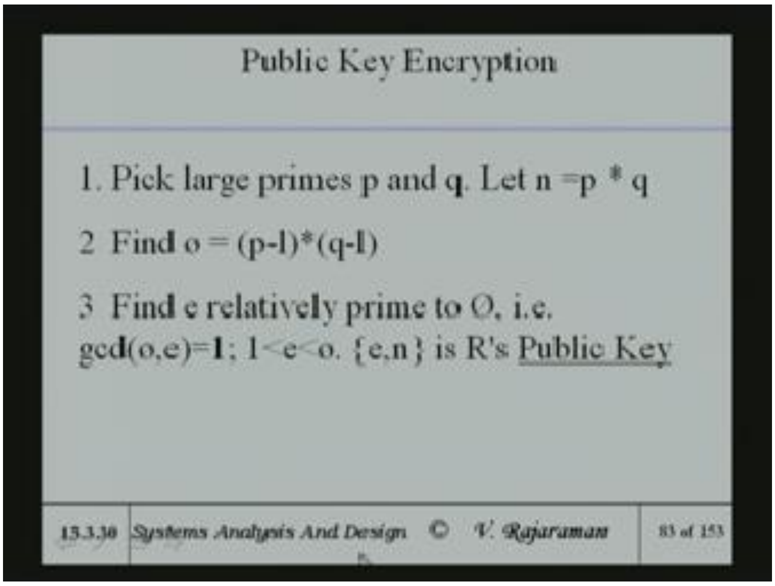
In others words you put it in a web site and if your website anybody wants to correspond with you. They look at out your website and know what your public key is. So, if you want to send an encrypted message to that that person whose public key I found out from the website you use his public key.

(Refer Slide Time: 30:13) Interrupt with you take your text and take the plain text and encrypt it with B’s public key. Because, B’s public key the recipient is the public key is known to you. So, you can encrypted it using that key. The encryption method is also publicized, what encryption is used? That is not secret only the private key is secret.

Now the when the cipher text goes to the recipient B. Now, what we can do is to decrypt it using B’s private key. And you get back the plain text. So, you can see the key distribution problem is completely eliminated. Because, what you do is you the public key of the recipient. You just use that public key and put. And then the recipients use this private key and decrypts. That is a straight forward a kind of a very interesting kind of symmetric method again.

Because, if you encrypt it your private key, you can decrypt it with public key of course,, that that is got a application in a digital signature, which we may look at later on. But when you want to send a message, you would normally use the public key of this person. Because, the persons is only intended recipients public key and then the recipient has his own key to decrypt. So, this is the very very simple idea.

(Refer Slide Time: 31:47)



Public Key Encryption

1. Pick large primes p and q. Let n =p * q

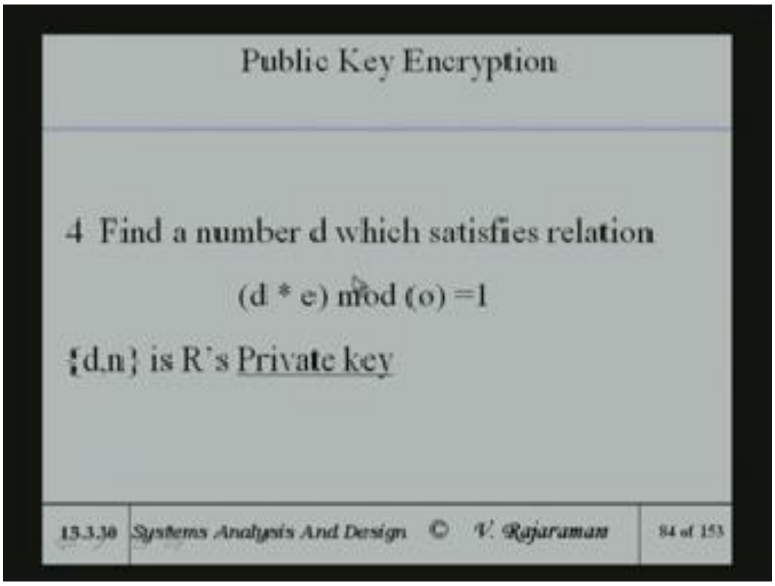
2 Find o = (p-1)*(q-1)

3 Find e relatively prime to O, i.e. gcd(o,e)=1; 1<e<o. {e,n} is R's Public Key

13.3.30 Systems Analysis And Design © V. Rajaraman 83 of 153

Now, the question is, how do you pick the two keys? And that also an algorithm is suggested from the straight forward pick two large prime numbers p and q. Let the n be product to these two primes. And find out p minus 1 times q minus 1 find the number phi, where find a number e relatively prime to phi. That is find out the gcd of phi and e. And now, you have take phi they have calculated it. And find out the value of e. So that, the gcd of phi e equal to 1. So now, that e is R’s public key.

(Refer Slide Time: 32:45)



Public Key Encryption

4 Find a number d which satisfies relation

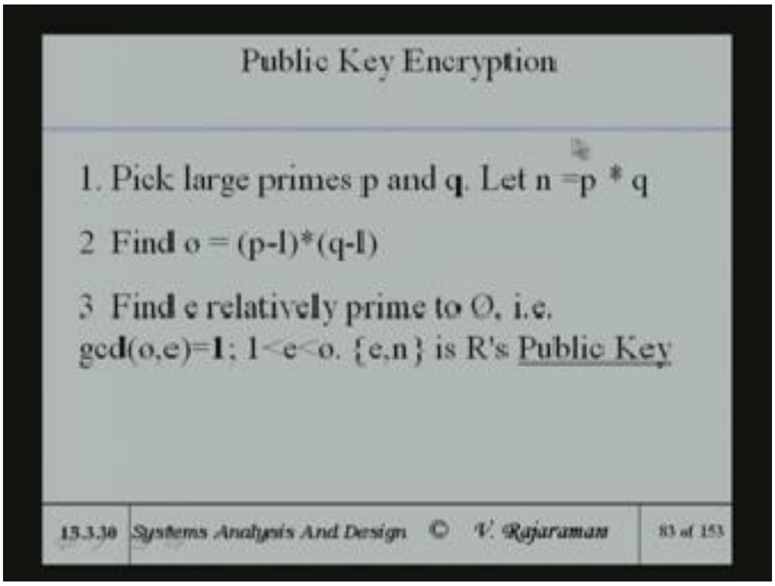
(d * e) mod (o) =1

{d,n} is R's Private key

13.3.30 Systems Analysis And Design © V. Rajaraman 84 of 153

So, we have to find out the number d which satisfies the relation d times e mod phi, phi is known is equal to 1. And d n is the R’s private. That is the tipple d n. And of course, is the part of d n that is known.

(Refer Slide Time: 33:00)



Public Key Encryption

1. Pick large primes p and q. Let n =p * q

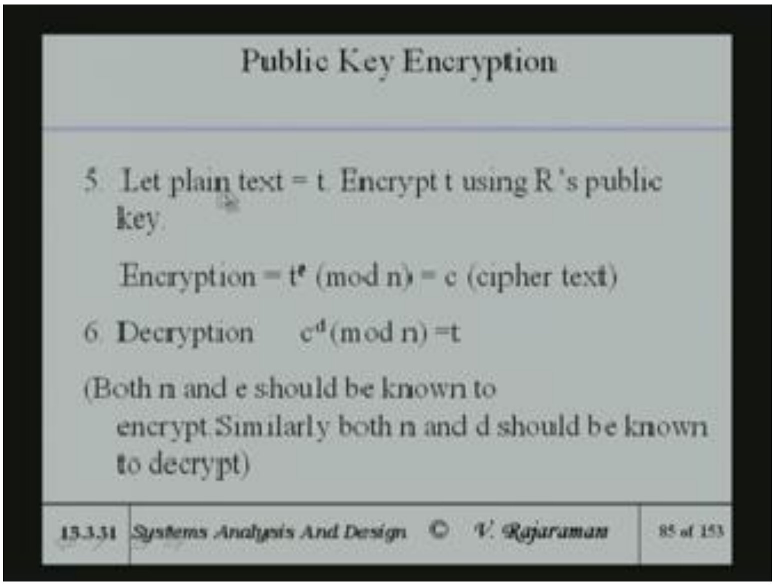
2 Find o = (p-1)*(q-1)

3 Find e relatively prime to Ø, i.e. gcd(o,e)=1; 1<e<o. {e,n} is R's Public Key

13.3.30 Systems Analysis And Design © V. Rajaraman 83 of 153

The individual primes are not known. Nobody knows p and q, but everybody knows the value of n and you (Refer Slide Time: 32:45) effectively can find out the d of course, is not known to anybody. Because, (Refer Slide Time: 33:00) have to find out (Refer Slide Time: 32:45) the public and private key pair is found out from the algorithm.

(Refer Slide Time: 33:25)



Public Key Encryption

5. Let plain text = t. Encrypt t using R's public key.

Encryption = t^e (mod n) = c (cipher text)

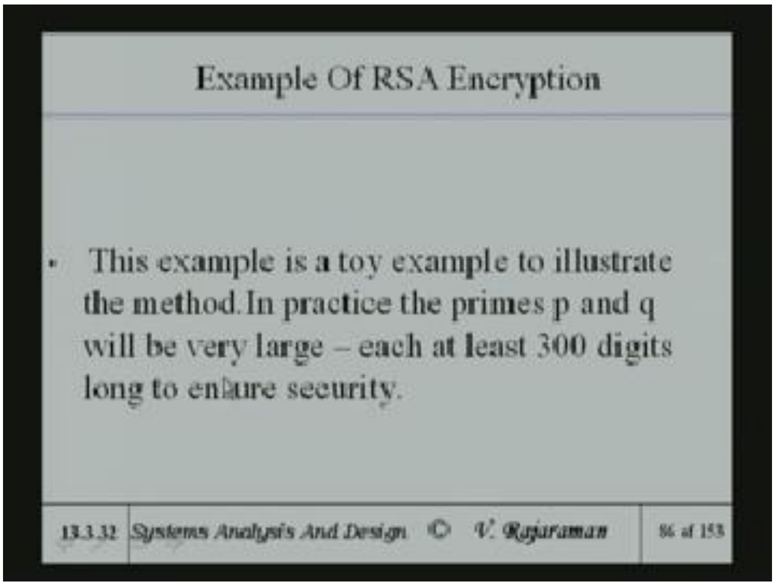
6. Decryption c^d (mod n) =t

(Both n and e should be known to encrypt.Similarly both n and d should be known to decrypt)

13.3.31 Systems Analysis And Design © V. Rajaraman 85 of 153

I will give an example of and now the steps in encryption and decryption. Let plain text be t encrypt t using R's public key t to the power e mod n is cipher text. Decryption is c to the power d mod n that is both n and e should be known to encrypt. Similarly both n and d should be known to decrypt n is known. The product is known the individual values are not known. So that is the whole idea.

(Refer Slide Time: 33:48)



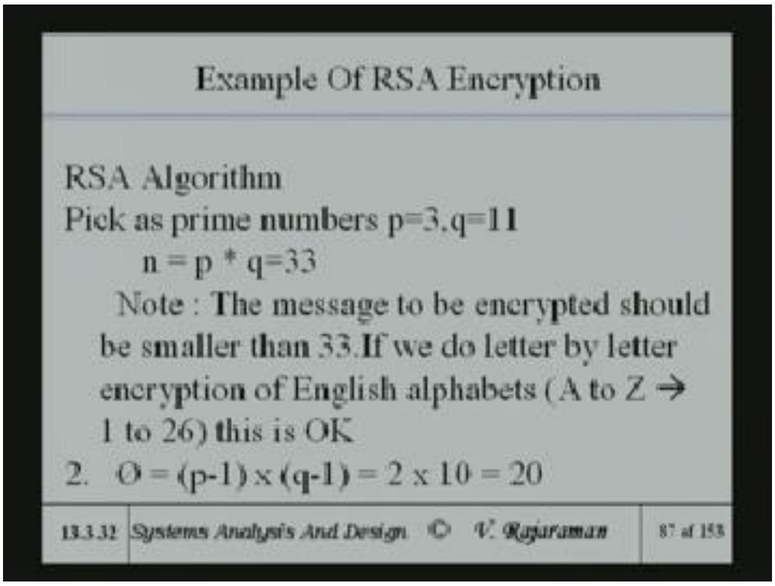
Example Of RSA Encryption

- This example is a toy example to illustrate the method.In practice the primes p and q will be very large – each at least 300 digits long to ensure security.

13.3.32 Systems Analysis And Design © V. Rajaraman 86 of 153

This example is a toy example, they had given a toy example to illustrate the method. In practice the primes p and q will be very large to ensure the actual good encryption. So, I will take a simple toy example to show how the algorithm works.

(Refer Slide Time: 34:08)



Example Of RSA Encryption

RSA Algorithm

Pick as prime numbers p=3,q=11

n = p * q=33

Note : The message to be encrypted should be smaller than 33.If we do letter by letter encryption of English alphabets (A to Z → 1 to 26) this is OK

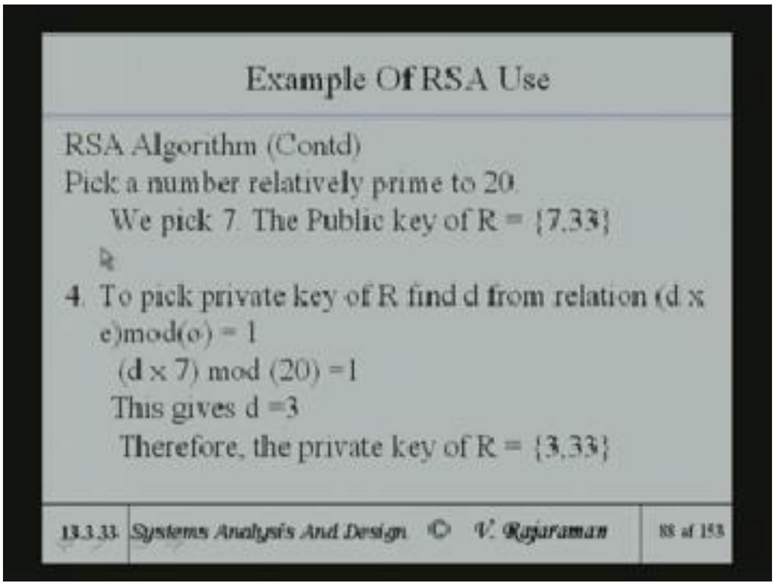
2. $\emptyset = (p-1) \times (q-1) = 2 \times 10 = 20$

13.3.32 | Systems Analysis And Design © V. Rajaraman | 87 of 153

So, this is called the RSA algorithm. See the RSA algorithm is known after the three people who together kind of invented this kind of this method. And so, it is commonly known as RSA algorithm, because its three people are working at MIT who invented this. So, pick and small prime numbers, because I can work them out. Very simply and the while going along, but actual in practice p and q are very large. So, pick as prime numbers some two prime numbers q is 11 and n is 33 of course.

The message to be encrypted should be smaller than 33. Because, if we do letter by letter encryption of English alphabets A to Z. I think this will work with A to Z, because each character is got to be encrypted with this. And the A to Z could be encrypted as 1 to 26 which is alright. Now, take phi as p minus 1 times q minus 1. So, p minus 1 is 2 and q minus 1 is 10 give get 20.

(Refer Slide Time: 35:29)



Example Of RSA Use

RSA Algorithm (Contd)

Pick a number relatively prime to 20.

We pick 7. The Public key of R = {7,33}

4. To pick private key of R find d from relation (d x e)mod(φ) = 1

(d × 7) mod (20) =1

This gives d =3

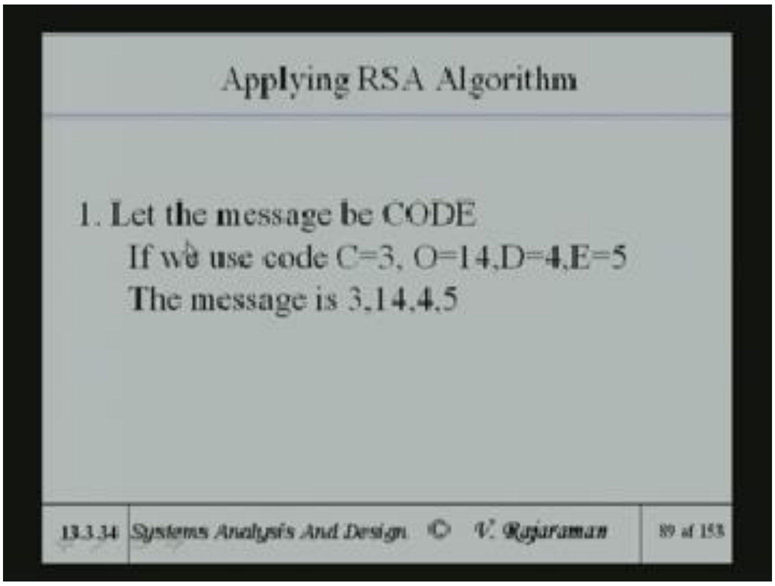
Therefore, the private key of R = {3,33}

13.3.33 Systems Analysis And Design © V. Rajaraman 88 of 153

And pick a number relatively prime to 20 that is 7 is not 20 cannot be divided by 7. So, public key of R is 7, 33. Pick a private key of R to find d from relation d times e mod phi equal to 1. So, d times 7mod twenty equal to 1 gives d equal to 3, 3 times 7 is 21 mod 20 is 1. So, the private key of R is 3,33. So, u can find out your private key and your public key. Each individual can find out his private and public key by picking some two large p’s and q’s.

And at least not values of p and q is not made this is made known to everybody known to anybody. So; that means, the public key is made known and, but this 3 is what is being important to us 3 is not made known. See the way, you calculated p is by knowing the value of p and q. And so that is the reason why the whole thing works, in other words the example exactly clarifies that the actual algorithm.

(Refer Slide Time: 36:39)



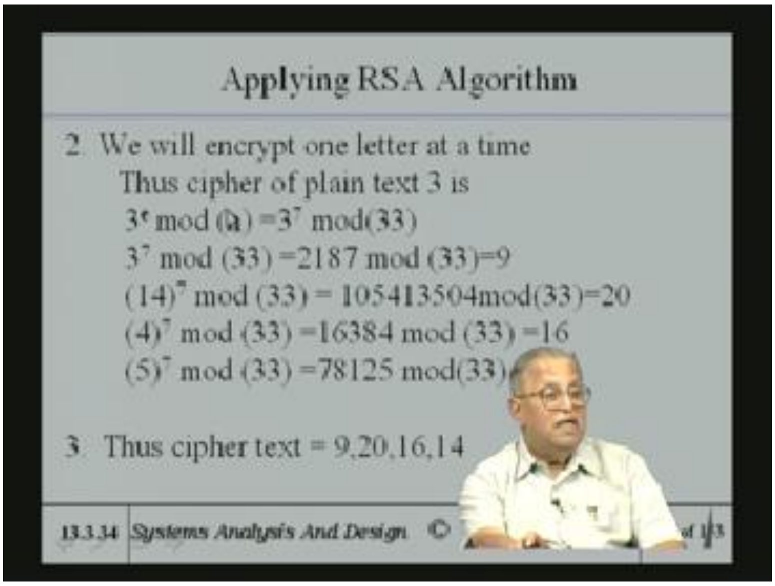
Applying RSA Algorithm

1. Let the message be CODE
   If we use code C=3, O=14,D=4,E=5
   The message is 3,14,4,5

13.3.34 Systems Analysis And Design © V. Rajaraman 89 of 153

So, now, this becomes you are so let the message be is CODE C A. If I use codes A equal to 1 B equal to 2 C equal to 3 and so on. C is 3, O is 14, D is 4, E is 5. The message is 3, 14,4, 5.

(Refer Slide Time: 36:57)



Applying RSA Algorithm

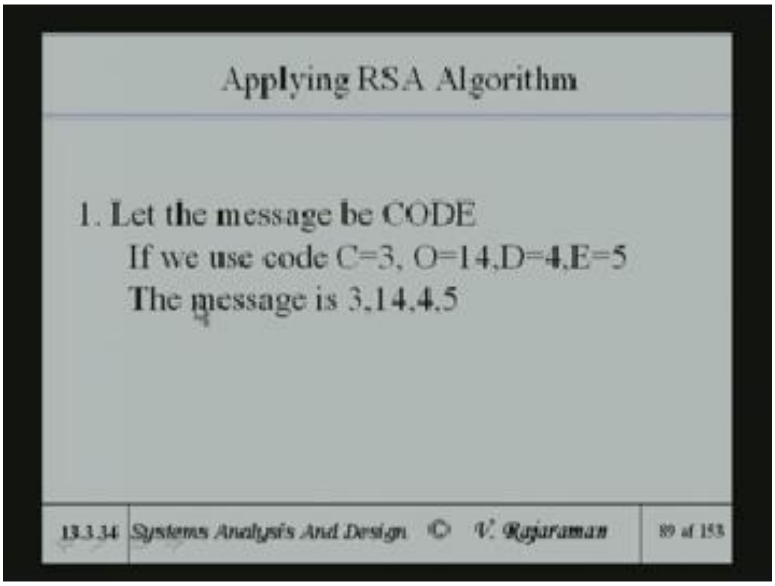
2. We will encrypt one letter at a time
   Thus cipher of plain text 3 is
   3^e mod (n) =3^7 mod(33)
   3^7 mod (33) =2187 mod (33)=9
   $(14)^7$ mod (33) = 105413504mod(33)=20
   $(4)^7$ mod (33) =16384 mod (33) =16
   $(5)^7$ mod (33) =78125 mod(33)

3. Thus cipher text = 9,20,16,14

13.3.34 Systems Analysis And Design © of 153

Now, I encrypt the message 3 to the power e mod n 3 to the 7 mod 33 is 2187 mod 33 is 9. 14 to the 7 which is the second digit mod 33 is this number 14 to the 7 is the large number mod 33 is 20. 4 to the 7 mod 33 is 16 and 5 to the 7 mod 33 is 14. So, cipher text is 9,20 16, 14 that is the input text was.

(Refer Slide Time: 37:32)



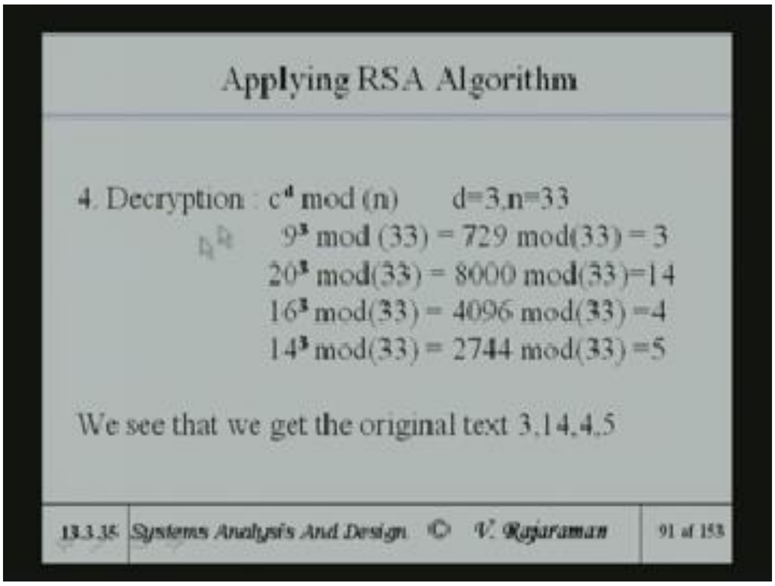
Applying RSA Algorithm

1. Let the message be CODE
   If we use code C=3, O=14,D=4,E=5
   The message is 3,14,4,5

13.3.34 Systems Analysis And Design © V. Rajaraman 89 of 153

It was I saw 3, 13, 4, 5 and output is (Refer Slide Time: 36:57) 9, 20, 16, 14.

(Refer Slide Time: 37:41)



Applying RSA Algorithm

4. Decryption : c^d mod (n) d=3,n=33

9^3 mod (33) = 729 mod(33) = 3

20^3 mod(33) = 8000 mod(33)=14

16^3 mod(33) = 4096 mod(33) =4

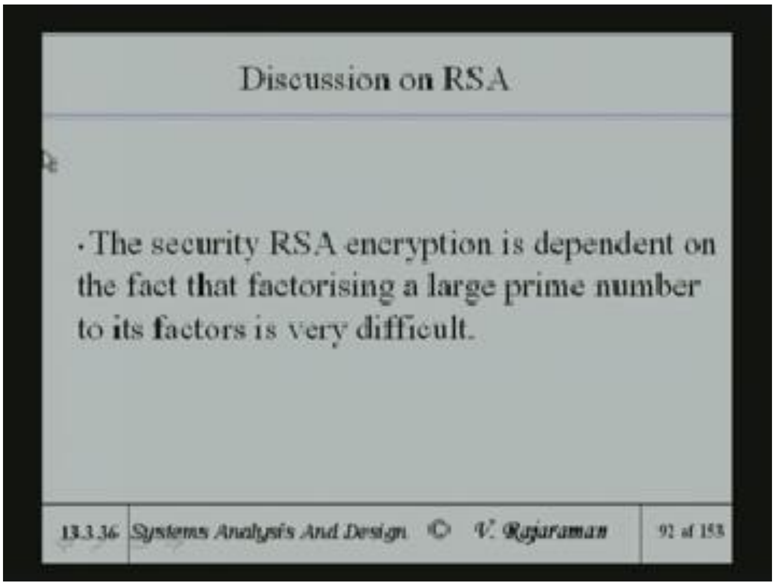
14^3 mod(33) = 2744 mod(33) =5

We see that we get the original text 3,14,4,5

13.3.35 Systems Analysis And Design © V. Rajaraman 91 of 153

Now the decryption is certainly straight forward. You take your public your private key is 3 and 33. So, it is 9 cubed mod 33 and it is 729 mod 33 given back 3 and 20 cube mod 33 you get 14, 16 cube mod 33, you get 4 and 14 cube mod 33 you get 5. So, we get the original text 3, 14, 4, 5.

(Refer Slide Time: 38:14)



Discussion on RSA

- The security RSA encryption is dependent on the fact that factorising a large prime number to its factors is very difficult.

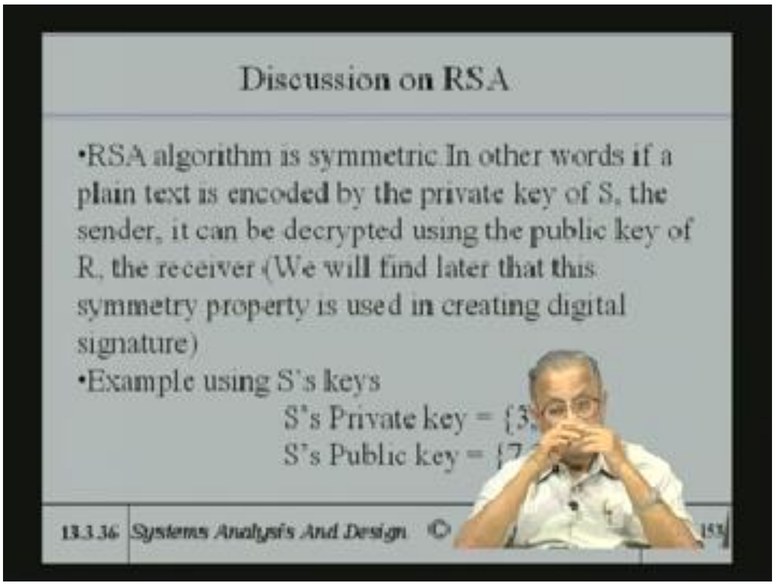
13.3.36 Systems Analysis And Design © V. Rajaraman 92 of 153

So, the simple idea is essentially to be able to encrypt with the public key as recipient. And the recipient decrypts it with your private key. So, each person has got a pair a public key and a private key. And each person finds out his own public and private keys by using the RSA algorithm. And because the security of the RSA encryption is depended on the fact that factorizing a large prime number to its factors is very difficult.

Because, the p and q are known to him and what he makes known to you is the product. If you find out the p and q from the product then you can use that algorithm to find out his private key. And that will identify the whole thing. So, the entire secrecy of the algorithm lies in the fact. That factorizing a large prime number which is a product of two primes into individual prime numbers to its factors, it is very very difficult.

It takes a long time it is not impossible, but if you use the brute force technique to do that it will take forever. That is the reason, why the primes, which are picked to make the product or the key something like may be some times 120 digit primes. So, very large primes and use very large primes to find out your public and private key.

(Refer Slide Time: 39:48)



Discussion on RSA

- RSA algorithm is symmetric In other words if a plain text is encoded by the private key of S, the sender, it can be decrypted using the public key of R, the receiver (We will find later that this symmetry property is used in creating digital signature)
- Example using S's keys

S's Private key = {3

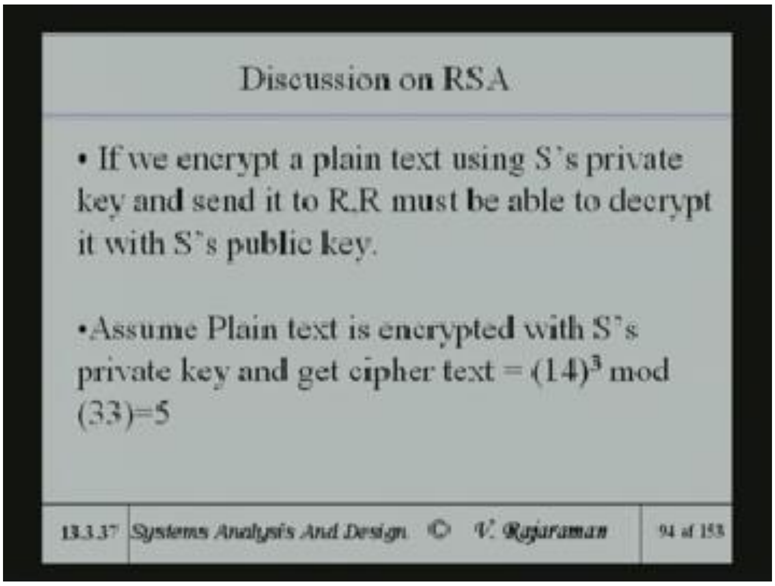
S's Public key = {7

13.3.36 Systems Analysis And Design © 153

And what it implies using very large primes? Is that the encryption time is going to become very large that is what I am going to explain. It says first of all its symmetric in other words in symmetric algorithm in the sense that the private and public key are interchangeable in that is in that sense.

In other words, if the plain text encoded with the private key of S. It can be decoded with the public key of R. This will find later on when I said for coding the digital signature digital signatures use effectively this idea.

(Refer Slide Time: 40:30)



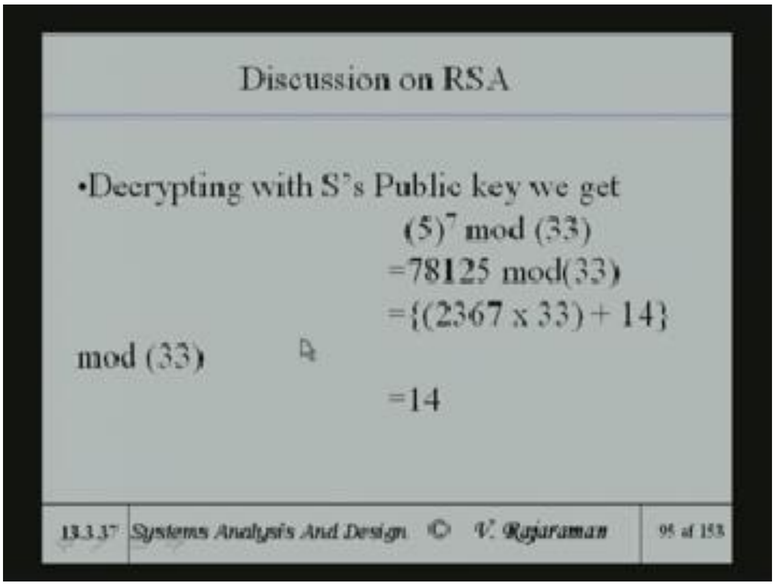
Discussion on RSA

- If we encrypt a plain text using S's private key and send it to R.R must be able to decrypt it with S's public key.
- Assume Plain text is encrypted with S's private key and get cipher text = $(14)^3$ mod (33)=5

13.3.37 Systems Analysis And Design © V. Rajaraman 94 of 153

As I pointed out 3 and 33, 7 and 33, which was found out that actually they found out. (Refer Slide Time: 39:48) A pair in the previous slides now I want to show the symmetric. See, encrypt a plain text using S S's private key and send it to R and R must be able to decrypt it with S's public key senders public key. Assume plain text is encrypted with S's private key and get a cipher text 14 cube mod 33.

(Refer Slide Time: 40:58)



Discussion on RSA

•Decrypting with S's Public key we get

$(5)^7$ mod (33)

=78125 mod(33)

={(2367 x 33) + 14}

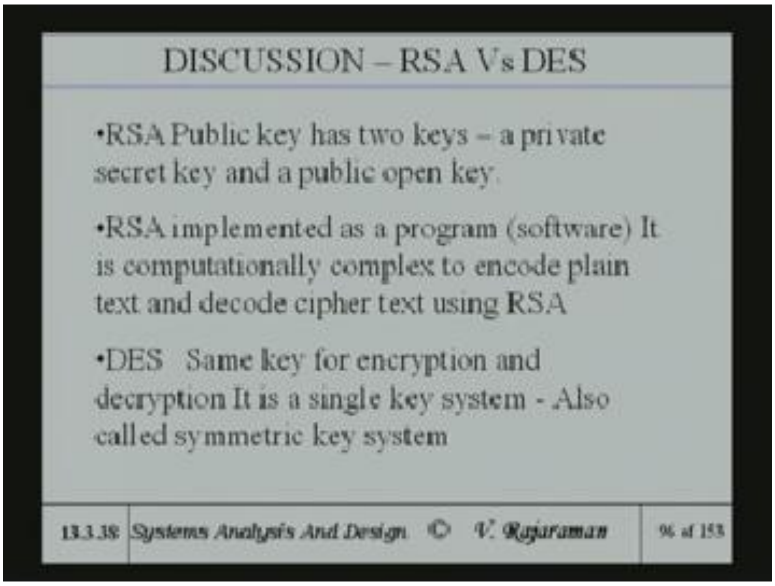
mod (33)

=14

13.3.37 Systems Analysis And Design © V. Rajaraman 95 of 153

Get back the 14 after applying the same algorithm over again 5 to the 7 mod 33. So, the point is that the private and public key is interchangeable in that sense. R is a public key it has two keys a private key and a public key.

(Refer Slide Time: 41:19)



DISCUSSION – RSA Vs DES

- RSA Public key has two keys – a private secret key and a public open key.
- RSA implemented as a program (software) It is computationally complex to encode plain text and decode cipher text using RSA
- DES Same key for encryption and decryption It is a single key system - Also called symmetric key system

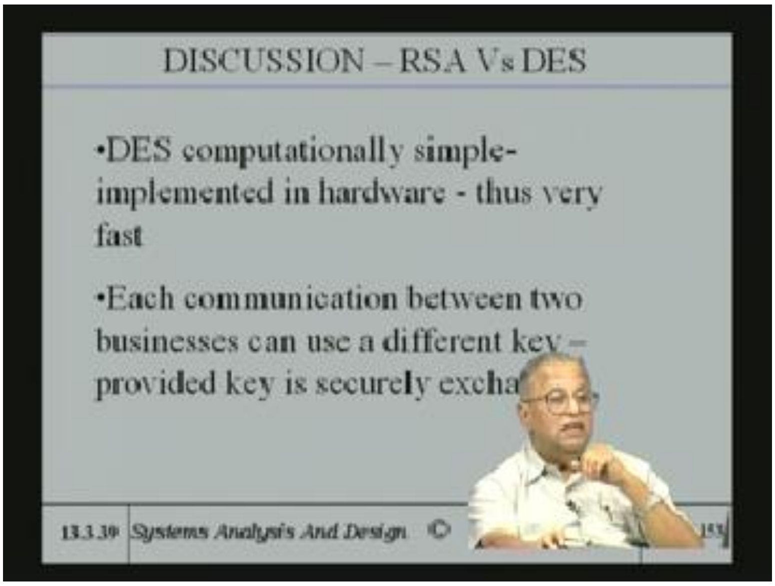
13.3.38 Systems Analysis And Design © V. Rajaraman 96 of 153

It is implemented in software, because it uses two large prime numbers. And the entire algorithm is as we saw requires a lot of arithmetic to be carried out on very large number of digits. So, hardware implementation our RSA algorithm is not very economically feasible. And because also, each receipt each person is going to you got a pair of private and public key is going to have a kind of a work with two large prime numbers which are arbitrarily picked nobody else knows.

So, to come up with a chip which will work arbitrary primes is very tough. And so, normally chips are not there, that is normally a software implementation. It is computationally complex to encode plain text and decode cipher text using RSA. Because of the large prime numbers, so it is implied in the software. And also because of the complexity of finding out the powers and then a finding out mod and all that is a very long process. So, the decryption does take a long time.

And DES on other hand is very fast even though the problem is the key distribution problem.

(Refer Slide Time: 42:58)



DISCUSSION – RSA Vs DES

- DES computationally simple-implemented in hardware - thus very fast
- Each communication between two businesses can use a different key – provided key is securely excha...

13.3.39 Systems Analysis And Design © 153

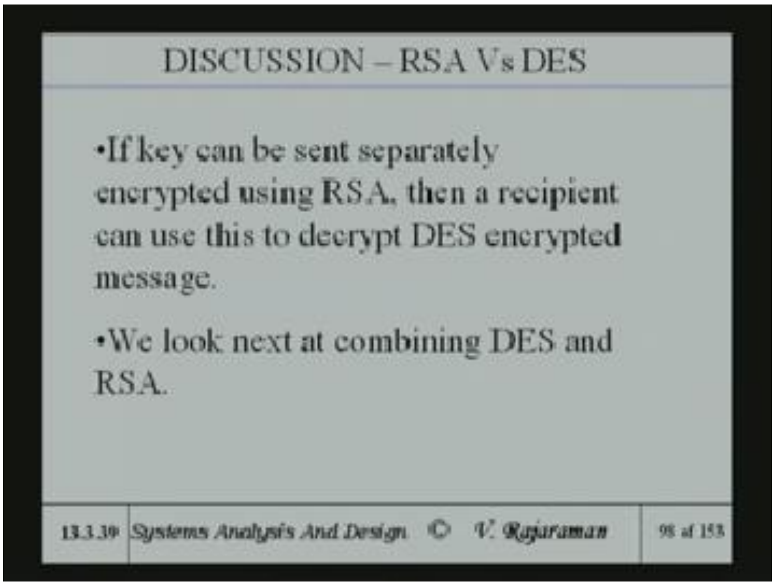
And so, RSA is that way. DES is completely simple and very fast and as I said you can implement in software and hardware. Each communication between two businesses can use a different key provided key is securely exchanged. In other words, the whole point is if you ask the question can we combine RSA and DES. In such a way that the advantage of DES in times of speed of encryption. And the advantage of RSA which is the load which is the need no the requirement of a transmitting key to a partner is unnecessary. These two are the two distinct advantages.

In DES, it is symmetric key very fast,, but you have you have key distribution problem. In RSA, it is again public key private key two everybody has got two keys public key is known to everybody private key is only known to you. And there is no need for key distribution problem, because public key is publicized to all. And the disadvantage is that it is slow. But, it is quite strong and the encryption method it is very strong.

So the question, which I have asked to the people is, can I marry DES and RSA. To retain certain advantages of DES namely speed and certain advantages of RSA which is that avoiding key distribution problem as I again pointed out earlier a DES algorithm will work very effectively. If I am used to if I am using different keys for different chunks and messages. So that even if an enemy is able to get hold of lots of chunks of messages. Because of being encrypted by different key in different times.

It will be extremely difficult for him to do brute force description, because he does not have enough samples to do a brute force decryption. So, this is the question which is raised and the answer is fortunately is DES, you can marry the two.

(Refer Slide Time: 45:18)



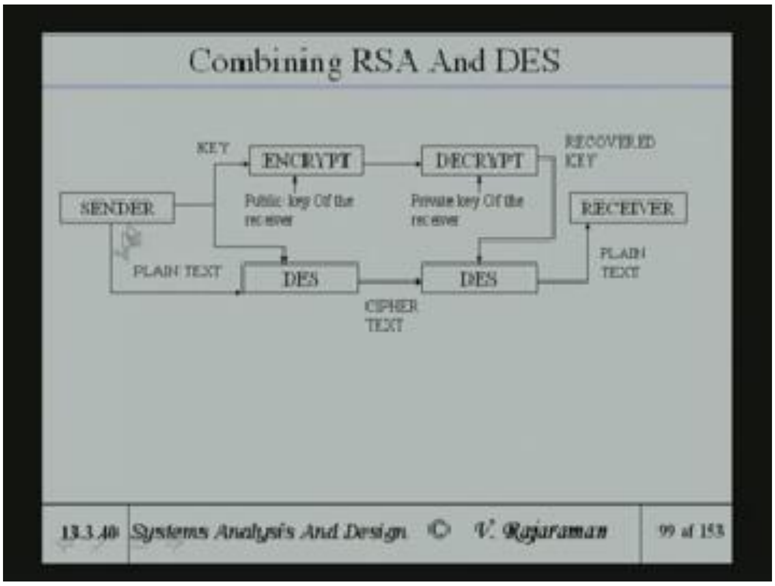
DISCUSSION – RSA Vs DES

- If key can be sent separately encrypted using RSA, then a recipient can use this to decrypt DES encrypted message.
- We look next at combining DES and RSA.

13.3.39 Systems Analysis And Design © V. Rajaraman 98 of 153

And I will see how this can be done by looking at this very simple picture.

(Refer Slide Time: 45:22)



Combining RSA And DES

13.3.40 Systems Analysis And Design © V. Rajaraman 99 of 153

Now the sender, if he wants to send a long plain text, what he does is, he sends the key, because the key the problem of this one is the key distribution problem. So, surviving a key distribution problem, where you keep both of the keys and so on. You pick an arbitrary key and use that arbitrary key and encrypt that key using RSA. Because, the key is a very not a very large number and only one number one single number, the encryption even though the software will be very fast.

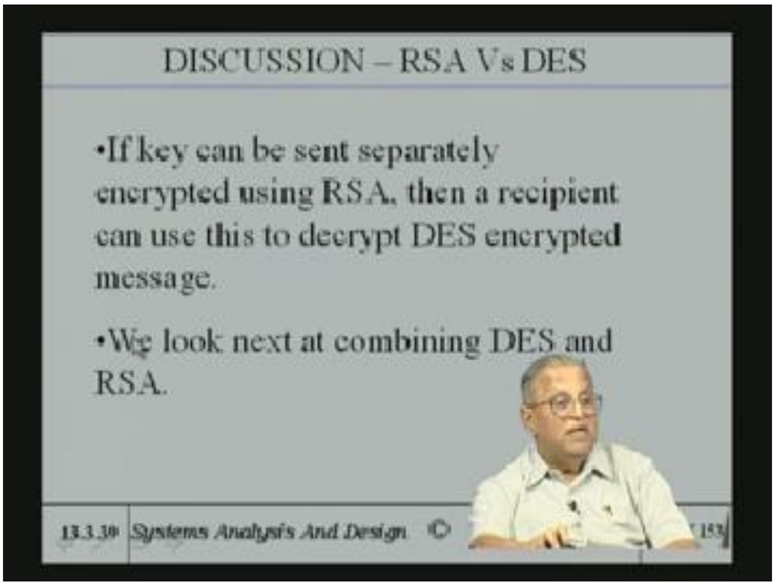
So, you do an encryption of the key using the public key of the intended recipient receiver. And you send it, the receiver can decrypt it using it is own private key and get hold of the key. The key distribution problem is somewhat solved besides that the keys sent using RSA. And for every different plain text, I can send a different key. And now the plain text using the same key is encrypted with this. And because this person knows the key he can decrypt it using a DES chip.

So now, the plain text can be a very long plain text and because the key is going to change from each plain text to the next plain text the receiver the reason with security in the, which resides in the key. So, the person who is trying to kind of break your code will find it difficult to break the code further if I use triple DES here is almost impossible to use it to break. The key distribution problem is completely eliminated.

But of course, one question you can ask is if the plain text is very long may be the enemy can kind of look at this long one and cut it up into pieces. And try to kind of guess the keys. Because, he has got enough of things, what you can do is cut up the plain text into different parts and for each part it may not be 64 bit. But may be 640 bits and for each 640 bits.

You can use a different key that way, it is almost impossible for the person to kind of decrypt it. So, the most interesting part is that this is RSA in which the key distribution is done by RSA. The encryption is done by a fast hardware and so you are able to combine the advantages of this. And the advantages of this to get a hybrid you might say hybrid method which is quite secure.

(Refer Slide Time: 48:29)

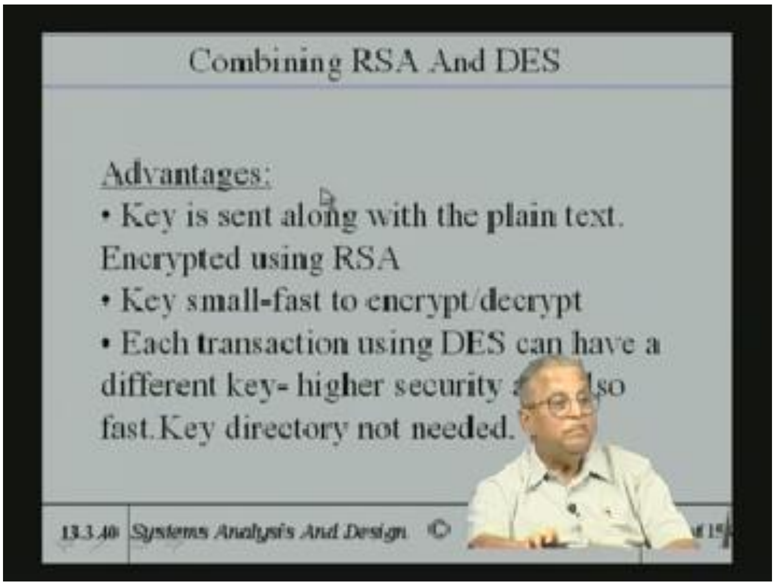


DISCUSSION – RSA Vs DES

- If key can be sent separately encrypted using RSA, then a recipient can use this to decrypt DES encrypted message.
- We look next at combining DES and RSA.

That is recently, what we you have, seen the key can be sent separately encrypted using RSA. Then, a recipient can use this to decrypt DES.

(Refer Slide Time: 48:40)



Combining RSA And DES

Advantages:

- Key is sent along with the plain text. Encrypted using RSA
- Key small-fast to encrypt/decrypt
- Each transaction using DES can have a different key- higher security also fast.Key directory not needed.

You look that is what is being done by combining and main advantages I already pointed out. Key is sent along with the plain text encrypted using RSA. Key is small fast to encrypt and decrypt. Each transaction using DES can have a different key, higher security and also fast, key directory is not needed. So, these are all the advantages which a grow because of the fact that the I am able to combine both of them.

Of course, this is as far as the encryption issue is concerned. To very quickly kind of do a review on what I have said, because I probably went a little fast in these transparencies. But, it would be very quickly kind of recapitulate, what we had done, what we started off with was that, we started off with a symmetric key encryption.

Using a digital encryption, what I would say is digital encryption standard d e s DES and when we use a digital encryption standard. I said that the standard uses a 56 bit key cut up the messages into 64 bits encrypts in 64 bit message with a 56 bit key by using a very complex permutation dropping and left right interchange and some exclusive oaring and so on.

Primarily it is a combination of what is called permutation and transposition that is what it did. And what we found out was that DES applies the same algorithm 16 different times, such a way as to kind of improve the security. In spite of that, because of the fact that brute force techniques can be used to find out the key it and with its increase in speed in computers, you can guess the key in reasonable time.

A single DES which is being great advantages are you can put in hardware has been found not very useful. So, one went for a triple DES for the same DES algorithm is applied 3 times over. And this gives you security, which is very good. Because brute force techniques, we take where ever to decrypt. Here three different keys are used and three steps are used encryption decryption encryption.

Because, DES is symmetric, the triple DES is also symmetric. That is the reason, we used E D and K. And at the end of that, we said that triple DES is very very secure; however, still it has got the problem of key distribution. Key distribution is a major difficulty with any symmetric key encryption system. So, people searched for newer methods and in newer methods were key distribution problem was got to be eliminated.

The key distribution problem is eliminated by an algorithm called RSA algorithm. The RSA algorithm uses a method where by encryption is done with a public key of a recipient which is made public. And the recipient decrypts it using its own private key. Because, this private key is known only to this person, there is no public key distribution.

Because, anybody who wants to send a message to you can use the public key which is found in your web site and when you receive the message you can decrypt it using your own private key. So, key distribution problem is eliminated. But, the disadvantage is the RSA algorithm depends on its security depends upon the fact that two long large prime numbers.

The product of two large prime numbers, which is made public as part of the public key. The public key consists of two digits one is the product of two prime numbers. And the other is the public key which is determined from the values of primes by the person who is created in his public key. We know an algorithm which uses finally, straight forward arithmetic gcd mod and things like that.

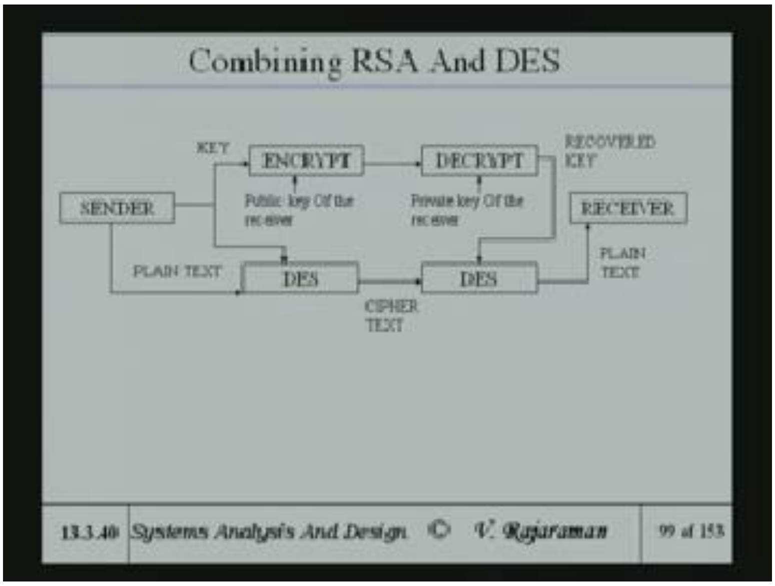
And so, one can use that algorithm the algorithm is made public. Only the prime numbers are not made public. So, prime numbers are secret with you and you create your public key private key pair which consists of each key consider of a pair, n and some key called E which may be which is your public key. And n another number called d you might say arbitrarily, which is your private key n d you keep it to yourself and E you make known to the two public.

Now, what you do is having publicized this. You anybody can kind of send a message to you using the RSA encoding and you can decrypt. However, the negative point is applying the RSA algorithm requires a far amount of arithmetic calculations with large primes, it is very difficult to implement in hardware. So, it is a software method. The software method also is very slow, because for that numbers are very large. But still, the greatest advantage of that is the elimination of the key distribution problem.

So now, you got the RSA, where everybody has got a private key public key pair. You have got a very nice method of exchanging messages without any possibility of some somebody else find again it has been found that the security lies in the prime numbers. So, you pick up very long prime numbers security lies in the fact that it is impossible to factor a product of two primes, what I mean by impossible is that, brute force technique will take forever to do the factoring.

You require a very very fast machine and it will take years to use if you brute force. And that is the reason, why it is considered quite secure. The longer the prime number, you pick the more secure is the RSA code. Because of the fact that it is software implementation, you ask the question, can I combine hardware implementation which is fast with the software implementation which is slower. But it can be tolerated, if it is used with a very small number.

(Refer Slide Time: 57:17)



Combining RSA And DES

13.3.40 Systems Analysis And Design © V. Rajaraman 99 of 153

And that is how where we came up with this idea of combining both we said that the key is very small one it is known by a tipple two digits. So that, key can be encrypted with RSA. And the time taken to encrypt will be very small. And the key distribution problem is eliminated, because the key which is I am going to encode is the one which is being sent by RSA.

So, the recipient is of course, using RSA can find out the key and I using the same key for encrypting using DES. And one because, I am changing the key for every different message, even if DES is weak one cannot actually decrypt it easily in triple DES it is strong in any case. So, the hardware is very fast. So, plain text can be very long plain text will be sent very fast and keys changed for every different every plain text.

And so, you got a very very nice marriage between RSA and DES. And DES, you have very secure method without having the disadvantage of key distribution. Now then, RSA is also symmetric, just like DES is symmetric. The symmetry of RSA can be used very effectively in what is known as digital signature. And I will talk about digital signature in certain amount of detail next time, because digital signature is very important in electronic commerce. So, I will stop at this point and carry on with talking about digital signature next time.