

**Demystifying networking**  
**Prof. Sridhar Iyer**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Bombay**

**Lecture - 72**  
**Secret of the Secret Box**

Welcome back to the course. So, this week what you saw was Aditi and Balraj with the Secret Box. Now what was very peculiar about the secret box was it could be closed with one of the keys and opened with the other. So, now, let us look at how can we use this to communicate secretly between Aditi and Balraj; what do you say?

Right. I think many of them have guessed rightly that Aditi would choose a pair of code and then keeps one to herself and shares other with everyone else and Balraj does the same.

Yes.

And if Aditi wants to send a message to Balraj, she locks it with the code that Balraj has shared with everyone and then sends it to Balraj. Balraj uses his own code which he has kept with himself to open that message.

Right. So, we could actually give them these code some name like we could call the code that they share with each other something like a public code. So, if they are if so, the idea is if Aditi wants to send a message to anyone, she could just give out her public code.

Right.

They could lock the message with that. So, that only Aditi could open it.

Right this also resolves the problem that if there is only one code which is shared with anyone everyone and then it is also used to open the message, it is, it can be leaked or it can.

Yes.

To used to used by others. So, this pair of codes would resolve that problem.

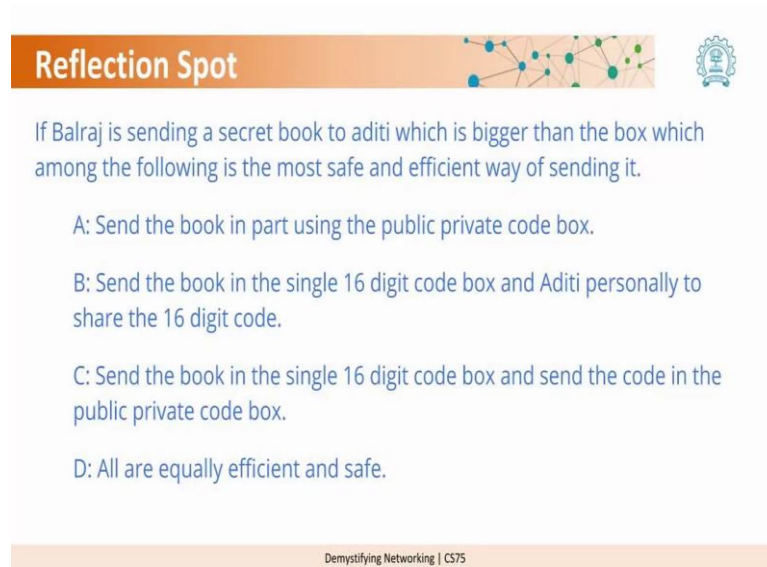
I agree, I totally agree.

I think this is a right time for a reflection question right.

Yes.

So, what we want you to do is pause and read the question, take your time to answer and then proceed.

(Refer Slide Time: 01:59)



The slide features a title bar with the text "Reflection Spot" in white on an orange background. To the right of the title bar is a network diagram with blue and green nodes and lines, and a small circular logo with a gear and a person icon. The main content area has a light blue background and contains the following text:

If Balraj is sending a secret book to aditi which is bigger than the box which among the following is the most safe and efficient way of sending it.

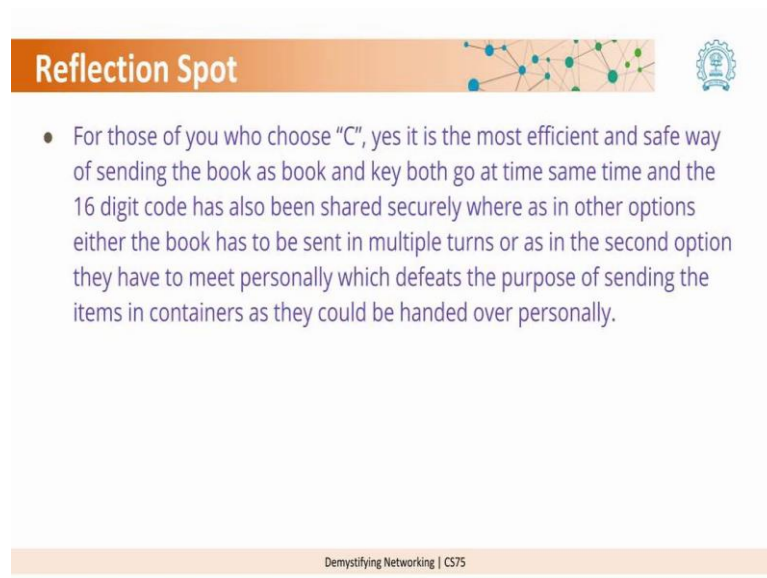
- A: Send the book in part using the public private code box.
- B: Send the book in the single 16 digit code box and Aditi personally to share the 16 digit code.
- C: Send the book in the single 16 digit code box and send the code in the public private code box.
- D: All are equally efficient and safe.

At the bottom of the slide, there is a footer bar with the text "Demystifying Networking | CS75" in a small font.

Here is your question. If Balraj is sending the secret book to Aditi which is bigger than the box, which among the following is the most safe and efficient way to sending it. Option A, send a book in part using the public private code box.

Option B, send a book in the single digit 16 code box and Aditi personally to share the 16 digit code. Option C send a book in the single digit 16 digit code box and send the code in the public private code box. Option D all are equally efficient and safe.

(Refer Slide Time: 02:43)



The slide features a header with the text "Reflection Spot" in white on an orange background. To the right of the header is a network diagram with blue and green nodes connected by lines, and a circular logo with a gear and a book. The main content is a bulleted list. At the bottom, there is a footer with the text "Demystifying Networking | CS75".

**Reflection Spot**

- For those of you who choose "C", yes it is the most efficient and safe way of sending the book as book and key both go at time same time and the 16 digit code has also been shared securely where as in other options either the book has to be sent in multiple turns or as in the second option they have to meet personally which defeats the purpose of sending the items in containers as they could be handed over personally.

Demystifying Networking | CS75

Those who choose C yes it is the most efficient and the safe way for sending the books as the book and the key go both at the same time. The 16 digit code has also been shared securely whereas, in the other options either the book has to be sent in multiple turns or as in the second option, they have to meet personally which defeats the purpose of sending the item in containers as they could be handed over personally.

So, now you have seen the analogy and what we saw there was that when Aditi and Balraj wanted to communicate with each other and they wanted to do it secretly that to use some mechanisms. So, something similar happens over the internet.