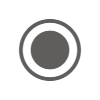
**3.Introduction to Cryptography II**

August 13, 2023, 12:27PM

2h 10m 49s

 **ASHUTOSH BHATIA .** 0:03  
All immediately, I think today or tomorrow.

 **ASHUTOSH BHATIA .** started transcription

 **ASHUTOSH BHATIA .** 0:06  
Tomorrow, possibly or in the not two days I'm going to provide you the first assignment on sniffing and spoofing.

 **CHITHIRALA HEMANTH GUPTA .** joined the meeting

 **MS TEAMS ONLINE LECTURES** left the meeting

 **ASHUTOSH BHATIA .** 0:17  
OK.  
So your first assignment on the same machine you will get.  
You have to run those experiments.  
Whatever is given in assignment, generate the results.  
Create your report and you probably have to submit it.  
That will be through your elearn.  
Uh, so that assignment will come to you through 11 only, OK?  
So now let's uh, where is the pen?

 **RAVISRI VENKATA RAMANA LANKA .** 0:45  
It's not before we start.  
Just a quick question.  
Person who says he is able to do it right can can I request him or her to take screenshots and share it for the wider audience because at least me I'm I'm not.

 **ASHUTOSH BHATIA .** 0:48  
Who?  
Umm.  
Yeah.  
Yeah, please, I think yes, yes, yes.

 **GANESH NAGA RAJESH H .** joined the meeting

 **RAVISRI VENKATA RAMANA LANKA .** 0:56  
I'm not a I'm not a technical guy, right?

 **ASHUTOSH BHATIA .** 0:57  
I was actually also also thinking I was also thinking the same that those who have done it, please share your screen through the Microsoft team.  
So can we do it right now if if anybody can just show it to this before moving?

 **RAVISRI VENKATA RAMANA LANKA .** 1:09  
Yeah, with the help.

 **ARUN R .** 1:15  
I'll share it.  
So just one moment, my realm is booting up.

 **ASHUTOSH BHATIA .** 1:17  
Yeah.  
Yeah. Umm.

 **THIYANESWARAN M .** joined the meeting

 **ASHUTOSH BHATIA .** 1:22  
So by that time, let me just uh share my screen.

 **JADHAV PRAJYOT SANJAY .** joined the meeting

 **TISMON VARGHESE .** joined the meeting

 **RAVISRI VENKATA RAMANA LANKA .** 1:30  
And so while you're sharing your screen, just a quick question, how much technical will this assignments be?  
Because I I'm a non technical person, right?  
I'm trying to learn, but how technical will it be?

 **ASHUTOSH BHATIA .** 1:39  
Everything, everything is distributed.  
It's like like learning how these things work, correct?  
So whatever technical knowledge you need, you just write me to me.

 **RAVISRI VENKATA RAMANA LANKA .** 1:45  
OK.

 **ASHUTOSH BHATIA .** 1:51  
And if that means technical means, any background knowledge is required to understand what's is happening, you just you can reach to reach out to me, but it is more about doing So what I can say teach you what?

 **RAVISRI VENKATA RAMANA LANKA .** 1:58  
Like.  
OK.  
Good.

 **ASHUTOSH BHATIA .** 2:05  
What I can tell you about this flipping and spoofing?  
OK, think it like this.  
Whenever.  
So let let me just share my screen and let me give it background a little bit.  
Networking background to everybody to carry out this experiment, OK.  
Uh before that?

 **ARUN R .** 2:23  
So my V Ms started, should I share my screen or can I put a screenshot of that image?

 **ASHUTOSH BHATIA .** 2:29  
No, no.  
You just take that, take the screenshot and put it on the, put it on the, paste it on here the Microsoft team.

 **ARUN R .** 2:32  
OK, sure.  
OK, Sir.  
OK, Sir.

 **K AKASH .** 2:38  
Uh.  
Similarly, Sir, I have one question I'm I mean, after very long, almost 1011 years I'm into this Linux and so for this what resources would you recommend at what level of Linux I should be aware?

 **ASHUTOSH BHATIA .** 2:42  
Uh-huh.  
Mm-hmm.

 **K AKASH .** 3:06  
Hello.  
Am I audible, Sir?  
Hello.

 **M DURGAPRASAD .** 3:17  
It's not that you are audible, but.

 **ASHUTOSH BHATIA .** left the meeting

 **NIHAL PRAKASH .** left the meeting

 **SOMNATH CHATTERJEE .** 3:29  
I just said got disconnected.

 **K AKASH .** 3:31  
OK.

 **THARUNKANTH D .** 3:33  
Yeah, let's wait.

 **SOWMYA N SWAMY .** 3:38  
So quick question guys.

 **M CHETHANA** left the meeting

 **SOWMYA N SWAMY .** 3:39  
So in the meantime, the person who was trying to show us, right.  
So can you just tell us so that we'll also try a live till the times are joins so you have to copy paste the script, is it to our VM machine?

 **K AKASH .** 3:44  
Yeah.

 **NIHAL PRAKASH .** joined the meeting

 **ARUN R .** 3:51  
Yeah, the.  
Yeah.  
Yes you you can go to that GitHub page.  
Just open that GitHub page.

 **ASHUTOSH BHATIA .** joined the meeting

 **ARUN R .** 3:59  
You'll get a raw file, so just create.

 **SOWMYA N SWAMY .** 4:02  
Once again, one no one second Somnath.

 **ARUN R .** 4:03  
I mean copy paste that.

 **SOWMYA N SWAMY .** 4:06  
So, Sir, Sir has passed that script in the source code folder, right?  
Are you talking about that?

 **ARUN R .** 4:12  
No, I think that was that in the chat.

 **ASHUTOSH BHATIA .** 4:16  
Source code folder I had created but I did not put it there.

 **ARUN R .** 4:16  
Let me.

 **NEERAJ KUMAR VIJAY .** 4:18  
You, you. You.

 **SOWMYA N SWAMY .** 4:22  
No, basically, from where should we take the script as as my question?

 **NEERAJ KUMAR VIJAY .** 4:22  
Uh.

 **ASHUTOSH BHATIA .** 4:26  
And there there, there is a there is a am I audible?

 **THARUNKANTH D .** 4:27  
At 1:40 PM, council.

 **SHYAMSUNDAR DAS .** 4:30  
But I have shared once again so that I hope this is the link right guys.

 **THARUNKANTH D .** 4:32  
Yes, Sir.

 **LOKESH BABU S .** 4:36  
Yes, that yes, yes, that's the late I mean.

 **SHYAMSUNDAR DAS .** 4:36  
GitHub sit labs.  
Yeah.  
Yeah.  
So after that, yeah, after we visit this link then what can you please say that what to do next?

 **NEERAJ KUMAR VIJAY .** 4:41  
So.  
Uh, I just pasted the command and it will.  
It will run this.

 **LOKESH BABU S .** 5:01  
I mean.

 **ASHUTOSH BHATIA .** 5:01  
OK.  
Am I audible?

 **K AKASH .** 5:04  
Yes Sir. So.

 **SOWMYA N SWAMY .** 5:05  
Yes, Sir.

 **JAGADEESAN P .** 5:05  
Yes, Sir.

 **ASHISH KUMAR BHATTACHARYA .** 5:05  
Yes, Sir.

 **JAGADEESAN P .** 5:05  
You are audible.

 **ASHUTOSH BHATIA .** 5:06  
OK. OK.  
So source code folder I had created but I did not put the code there.

 **ROHITH N V .** joined the meeting

 **SOWMYA N SWAMY .** 5:13  
No. OK.

 **ASHUTOSH BHATIA .** 5:13  
You can either download it from the link, that means just click on that and then just store that and then dot TSV file and return it within your VM machine.  
To run it, you just write bash and then the SH file.  
That's all.

 **SOWMYA N SWAMY .** 5:31  
So quick question here.

 **JAGADEESAN P .** 5:32  
But.

 **SOWMYA N SWAMY .** 5:32  
So.  
So which NEERAJ has pasted here right that HD app is rocked it fingerprint dot SH so.

 **LOKESH BABU S .** 5:38  
No, no, no, no, no, that's not the file.  
There is only one file in the file folder which Sarah has kept which is called VM fingerprint F dot SH.

 **M CHETHANA** joined the meeting

 **LOKESH BABU S .** 5:48  
That's the file you have to download and you have to run it.

 **SOWMYA N SWAMY .** 5:49  
That's.  
Correct.

 **NEERAJ KUMAR VIJAY .** 5:51  
No.

 **SOWMYA N SWAMY .** 5:52  
That's what.

 **NEERAJ KUMAR VIJAY .** 5:52  
Uh, just not.  
This is the file I got it from the link.  
Is pasted so uh.

 **SOWMYA N SWAMY .** 5:59  
The to rule out this.

 **JAGADEESAN P .** 5:59  
So this VM fingerprinter dot such is available in source code.  
Also, you could see in teams source code.

 **SOWMYA N SWAMY .** 6:04  
It Sir.

 **LOKESH BABU S .** 6:05  
Yeah, that's right.

 **HEMANT KUMAR SINGH .** joined the meeting

 **LOKESH BABU S .** 6:06  
That's what I'm telling.  
It's available in the source code folder.

 **JAGADEESAN P .** 6:08  
OK, OK.

 **SOWMYA N SWAMY .** 6:09  
Yeah, that's what I was trying to ask.  
So is that the right thing?  
What we are trying to do, Sir, is.

 **ASHUTOSH BHATIA .** 6:14  
Yeah, I see the problem with the the source code folder file is.  
It has dot TXT extension by default.  
OK, So what you have, you'll have to remove that.

 **LOKESH BABU S .** 6:23  
Yes.  
I we we just have to move that, yeah.

 **ASHUTOSH BHATIA .** 6:27  
So those who are not techies and that's why I was thinking that I just avoid that.  
But seeing you just download it and then remove it dot TXT because if you are doing in Windows automatically it takes it dot TXT extension.  
You have to remove that task TXT extension and then whatever name you want to give your name dot SH or doesn't matter.  
You just run that dot TSV file into the VM machine.  
OK, is my street.

 **NEERAJ KUMAR VIJAY .** 7:00  
Send me share.  
Shall we share the screen?  
What in the output to show or it's fine?

 **ASHUTOSH BHATIA .** 7:06  
Yeah, whoever has done it, please share so that others can see.  
And if you can show the process.

 **LOKESH BABU S .** 7:11  
Yeah, I can show that, Sir, but I'm not able to.

 **NEERAJ KUMAR VIJAY .** 7:13  
I. How much?

 **LOKESH BABU S .** 7:14  
I don't have access to share the photo.  
Share the screen, yeah.

 **NEERAJ KUMAR VIJAY .** 7:16  
Yeah. OK.

 **SOWMYA N SWAMY .** 7:17  
I I, Sir, I think you have to make that person as a presenter I guess.

 **ASHUTOSH BHATIA .** 7:18  
OK.  
OK, let me just try because this is important for everybody. Ohh.

 **LOKESH BABU S .** 7:28  
Then I can show how I give them.

 **NEERAJ KUMAR VIJAY .** 7:29  
Give me access, Sir. Need.

 **ASHUTOSH BHATIA .** 7:33  
OK, need it and Everly?

 **SOWMYA N SWAMY .** 7:34  
Yeah, both.  
Yeah, you can give it to NEERAJ as well.

 **ASHUTOSH BHATIA .** 7:38  
There are so many needed.

 **NEERAJ KUMAR VIJAY .** 7:40  
Needed she will Kumar, Vijay.

 **ASHUTOSH BHATIA .** 7:42  
OK.  
For more visit what should I do I should say?

 **KAVYA K M .** left the meeting

 **ASHUTOSH BHATIA .** 8:12  
How to make a person presenter?

 **NEERAJ KUMAR VIJAY .** 8:17  
Yes, thank resting Parliament.

 **SOWMYA N SWAMY .** 8:19  
Once it so one second, let me just try to tell you.

 **NEERAJ KUMAR VIJAY .** 8:21  
Stop.

 **ASHUTOSH BHATIA .** 8:23  
That's the is this ASHUTOSH friend me straight spotlight or makes very difficult.  
They are uh.

 **LOKESH BABU S .** 8:32  
Where are you?

 **THIYANESWARAN M .** 8:37  
I think so.  
You have to go to a more and then click on more.

 **ASHUTOSH BHATIA .** 8:40  
Yeah.

 **THIYANESWARAN M .** 8:41  
Anyway, give the option.

 **SOWMYA N SWAMY .** 8:42  
More options.

 **ASHUTOSH BHATIA .** 8:50  
In my more there's no option.  
It's only a settings.

 **SOWMYA N SWAMY .** 8:55  
Correct, correct.

 **NEERAJ KUMAR VIJAY .** 8:55  
Umm.

 **SOWMYA N SWAMY .** 8:56  
Yes, that's what it is.

 **AMIT KUMAR PANDEY .** 8:57  
So in the.

 **ASHUTOSH BHATIA .** 8:57  
Device option meeting options correct.

 **THIYANESWARAN M .** 9:01  
He is meeting options, yeah.

 **ASHUTOSH BHATIA .** 9:03  
OK, people in my who can bypass the lobby and nouns who can present OK, and everyone.

 **THIYANESWARAN M .** 9:09  
So working better, yeah.

 **SOWMYA N SWAMY .** 9:10  
Yes.

 **ASHUTOSH BHATIA .** 9:11  
Everyone can present fine.

 **THIYANESWARAN M .** 9:14  
Exactly.

 **ASHUTOSH BHATIA .** 9:19  
And say OK now try.

 **NEERAJ KUMAR VIJAY .** 9:23  
Can you know?  
OK, I can access it now.

 **ASHUTOSH BHATIA .** 9:31  
I'm stop.  
I've stopped shaving.

 **NEERAJ KUMAR VIJAY .** 9:36  
Are you all able to see my screen?

 **K AKASH .** 9:39  
Yes.

 **LOKESH BABU S .** 9:40  
No, we can still see the OK.

 **SOWMYA N SWAMY .** 9:43  
No budget?  
No NEERAJ, we can't.

 **NEERAJ KUMAR VIJAY .** 9:48  
No.

 **K AKASH .** 9:48  
I think locash.

 **HARSH KUMAR .** 9:48  
Yeah.  
Yes, we can see now we can now.

 **JAGADEESAN P .** 9:49  
Yes, we are able to locations.

 **ASHISH KUMAR BHATTACHARYA .** 9:49  
Now it is visible now.

 **SOWMYA N SWAMY .** 9:51  
Now yes, now yes.

 **K AKASH .** 9:51  
Sharing the screen, yeah.

 **NEERAJ KUMAR VIJAY .** 9:54  
OK.  
So this is what I did. Ohm.  
So OK, I simply use this W gate command to download this file.

 **CHITHIRALA HEMANTH GUPTA .** left the meeting

 **NEERAJ KUMAR VIJAY .** 10:11  
You might get one error, so you can add this option no check certificate so it will allow you to download from GitHub and once you download it just look at this file and run this pseudo best command.

 **CHITHIRALA HEMANTH GUPTA .** joined the meeting

 **NEERAJ KUMAR VIJAY .** 10:27  
This is the same file which had downloaded.  
I just looked at a few of the things and it will ask you to install the dependencies for SE carrecter and once it resolved.  
Ohh it will ask you few things like your name, bits ID, email address and once you do this this is the banner with the ohh.  
This detail will come in so.

 **LOKESH BABU S .** 10:59  
You can maximize the window.  
OK, so that people can see.

 **NEERAJ KUMAR VIJAY .** 11:03  
OK.

 **LOKESH BABU S .** 11:06  
Thank you.

 **NEERAJ KUMAR VIJAY .** 11:08  
So this is what I did.  
Anything else beyond this, Sir?

 **ASHUTOSH BHATIA .** 11:12  
Yeah.  
So I think means the simple thing is the first you get that such file.  
If you are not able to understand it how to use it and all, you just get the SH file OK, just click on the link what I've provided.  
Probably it will take you to.  
It will open a window.  
You just control a control C and then in your machine save it as a dot TSV file.  
That's all.

 **NEERAJ KUMAR VIJAY .** 11:38  
Yep, that also you can.

 **ASHUTOSH BHATIA .** 11:39  
OK.  
Yeah.  
And once you have a dot SH file, you just run it using the command bash Dot Bash command.  
Just go to the bash command.  
First you go to the bash command. Yeah.

 **NEERAJ KUMAR VIJAY .** 11:49  
Just this is, yeah, this is the I use the studio.

 **ASHUTOSH BHATIA .** 11:52  
So this is either you can use sudo so let me give you 2 things one.  
You understand?  
Correct.  
So each container is one network, one node.  
So let's say if you have 3 nodes, one is attacker, one is a general machine.  
So what happens attacker window is having more credentials, so there you don't need this pseudo wash just you need bash.  
But if you are running on other windows then probably you need pseudo wash.  
So just choose either pseudo bash or bash and then this command.  
It will ask you to install some dependency.  
If somebody is after this saying yes for some cases it may say that permission denied and this and that.  
And that means there is some problem with your?  
Ohm, the positively system of Windows, is part of Linux.  
So then you just follow whatever it is saying.  
You just try to delete that thing and then retry.  
Otherwise it will work.

 **NEERAJ KUMAR VIJAY .** 12:59  
Yeah.  
So one thing is this is the banner and this came in so which information you want Sir?  
All this information or umm?

 **ASHUTOSH BHATIA .** 13:08  
So, so.  
So whatever that comes now, so whenever you are actually doing, let's say you are running some command, run some commands.  
Some uh, something Earth command or any command here for networking related?  
And that is state yes or maybe IP config.  
Yeah.

 **RAVISRI VENKATA RAMANA LANKA .** left the meeting

 **ASHUTOSH BHATIA .** 13:29  
So this is the output you got correct.

 **NEERAJ KUMAR VIJAY .** 13:31  
Yes.

 **ASHUTOSH BHATIA .** 13:32  
Now, whenever, whenever whenever I'm asking is screenshot of this output.

 **RAVISRI VENKATA RAMANA LANKA .** joined the meeting

 **NEERAJ KUMAR VIJAY .** 13:39  
Mm-hmm.  
We lost your voice.

 **ASHUTOSH BHATIA .** 13:47  
Yeah.  
What I'm saying that whenever you are taking the screenshot of this output, your banner should also be there in that screenshot.

 **NEERAJ KUMAR VIJAY .** 13:57  
Yeah.  
So in this output what I just a minute. Ohh.

 **ASHUTOSH BHATIA .** 14:03  
Means sometimes these outputs are not so big, so banner will be there.

 **NEERAJ KUMAR VIJAY .** 14:07  
So this kind of thing is it good enough for this?  
Also the below 1.

 **ASHUTOSH BHATIA .** 14:13  
Yeah, the below one is the axis specially the Mac address and all you go to this this system ID.

 **NEERAJ KUMAR VIJAY .** 14:20  
Yeah.

 **ASHUTOSH BHATIA .** 14:21  
Yeah.  
If the banner is not coming, it's fine, but the system ID VMCU information and all that.

 **NEERAJ KUMAR VIJAY .** 14:24  
Upper.

 **ASHUTOSH BHATIA .** 14:26  
So this this actually is saying that this is a unique system.

 **NEERAJ KUMAR VIJAY .** 14:31  
OK, so as you one time activity we can capture it and keep it, right?

 **ASHUTOSH BHATIA .** 14:36  
No, but then how I will you, how I will know that see it?  
It should be attached with every screenshot, correct?

 **NEERAJ KUMAR VIJAY .** 14:43  
OK, you won't get the screenshot OK.

 **ASHUTOSH BHATIA .** 14:45  
So that I can know that it was run on this machine.

 **NEERAJ KUMAR VIJAY .** 14:50  
Hmm.

 **ASHUTOSH BHATIA .** 14:50  
So the purpose is in very simple.  
That means he ran on his machine, his or her machine.

 **NEERAJ KUMAR VIJAY .** 15:02  
OK, I think that is.

 **ASHUTOSH BHATIA .** 15:03  
Yeah.  
So you try to.

 **NEERAJ KUMAR VIJAY .** 15:04  
Yeah.  
The only challenge will be if output is too big.  
How to capture?

 **ASHUTOSH BHATIA .** 15:08  
Yeah.  
Then it's, but it's OK means like some for some of the screenshots it's there. It's fine.  
Ultimate purpose is that it will avoid any kind of exchanging the output screenshots.

 **NEERAJ KUMAR VIJAY .** 15:23  
Yeah, sure, Sir.

 **ASHUTOSH BHATIA .** 15:24  
OK.

 **NEERAJ KUMAR VIJAY .** 15:26  
Thank you.  
I will disconnect my social, OK.

 **RAVISRI VENKATA RAMANA LANKA .** 15:27  
Some, it said.  
We will try to do the way it is meant instead of just now.  
Installation assuming that things work, we should be no problem.  
But just in case it does not work, at least for the.

 **ASHUTOSH BHATIA .** 15:36  
Otherwise I will.  
I will provide some expert don't worry miss.  
As of now, you are not submitting correct means I have an expert so yeah, this is skill.

 **RAVISRI VENKATA RAMANA LANKA .** 15:40  
OK.  
No, I mean, they're coming for upcoming assignment.

 **ASHUTOSH BHATIA .** 15:45  
Plot is actually my one of my future company.  
I tell you the the story behind this.  
So you just see that there is skill plot GitHub repositories there, correct?

 **RAVISRI VENKATA RAMANA LANKA .** 15:57  
Yes.

 **ASHUTOSH BHATIA .** 15:58  
So the skill plot is my future startup, where I one myself and one of my PhD student.  
We are developing a high quality educational content for not only for students, for for basically industry people as well.  
So even whatever we are going to develop here in this course that will be available to everybody open all the time and in this way after 5.  
Even be able to contribute like this particular gap that a lot of skills are required in IT industry which are either very heavily paid or people don't have proper resources to learn.  
So this we will, we will try to read this reach.  
Probably based on the same, we will provide the training study different negations.  
So that could be paid as well, but as of now this is our vision.  
So not only right now, even for IoT course, if you see it means for anything.  
Am I audible?

 **NEERAJ KUMAR VIJAY .** 17:15  
Yes, yes.

 **ASHUTOSH BHATIA .** 17:16  
Yes.

 **K AKASH .** 17:16  
Yes, Sir.

 **ASHUTOSH BHATIA .** 17:16  
So for anything, if you, if you frequently visit that you will find somewhere it's.

 **ASHISH KUMAR BHATTACHARYA .** 17:18  
Yes.

 **ASHUTOSH BHATIA .** 17:20  
So for example, how to use Raspberry pie?  
How to read?  
How to use different application live layer protocols?  
How to use make a chat bot personalized chat bot using WhatsApp.  
So there are so many things.  
What we found is like ultimately prevail provide blocks, but there is no concrete.  
You can say place from there you can get end to end complete everything.  
So this is this is our initiative.  
That's why I just provided it you through the through through that because see what happens like right now if I just give you then it will go somewhere and then later people can't use it.  
So the best way is like whatever effort we do, let it be available to everybody and for every time there's like more open source culture.  
Uh, I didn't.  
Future.  
We'll see how we can actually monetize this effort.  
OK, should be fired.

 **K AKASH .** 18:17  
Yes, Sir.

 **ASHUTOSH BHATIA .** 18:18  
OK, screens and then share.

 **K AKASH .** 18:22  
Or as I said before, going ahead my small question, I think we are we lost you in a moment.  
So am I audible?

 **ASHUTOSH BHATIA .** 18:31  
Yes, yes.

 **K AKASH .** 18:33  
So I think, uh, this question maybe applies to many of us as we are like, I'm especially myself little new or using Linux after so long from a basic background.

 **ASHUTOSH BHATIA .** 18:46  
Umm Jared Gupta?

 **K AKASH .** 18:47  
So any resource would you recommend so that we?

 **ASHUTOSH BHATIA .** 18:50  
Just do what is the command from this type the word and then it will give you better than any other expert how to do this.  
OK.

 **K AKASH .** 19:03  
Uh, OK, for basic clinics, what level?

 **ASHUTOSH BHATIA .** 19:05  
What?  
What even if you want if, if you are, if you see you just go to the chat Gupta.  
OK.  
And if you, let's say if you don't know how to write a shellscript if you don't know what is this what this command does, let's say let's say add net state is returned.

 **K AKASH .** 19:14  
OK.  
Hmm.

 **PAVITHRA S .** joined the meeting

 **ASHUTOSH BHATIA .** 19:22  
If you don't know how the R protocol does is you don't know what is the IP address this person is talking about.

 **K AKASH .** 19:23  
OK.

 **ASHUTOSH BHATIA .** 19:28  
Any command just you put it there and say it.  
Explain me. Done.  
OK, you say give some examples so that I can run it will give you example.  
Run it here.  
You can take it from me that at least for the coders and ID industry, it is better than most of the experts.  
OK.  
So just try using that and then you will find me a much more empowered you won't believe that in last one month I created 3 softwares, one for my convocation 1 chat bot, one blockchain based and I use Java scripts.  
I used a.  
You can say node JS different technologies and these previously I used to depend upon students for doing things to Wi-Fi converting my ideas.  
But now I feel so much empowered.  
I really don't need them.  
See if there isn't any issue.  
I'm not understanding what this code is doing.  
Just write it there, he will explain you that this is the problem with this code.  
So you you just try to use it, take it from my side.

 **K AKASH .** 20:30  
OK.

 **ASHUTOSH BHATIA .** 20:34  
Mean.  
OK.

 **K AKASH .** 20:36  
OK, Sir.

 **ASHUTOSH BHATIA .** 20:36  
And then you will find it that the question like I don't need.  
The only thing is that one has to be smart using things correct?  
You really spend time, understand you use it, but it will help.

 **K AKASH .** 20:45  
OK.

 **ASHUTOSH BHATIA .** 20:48  
It will surely help you.  
You don't need to go anywhere. Ticket. OK.

 **K AKASH .** 20:51  
OK. Yeah.

 **ASHUTOSH BHATIA .** 20:53  
Hear what?  
OK, so now let's let's continue our discussion.  
Where is my friend.  
So we're going to discussing about cryptography.  
So in general, the cryptography is all about the protecting the the content from adversary.  
It's primarily two goals.  
One is like data privacy and one is data integrity.  
OK.  
And the the authenticity of data.  
So data integrity means the data is coming the the the origin of the source, the origin of the data is authenticated and authenticity is uh yeah.  
Sorry, the data integrity means data has not been modified in between and authenticity means that it is coming from the right origin.  
OK, so the origin of the data is authenticated.  
Privacy means nobody is able to see it.  
So what exactly you want is a.  
You can say if you think about an adversary, you always think about as a clever person with a powerful computer.  
OK, don't underestimate the adversary.  
Whenever you are trying to design things so like in this case admin just trying to talk to Bob and then this is a through a public network means if it is not a public network that anyhow we don't need all this photography.

 **ABDUL ALTAF SHAIK .** left the meeting

 **ASHUTOSH BHATIA .** 22:12  
So you are going through a public network and adversaries trying to ease drop here.  
Uh.  
Similarly yes.

 **TISMON VARGHESE .** joined the meeting

 **ASHUTOSH BHATIA .** 22:18  
So for the data privacy, the goal is to ensure the adversary does not see any data and like and could see the credit card number and all that whatever is being communicated.

 **ABDUL ALTAF SHAIK .** joined the meeting

 **ASHUTOSH BHATIA .** 22:29  
Authenticity means the goal is to ensure that M really got originated with Alice, not with someone else.  
So when the Bob is receiving a message M, actually it has to ensure that it is actually coming from Alice, not from somebody else like adversary.  
Similarly, that M has not been modified, so whatever M dash you are getting, you know that this is not modified.  
If you're talking about the ideal world where you have a communication secure communication channel between Alice and Bob, then you really don't need.  
You can say the the cryptography, but you don't have such channels mean you try to make such some channel logical channels like through VPNs and all that.  
But technically you might have heard about like hotline like 2 prime ministers between two countries talk.  
Yeah, using an hotline they don't use, so it's like a dedicated line.  
I'm laying down over the sea means it's like there's nobody actually else shares that line and probably that is the notion of hotline.  
And then you are talking, so you are actually using the physical layers level security so that there is no eavesdropping is not possible correct?  
So for example, if I just combine all these things into in their example that medical database the doctor is there, doctor will get.  
So Alice goes to Doctor, Doctor Will fetch the Alice related data.  
It's medical records, so it will send an request to the database and it will get the data.  
I then we'll read the database, it will modify.  
Possibly he has now seen new reports.  
So his modified the data and put it back to the Alice record, correct?  
This is the whole process is happening now in this whole process.  
If you see there is all sorts of security requirements are coming.  
So for example, when database is actually receiving the Get list command from the doctor OK from the doctor, how does it know that is is actually?  
The doctor is authenticated.  
This is authentication problem.  
When database is giving FA to the doctor, how does the doctor know that the affair has not been modified to Effie Dash and at the same time that that this FA is actually coming from a genuine database? Correct?  
Similarly, when it will read and modify it, you have to ensure that whether this modification is authorized to do and at the same time when he is putting that data, if it is back, you need to again ensure that whether this appear dash has been not modified, and when the data is Effie Dash is coming back to the database, it is actually coming from the doctor and also it is coming the same thing what he had sent.

 **NIHAL PRAKASH .** left the meeting

 **ASHUTOSH BHATIA .** 25:15  
So it is not coming off a double dash, so that is what in in you see that authenticity, data integrity data, origin integrity.  
I I entity authentication everything is there in this this example correct?  
So yeah, for example, you need to ensure that the doctor is authorized to get.  
So this is like authentication.  
Uh FF days are not modified in classmate.  
FA is really sent by the database and so on and so forth.  
OK, now when we talk about different cryptographic schemes you we usually have an encryption in your them they are you have an encryption algorithm which takes some kind of key from that list to encrypt and the messages and input and generates an C which is called ciphertext which is gets communicated from here to here.  
And then you get C dash now because it might have been changed in between.  
You don't know what all you need to ensure is that decryption algorithm which uses MOK and so which uses decryption key and this algorithm and then it generates M if C equals to C dash, else if she's not equal to she dash then it will generate null.  
That means kind of rejection, so it will say that say I'm not going to decrypt.

 **SAURABH RAUTELA .** left the meeting

 **ASHUTOSH BHATIA .** 26:40  
This means means I'm not going to use this because I found that it has been modified.  
OK, so the, the, the authentic, the the integrity and it is and privacy both are integrated together.  
OK.  
So it's not like that that first two will first you will decrease and then you will check no.  
This whole algorithm should not.  
Uh will always return null if she was not actually.  
See that?  
So then then you simply discarded from this KKD&KE perspective if KE is equals to KD, that means both the parties are have a pre shared secret key.  
This is called symmetric key encryption.  
Symmetric key encryption that the examples of AES and ADS the D as you can see and but it's K and KD are different.  
That means if K and is not equals to KD, then we call it what we call it. Anybody.

 **THARUNKANTH D .** 27:47  
Automatically.

 **ASHUTOSH BHATIA .** 27:48  
A symmetric key or public key encryption, public and private?

 **JAGADEESAN P .** 27:49  
The restriction.

 **THARUNKANTH D .** 27:52  
Public and Trinity.

 **K AKASH .** 27:54  
Uh.

 **ASHUTOSH BHATIA .** 27:55  
Maybe it's it's the world is public key encryption only, but actually KE is pair and KD pair makes public and private key.  
Later you will come to know that.  
See, you can make any one of this public and one anyone of that private.  
So in this particular example, this K&KD belongs to whom?  
Alice or Bob?

 **THARUNKANTH D .** 28:25  
A dog nation, maybe?

 **C RUKMANANDUDU .** 28:27  
Alice.

 **ASHUTOSH BHATIA .** 28:27  
Now, in this particular example.

 **SOWMYA N SWAMY .** 28:28  
I I Alice.

 **TARANVIR SINGH SAINI .** 28:30  
Alice.

 **ASHUTOSH BHATIA .** 28:31  
So what is K?  
What is Alice?  
What is OK?

 **SOWMYA N SWAMY .** 28:37  
The encryption key.

 **ASHUTOSH BHATIA .** 28:39  
Ah, no, there's there's this is either.

 **K AKASH .** 28:40  
Is public key, Sir.

 **NEERAJ KUMAR VIJAY .** 28:41  
In private.

 **K AKASH .** 28:42  
These public key and K's private key.

 **ASHUTOSH BHATIA .** 28:43  
OK, OK.  
So that means Alice is using its own public key to encrypt the data from the Bob.  
Is it what you're saying?

 **K AKASH .** 28:51  
No.  
Alice is using public key of Bob and Bob is using private key of his own.

 **ASHUTOSH BHATIA .** 28:54  
Yes.  
Excellent.  
So this KKKD pier belongs to.

 **K AKASH .** 29:01  
Bob.

 **ASHUTOSH BHATIA .** 29:02  
Bob, when Bob created AC KKD pair.  
See, there are simple algorithms.  
You just find one.  
Just just search, maybe I can provide you the program in Python.  
Just run a program, it will generate a KD pair for you.  
This I had done with some of my students long back.  
I have provided them and this script with.  
Using that script, they generated KD pair.  
They provided me KE and kept themselves with KD, so in any future communication I was using this key to communicate with them and this is very used.  
This was very useful.  
For example, I am a communicating, let's say marks.  
For each of you means nowadays there are different pairs, but I'm just explaining now I cannot basically show in an Excel sheet, correct?  
I cannot actually show every other mask to everybody, So what I can do?  
I can have your encrypted marks in one column, and let's say this.  
This is a student X1 and this is the student X2.  
So this one this cell is in gifted with this marks even with with X one OK and X1 public key and this is encrypted with X2 public key.  
Now you can take your own and then decrypt.  
You can take your own and your decrypt correct.  
So I just put one excel sheet, but then nobody can see that that's not.

 **K AKASH .** 30:25  
Uh, sorry.  
In this example, C dash is it, uh encrypted message or uh compromised uh message.

 **ASHUTOSH BHATIA .** 30:32  
Yeah.  
So we actually say we, let's say as let's assume that you are using C dash because you will receive something correct.  
So either C dash could be C or C dash may not be equals to C.

 **K AKASH .** 30:39  
Yes.

 **ASHWIN SIDDHARTH S .** left the meeting

 **ASHUTOSH BHATIA .** 30:44  
OK, if she does equals to C then this all this decryption algorithm should deterministically return M.  
Otherwise my whole system is failed, correct?

 **K AKASH .** 30:58  
OK.

 **ASHUTOSH BHATIA .** 30:59  
But if she does, is not equals to C, then it should not basically say that it it should not return something something M does because there are attacks.  
We means this, this, this simple thing is not that much simple that way.  
It is looking because if seed Dash was something else I decrypted, I may get something M dash correct and then you will deliver this M dash to your higher level applications and probably somebody has a mechanism to to modify this.

 **VANAM VIJAY KUMAR .** joined the meeting

 **ASHUTOSH BHATIA .** 31:29  
See to seed as in such a way so that it will get M dash so that it can have some disastrous effect on application.  
So idea is like at the down level only it should not happen that I'm I'm not able to identify that this was actually changed.  
I I should be able to identify and drop it at very lower layer, correct lower layer should not deliver the wrong data to the higher layers.  
Got my point.

 **K AKASH .** 32:02  
Yes.

 **ASHUTOSH BHATIA .** 32:03  
Yeah.  
So this is very important that this is saying that you are able to not only get the correct data back, but also if it has been modified then you just return null.  
Your algorithm returns null.  
It does not return M dash.  
This is very important.  
With respect to C dash and does not return M-OK and therefore there were actually attacks.  
Let me tell you how, for example, let's assume that this is an.  
Actually this is data which is say I am giving you very subtle example OK and let's try to understand this is the data add this data is saying that uh that port number is 25.

 **BHAVANAM NAGA SAHITYA .** joined the meeting

 **ASHUTOSH BHATIA .** 32:52  
So when this data will be decrypted, this in the in the machine.  
This is an OS and then you are running multiple multiple applications and this port number is 25 S application is running and let's say now I'm an attacker.  
Somehow I am able to install in malware within the system which is running at port number, let's say 70.  
OK.  
The deal, despite it's fine now, there is a legitimate communication is happening from somewhere.  
So that packet is coming and it has to go to 25, but then in the attacker in between it was seen as he modified this in such a way so that when this will be decrypted precisely the port number will part will become 70.  
OK.  
So then OS will actually decrypt it, but after decrypting it actually where to deliver to port #70 where the malware is running.  
So instead of delivering it to 25, it will deliver it to 70 and already it has decrypted everything.  
Correct.  
So you are actually able to craft fully modify the data metadata of the the the message so that instead of to the right person is being delivered to the wrong person.  
Here.

 **K AKASH .** 34:19  
Yes, Sir.

 **ASHUTOSH BHATIA .** 34:21  
OK, maybe what works.  
It's OK.  
I think it means you really need to know some of the networking basics.

 **JAGADEESAN P .** 34:27  
So one question here.

 **ASHUTOSH BHATIA .** 34:29  
Yeah, OK.

 **JAGADEESAN P .** 34:30  
So even if it is delivered to wrong person, right?  
So until they have the private key, they will not be able to decrypt it and see, right?

 **ASHUTOSH BHATIA .** 34:36  
Non decryption PCP has already done.

 **BHAVANAM NAGA SAHITYA .** left the meeting

 **ASHUTOSH BHATIA .** 34:40  
The TCP is like the correct, so this is how the communication happens.

 **JAGADEESAN P .** 34:41  
Ohh.  
OK.

 **ASHUTOSH BHATIA .** 34:45  
At DTLS, layer has already done the decryption.  
It is being delivered to the OS, I mean the application.  
You're not doing application layer and that's why some of the people say call end to end.  
What is called end to end encryption?  
Which WhatsApp does correct?

 **JAGADEESAN P .** 35:01  
Think of.

 **ASHUTOSH BHATIA .** 35:03  
So it's like even if you're Android OS, Android OS don't have the key means it is actually delivering everything to you, correct?  
And then at your application layer you have the key, so the kind of a scenario what you are talking about is called end to end encryption.  
So you have TCP which is a transport layer, TLS, and then you have an application.  
So the encryption happens here.  
The things encrypted go here and then in the destination machine it reaches to TCP and then they list the decryption has his here.  
So at this boundary you are actually giving plane clear.

 **SOWMYA N SWAMY .** 35:46  
Sir, what is MM and perpendicular here is in this case.

 **JAGADEESAN P .** 35:46  
Yes.

 **ASHUTOSH BHATIA .** 35:51  
Message.  
Any message?

 **SOWMYA N SWAMY .** 35:52  
Emma's message, OK.

 **ASHUTOSH BHATIA .** 35:55  
M is message you are encrypting it.  
So let's say if I'm saying, I'm saying that the uh, let's say send ₹20 to Bob, this is my message.  
OK.  
And then after encrypting it will become something garbled.  
Means like tea RPQSN means you can't understand.  
If you try to understand in this manner, the encryption means that this has no step, there is no way that you can actually get any bit of information about the message from just knowing the ciphertext.  
This is the technical definition of encryption.  
OK, you can't infer anything about the message just by saying this.  
So this means if you see this, you can't tell anything about him.

 **SOWMYA N SWAMY .** 36:53  
Correct.

 **SHYAMSUNDAR DAS .** 36:53  
Uh, Sir, I have a question.  
So this uh, so you are taking this KKE&M and then you are passing it to the ER, the summation E to get the C right?

 **ASHUTOSH BHATIA .** 37:05  
No, no, no, don't don't.  
This is not summation.  
This is an encryption algorithm.  
This is sign symbol encryption algorithm.

 **SHYAMSUNDAR DAS .** 37:11  
Yeah, yeah, yeah.

 **ASHUTOSH BHATIA .** 37:13  
So this is AES.  
It could be AES or it could be Roshan.  
These things are standard.  
You don't design in last class.  
I've already talked about and this there is open.

 **SHYAMSUNDAR DAS .** 37:24  
Yeah.  
Yeah.  
And and so you are getting you are.  
Yeah.  
And you are getting.  
See, so this C is what actually play for text.

 **ASHUTOSH BHATIA .** 37:30  
Ciphertext we call this this plaintext and this is Cypher text.

 **SHYAMSUNDAR DAS .** 37:37  
OK.

 **ASHUTOSH BHATIA .** 37:38  
Correct, so now.

 **SHYAMSUNDAR DAS .** 37:38  
And and then, yeah, you are, yeah.

 **ASHUTOSH BHATIA .** 37:41  
Yes.  
Yes, please, please.

 **MANISH MEHTA .** 37:43  
This.

 **SHYAMSUNDAR DAS .** 37:43  
Yes, Sir.  
So I was trying to understand.  
So after that, see now you are getting the C dash right after that in the right.

 **ASHUTOSH BHATIA .** 37:49  
Uh, we are saying that either it could be changed.  
See, it could be either it will reach as it is after traveling to the Internet correct, or it may be possible that some error has happened because of some natural error like wireless error.

 **SHYAMSUNDAR DAS .** 37:59  
Yes.

 **ASHUTOSH BHATIA .** 38:05  
And there are like lot of noises there or somebody has deliberately changed it using them.

 **MANISH MEHTA .** 38:07  
Yeah.

 **ASHUTOSH BHATIA .** 38:10  
We don't know.  
Ultimately, whatever I'm receiving, I don't know whether this is exactly what it was sent, but I will receive something correct and that's why we use the term C dash.

 **K AKASH .** 38:25  
Well, Sir, one but yeah.

 **ASHUTOSH BHATIA .** 38:26  
Correct.  
Hmm.

 **K AKASH .** 38:30  
One basic question, Sir, maybe very busy in in an.

 **ASHUTOSH BHATIA .** 38:32  
Yeah.  
No, no, no, don't.  
Don't be shy.  
It's fine, it's fine.

 **K AKASH .** 38:37  
Yeah, let's say in a LAN, I mean, I just wanted to correlate this with real time example.

 **ASHUTOSH BHATIA .** 38:44  
Yes.

 **K AKASH .** 38:44  
This message communication, is it an SMTP or is it any message, let's say in a lab from one node we are sending a message to another node.  
So exactly this encryption happens at which layer application layer?

 **ASHUTOSH BHATIA .** 38:55  
Yes.  
OK, so so this is this is this is the note fine because this not you have an OS, OK you have any application, OK OS usually uses TCP protocol or UDP protocol to communicate down.

 **K AKASH .** 39:00  
Physical layer?  
Yeah.  
Yes.  
Yes.  
Yes.

 **ASHUTOSH BHATIA .** 39:20  
You have Mac layer also and then actually the information so goes down.  
OK, so you can think about this as the the physical channel, correct?  
And then physical channel and then you have Mac protocol and then you have TCP protocol and everything is there and then you have an application.

 **K AKASH .** 39:35  
Yes.

 **ASHUTOSH BHATIA .** 39:39  
This is without encryption.

 **K AKASH .** 39:39  
Yes.

 **ASHUTOSH BHATIA .** 39:41  
OK, you are just giving it to the TCP and then this is now big.

 **K AKASH .** 39:42  
Yes.

 **ASHUTOSH BHATIA .** 39:46  
Boss, people have designed and then see whenever OS gets a TCP packet.  
It knows that on which port?  
So then you will receive a port, correct?  
So once you receive, let's send the packet is going from here to here you will receive that port number as part of the TCP header.  
You understand that.

 **K AKASH .** 40:06  
Yes, Sir.

 **ASHUTOSH BHATIA .** 40:07  
Yeah.  
Now depending upon that that in this at different ports different applications are running.  
OK.  
So then it will deliver the message to that application.  
This is like your usual communication.  
This is how it happens.  
Application asynchronously keeps on running a system call which is called receive.  
OK, so whenever I call and receive and if OS has received something, some packets or some message from me it will just be really give it to me.  
OK, this much is clear.

 **K AKASH .** 40:42  
Yes, Sir.  
Yes, Sir.

 **ASHUTOSH BHATIA .** 40:43  
OK, after that, what happens?  
They realize that, but this is not secure.  
How to do it so then they introduce the layer called TLS in between TCP and Mac player.  
All transport layer security.  
OK, so so they.

 **K AKASH .** 40:59  
OK.

 **ASHUTOSH BHATIA .** 41:02  
No, I'm sorry.  
I'm not here on top of it, OK?  
So when you are your application is actually giving the packet to the OS.  
The first this actually encrypts and then it gives to the Mac layer and then that goes over the channel.  
So this is the see what I'm talking about.  
Correct.  
So this encryption happens.

 **K AKASH .** 41:24  
Yes.

 **ASHUTOSH BHATIA .** 41:26  
Now you may ask that see when this happened that this particular TLS layer this there's a complete negotiation that happens.  
So this is node one and this is node two.  
Let's say this is your browser and this is your Internet.  
Okgoogle.com google.com and this is your browser the first time you try to access the google.com the whole the all lot of TLS negotiation happens where you negotiate keys and everything.

 **K AKASH .** 41:43  
Yes.

 **ASHUTOSH BHATIA .** 41:57  
So this whole thing happens.  
OK, once all the keys establishment and authentication and everything has happened, then you start then internally start sending the data using those credentials.

 **CHITHIRALA HEMANTH GUPTA** joined the meeting

 **ASHUTOSH BHATIA .** 42:11  
So when we are talking about that.  
Is this?  
It's called exchange process.

 **K AKASH .** 42:21  
Yes.

 **ASHUTOSH BHATIA .** 42:21  
So all that is part of our all that is part of this.  
No realest protocol, which probably later part of this course, we'll see the complete protocol.

 **K AKASH .** 42:32  
OK.

 **ASHUTOSH BHATIA .** 42:32  
OK, so this is this is how the communication happens and means it could be TLS but when you are doing SSH for example if you are do not doing you collecting those server.

 **K AKASH .** 42:33  
Yeah, understood.

 **ASHUTOSH BHATIA .** 42:45  
If you are doing SSH to a machine, let me again put it in this way.  
Uh.  
If if you are on the same let and let's say you are actually in your company, you have server.  
OK, you are the client machine.

 **K AKASH .** 43:04  
Yes.

 **ASHUTOSH BHATIA .** 43:08  
As I said protocol, that's a different protocol.  
OK, it's it's a secure socket layer protocol instead of TLS protocol.  
Alternately, the purpose of all these protocols is to negotiate the key and negotiate what is the algorithm that we are going to use for encryption, decryption and authentication.  
That's all OK once they have done the negotiations, you just use that and encrypt using it and send it clear.

 **K AKASH .** 43:33  
OK.  
Yes.

 **NEERAJ KUMAR VIJAY .** 43:41  
Ohh what one question Sir ohm.

 **ASHUTOSH BHATIA .** 43:44  
Umm.

 **NEERAJ KUMAR VIJAY .** 43:46  
So you said that it is just after the application you it is putting into a TLS encryption and then it goes to TCP and the OS, right?

 **REHAN AKHTAR .** left the meeting

 **ASHUTOSH BHATIA .** 43:56  
That is for the Internet browsing and SL case, but if you are free to actually make encryption at application layer also nobody is stopping it.  
So you may have a double encryption.

 **NEERAJ KUMAR VIJAY .** 44:09  
Yes, yes, yes, so.

 **ASHUTOSH BHATIA .** 44:10  
You can do encryption here and then you are giving it to TLS means for TLS.  
This is a payload, so it doesn't care, but for him it is a plaintext.

 **NEERAJ KUMAR VIJAY .** 44:20  
OK, so titles is again application layer only stop right?

 **ASHUTOSH BHATIA .** 44:24  
A TLS is actually a transport layer service.  
OK, transport layer security.  
It's this is not application, this is a service running at OS operating system.  
So see it operating system.  
Whatever programs are running are called services.  
They are not applications.

 **NEERAJ KUMAR VIJAY .** 44:41  
Yeah. True.  
True.  
Yeah, my mistake.  
I'm always confused that because in transport that you TCP and UDP and TLS is also at that level security so so so I.

 **ASHUTOSH BHATIA .** 44:52  
OK. OK.  
So so TNS basically DNS only works on top of TCP.  
If you want secure communication using UDP, now it's a something different because because there is no all the website runs on top of HTTP protocol or HTTPS protocol.  
OK.

 **PANCHAL MAHESH MAROTRAO .** joined the meeting

 **NEERAJ KUMAR VIJAY .** 45:14  
Yep.

 **K AKASH .** 45:15  
Yes.

 **ASHUTOSH BHATIA .** 45:15  
And then that is actually inherently running on top of TCP.  
OK, so if you are designing a communication between 2 nodes on your own, let's say Ethernet lab means on your lab or maybe this you can think about your virtual machine within your system, correct?  
And these are the two containers container one and container two and then you just want to use UDP to communicate using securely.  
Then probably you have to use some encryption algorithm here on your own.  
Then you don't have protocol standard defined protocol.

 **NEERAJ KUMAR VIJAY .** 45:52  
Hmm.

 **ASHUTOSH BHATIA .** 45:53  
OK, there, there, there are.

 **NEERAJ KUMAR VIJAY .** 45:53  
OK, you don't know.

 **ASHUTOSH BHATIA .** 45:55  
There are four variations for TCP.

 **NEERAJ KUMAR VIJAY .** 45:56  
I.

 **ASHUTOSH BHATIA .** 45:58  
One is HTTP, one second is HTTP.  
I mean application Layer Protocol 1.01.  
Sorry 1.11 point two HTTP 2.0 and HTTP 3.0.  
Now STP3, everybody knows what it is.  
This uses a protocol called Quick.

 **ANUBHAB SAHU .** 46:23  
This.

 **ASHUTOSH BHATIA .** 46:27  
Instead of.

 **ANUBHAB SAHU .** 46:27  
Sir, I think very, you know, she didn't know.

 **THARUNKANTH D .** 46:28  
He explained last thing about.

 **NEERAJ KUMAR VIJAY .** 46:29  
I think I think I should keep it.  
Two is kind of Websocket 3I I drink beer.

 **ASHUTOSH BHATIA .** 46:34  
You.  
No, no two is actually an improvement over 1.2, which has a problem called head of line blocking.  
OK, I'm not going into that head of line blocking, which was actually a performance issue.  
So that 2.0 solves this.  
Another problem 2.0 solves is is a push based push based communication.  
See this STP is based on a project is an architecture called rest.  
You have you heard about it?  
So what you do is you do get and then post.

 **SOMNATH CHATTERJEE .** 47:07  
Yes, yes, this service.

 **NEERAJ KUMAR VIJAY .** 47:08  
Yes.

 **ASHUTOSH BHATIA .** 47:10  
So you say to the to the web server you say send a get API and then it basically sends you the reply in terms of HTML page.  
OK, so that is get and post.  
This is how HTTP works, but the problem was in the push was like suppose I'm I'm watching a A you can say online match and what I want is that server should periodically push the latest update in my page I should not.  
I need not have to refresh it correct?  
So this was a fundamental problem in 1.2 because until unless you don't ask me, I'm not going to give you.  
OK, so how do you make real time pages which actually automatically get updated?  
But nowadays you might have seen means all those pages which actually automatically update the content in the page without you sending the request, correct?

 **GOVIND PARMAR .** joined the meeting

 **NEERAJ KUMAR VIJAY .** 48:04  
Yes.

 **SOMNATH CHATTERJEE .** 48:04  
Yes, yes.

 **NEERAJ KUMAR VIJAY .** 48:04  
So that is the synchronous that is asynchronous request, right? Yeah.

 **ASHUTOSH BHATIA .** 48:05  
Yeah. So.  
Yeah, but fundamentally rest is not designed in that manner.  
List means it's an API.

 **NEERAJ KUMAR VIJAY .** 48:14  
No, no.

 **ASHUTOSH BHATIA .** 48:16  
Use.  
You ask me, I will give you.  
You ask me the resource information, whatever you want, STL page or whatever endpoint resource you are asking.  
For me, I will just provide you.  
I'm not going to keep on giving you on my own.  
So STP 2.0 actually provided an improvement on top of it STP3 point.

 **DIVYA JYOTI MISHRA .** joined the meeting

 **ASHUTOSH BHATIA .** 48:41  
So this along with TLS becomes HTTP S OK, but this is still with TCP, but now I STP 3.0 Google have removed this.  
This is a quick protocol which combines HTTP and TCP both in one.  
So now the transport Layer protocol is gone and then you have a TCP TLS.  
So everything is in one protocol.  
OK.  
So yeah, there's a lot of architectural advancements are happening, but fundamentally you have always one transport layer means the functionality of transport layer is always there.  
The functionality of encryption and decryption and authentication is a part of a layer.  
Whether you implement together, you don't implement together.  
You implement as part of application you implement as part of OS.  
That's a different means.  
You can say design issue, OK?  
Any doubt?

 **ANUBHAB SAHU .** 49:50  
So that you want, Sir, I have one question.

 **ASHUTOSH BHATIA .** 49:52  
Hmm.

 **ANUBHAB SAHU .** 49:53  
So that has there any HTTP version name HTTP 1.2 because I never saw that.  
I mean, I know that HB starts from HTTP 0.9, then 1.1, then 2.0, but I never.

 **ASHUTOSH BHATIA .** 50:06  
Or is it like that?

 **ANUBHAB SAHU .** 50:08  
I never heard about this.  
Should we wanted to.

 **ASHUTOSH BHATIA .** 50:10  
You are saying 1.1 and then 2.0.

 **ANUBHAB SAHU .** 50:14  
Yeah.

 **ASHUTOSH BHATIA .** 50:15  
No, there are two versions of 1.  
One was using pipeline and so it is TP.  
In my opinion, it could be 1.0 or 1.1 also, but let me just tell you the difference between the 1st 1.1 and 1.2 or whatever 1.0 or 1.1.  
The basic difference was that the first one was making a TCP connection for every get request.

 **ANUBHAB SAHU .** 50:40  
Yeah.

 **ASHUTOSH BHATIA .** 50:41  
OK.  
And then they'll improvement was that you make you just use one connection, but within one connection you use different streams.

 **ANUBHAB SAHU .** 50:52  
Yeah.  
I think, Sir, the first one was HTTP 0.9 where we can send zero to 9 then 1.0.

 **ASHUTOSH BHATIA .** 50:56  
OK.  
OK, OK, that could be you.  
You OK that, that, that could be the possibility.

 **ANUBHAB SAHU .** 51:03  
Yeah.

 **ASHUTOSH BHATIA .** 51:03  
I I will.  
I will verify it, but I think, yeah, this this was so it's like and there is a there is a you can say history of improvement in HTTP protocol and then the TLS also came along and this is this is how the thing works.  
Uh, if you allow your people allow, should I move ahead?

 **ANUBHAB SAHU .** 51:25  
If it's you.

 **SOMNATH CHATTERJEE .** 51:26  
That what?  
One last question, quick question related to this reservice and the soap service.

 **ASHUTOSH BHATIA .** 51:27  
Ha, ha.  
OK, OK. Yeah.

 **SOMNATH CHATTERJEE .** 51:31  
So this is soap and rest.  
We have found that a rest service is much secure than soap.  
It is something like that.  
It is generally told.

 **ASHUTOSH BHATIA .** 51:41  
I see I can't.  
Rest is built on top of HTTP, but in see it's fundamentally rest is an architecture and it's a principle guiding principle and you cannot tie up rest with any protocol.  
OK, it's an architectural way of doing things.  
However, most of these people attach STP as just think that that is the only rest means.  
This is the one thing our security wise how they are actually different.  
I don't know means it's like.  
Ohh, probably as I have to look into that.  
How SO?  
PE deals with the things and then what?  
Which component is weaker and all that but see means it's like which aspect of security?

 **DURVASULA DEEPIKA ANNAPURNA** left the meeting

 **NEERAJ KUMAR VIJAY .** 52:28  
I can't.  
I can breathe, but it is way outside of this topic.

 **ASHUTOSH BHATIA .** 52:35  
Maybe we can leave because this is little bit the different course we are going in that direction.

 **SOMNATH CHATTERJEE .** 52:35  
Yeah.  
Yeah, sorry for that actually.  
Yeah.

 **NEERAJ KUMAR VIJAY .** 52:40  
Yes, yes, so.

 **SOMNATH CHATTERJEE .** 52:41  
Yeah, exactly.  
Yes, yes.

 **ASHUTOSH BHATIA .** 52:42  
Take it.  
Hello.  
OK, let's go.  
Move ahead.

 **K AKASH .** 52:44  
Yes, Sir.

 **ASHUTOSH BHATIA .** 52:45  
So we have to, yeah.

 **TARANVIR SINGH SAINI .** 52:45  
Which is a one.  
One more doubt.  
Hey.  
Yes, Sir.  
Actually here like you can see right, there's one public key with Alice and one private key with Bob.

 **DURVASULA DEEPIKA ANNAPURNA** joined the meeting

 **TARANVIR SINGH SAINI .** 52:54  
So in future if this private key with the Bob is having so that gets manipulated or gets deleted.  
So so in future for the future communications, then Alice and again needs to generate a new public key, right?

 **ASHUTOSH BHATIA .** 53:05  
OK, so I think, yeah, you you put a right question.  
The idea is if you think about the this is.  
This is a fundamental way.  
It works, but actually what are the actual communication models in this work which are running over the Internet?  
Usually these people are servers like google.com or these people are clients, so client server architecture.  
Usually we work on correct in that setup.  
This person is is actually a.  
You can say this person simply generates a public key be a pair, let's say key P, public key PB and PB public Key and PR private key pair.

 **PRAMOD KUMAR N .** joined the meeting

 **ASHUTOSH BHATIA .** 53:54  
Let's say this is a Google.  
It generates PB and PR OK Now then it basically publics this PB throughputs this PB into a certificate.  
B and my name is Google and then this gives it to his certification authority.

 **NAMAN KANDPAL .** joined the meeting

 **ANUBHAB SAHU .** left the meeting

 **ASHUTOSH BHATIA .** 54:15  
The certification authority actually digitally signs digital signature on this and then this digital signature.

 **ANUBHAB SAHU .** joined the meeting

 **ASHUTOSH BHATIA .** 54:23  
It returns back to you.  
Now you have this.  
Whenever somebody communicates to you, you just take this digital signature digital certificate, then the certification authority not come into the picture.  
You take this digital certificate and then give this public key.  
If somebody is so this is how the person is going to get your public key and at the same time he knows that yes, you are Google.  
It is not like that somebody else is saying I am Google and this is my public key because you have a certificate and the this person knows the public key public key of certification authority.

 **G PHANI KUMAR .** joined the meeting

 **ASHUTOSH BHATIA .** 55:02  
This is pre known so pre known means when you install your browsers correct the browsers have pre known certification authority public key so they can actually verify the the certificate provided by any website to them.

 **TARANVIR SINGH SAINI .** 55:02  
Umm.

 **ASHUTOSH BHATIA .** 55:17  
OK, so this is how you verify once you Fr verify you've got the public key and then you use that public key to encrypt the message and then this will we will use as private key tomorrow in that private key is lost.  
It's OK, you just generate a new public private key pair and then this.  
Not only that, this certificate has a mechanism that what is the lifetime of this certificate?  
All already this is a part of this, so the time is written.  
So for example, if the certificate has expired, I will not use this key and the reason for the certificate being expired is that in fundamentally in crypto we say that you should not use the same key to encrypt the 10's and 10s of information.

 **TARANVIR SINGH SAINI .** 55:58  
Yeah.

 **ASHUTOSH BHATIA .** 56:00  
So there is a revocation mechanism that automatically the certificate will die.  
So see, there is no scarcity of keys means you can have two raised to power 128 one 256.  
Like if you are talking about public key, sorry it is 20482 raised to power 2048 keys are there and this is like if you take all the universe all the you can say items in the whole universe.  
Uh, it is much, much larger than that.  
Don't worry about this.  
There's no scarcity.  
You just throw away that if you just forget that only thing is that you cannot decrypt your old messages and this is the biggest problem with Bitcoin.  
If you are holding a Bitcoin and if you lose your private key, then that money cannot be reclaimed by anybody in future.  
Done.  
Gone.  
That money is scrap means it's like it is out of the system.

 **TARANVIR SINGH SAINI .** 57:00  
Thank you.  
Good.  
OK.  
OK.  
So yeah, yeah, that's that.

 **ASHUTOSH BHATIA .** 57:03  
OK.  
Because that's that's the fundamental notion, correct.  
If you have a mechanism, then that mechanism can be actually used to yeah, to subvert the system completely.

 **TARANVIR SINGH SAINI .** 57:06  
Yeah, got it.

 **ASHUTOSH BHATIA .** 57:17  
OK.

 **TARANVIR SINGH SAINI .** 57:17  
OK. Yeah.

 **ASHUTOSH BHATIA .** 57:17  
So let's move ahead.  
This is like if EE algorithm case, the encryption key and whenever those so now.

 **VANAM VIJAY KUMAR .** left the meeting

 **ASHUTOSH BHATIA .** 57:26  
Now, yeah, this is more important.

 **SHILPASHREE H L .** joined the meeting

 **ASHUTOSH BHATIA .** 57:28  
How do keys get distributed?  
Means fine.  
We talked about that.  
I think the public key private key I already explained how it got distributed correct?  
But what about the key K Selectric key means?  
How do you when, when you people actually exchange?  
You are far from each other.  
If you how did you send this key to him that see, we are going to use this key, correct.  
So key exchange itself is a is a problem and the Diffie Hellman and all researchers say that I didn't.  
You don't solve the problem of key axis.  
There is no use of encryption as such.  
OK, you can't the problem until unless you don't have a way to securely exchange the key, because to exchange the key sectorally you need encryption, but then that requires another key.  
So then, when did you actually exchange that key?  
Clear you can't send.  
This person cannot decide a key key and just send to him that we are going to use this because then adversary can also see this.  
Do you have any suggestion how this can be done?  
Is there any way something is coming in your mind and how two people can exchange the key over a over Internet?  
OK, it's not like you are sending him the key.  
How you can exchange the key?

 **NEERAJ KUMAR VIJAY .** 58:49  
Using public key like so.

 **SHYAMSUNDAR DAS .** 58:50  
Or we can use the S yeah, we can use the asymmetric key cryptography like the we can use the public key of that person to sign it.  
Sign that key and that person can decrypt it in his private key.

 **ASHUTOSH BHATIA .** 58:59  
Hmm, so this is precisely TLS does.

 **GAURAV SHOREY .** 59:06  
So in this case I mean one can use its own private key which is being given by the authority.  
Likewise, we are using our.

 **ASHUTOSH BHATIA .** 59:18  
There's no authorities in in in, in, in this in cryptographic were not there is no authority.  
So do people just want to exchange?

 **GAURAV SHOREY .** 59:27  
OK.

 **ASHUTOSH BHATIA .** 59:34  
Is the key that anybody can see?  
I cannot use another key card as to encrypt this key using K dash.  
Correct.  
Because then when I actually use this K dash was exchange this K dash.  
So I think somebody talked about you using the public key cryptography.  
This is precisely the DNS protocol does OK, so the way TNS protocol works first is it authenticates the certificate that yes, you are the Google.

 **NEERAJ KUMAR VIJAY .** 59:59  
You know.

 **VANAM VIJAY KUMAR .** joined the meeting

 **ASHUTOSH BHATIA .** 1:00:09  
But now I know the public key your public key, I will generate a a a random key key and I will encrypt that key key using the public key of the server and give it to him.  
He has the private key, he can decrypt it.  
He will also get the key correct.  
So now we both are having the key.  
That's all.  
So if you have already established and authenticated, you have already authenticated the second party and you have his public key.

 **JADHAV PRAJYOT SANJAY .** left the meeting

 **ASHUTOSH BHATIA .** 1:00:42  
That means the public key.  
What you are using is for the right person.  
OK, you you you have to be very careful because anybody can say that I am Google.  
This is my public key and then you will end up setting up a wrong key.  
Mean you are end up setting up a key with the wrong person, thinking that he is Google.  
So you have to 1st authenticate that the public key that you are using for him is for the right person.  
That is through the certificate.  
Once you have done that, you can use simply this mechanism to establish clear clear.  
Say something.

 **JAGADEESAN P .** 1:01:21  
Sir, how do we authenticate the certifications and all here or whether we go to any site to authenticate it uh during the transaction or?

 **ASHUTOSH BHATIA .** 1:01:28  
No, no, I I I talked about this certification authority.  
I talked about this certification 30, so this is the certificate certificate from Certificate basically contains the public key in it.  
There's a standard.  
OK, it's called X .02 standard, which basically says that this is how the certificate should be designed.

 **JADHAV PRAJYOT SANJAY .** joined the meeting

 **ASHUTOSH BHATIA .** 1:01:56  
But let's let's see very minimal public key and the name name is ASHUTOSH.  
Then I get it and then I can I have a digital signature signed by the certification authority and then you have it, the name of the certification authority.  
OK, clear.  
Let's say this is the certificate.  
OK, I give this certificate to you.  
I am ASHUTOSH.

 **SREEKANTH R .** joined the meeting

 **ASHUTOSH BHATIA .** 1:02:27  
Somebody has signed my certificate by verifying my physical documents or whatever he's saying.  
Yes, he's ASHUTOSH and this is his public key.  
The public key I have decided this is a corresponding.  
You can say private key and then there's a public key.

 **SREEKANTH R .** left the meeting

 **ASHUTOSH BHATIA .** 1:02:44  
I generated a pair.  
I gave this public key to him and say that, see, I'm ASHUTOSH.  
You can verify my other documents and sign it, and that's all.  
This becomes the complete certificate.  
Now the certification authority out of the picture.  
See.  
It is just like your icard correct when icard is having your companies, we see CEO signature or VC signature and in case of I academic.  
Yeah, university.  
So we see is not coming all the time correct.  
When you are showing ID card correct.  
So this is this is the certificate any doubt here?

 **JAGADEESAN P .** 1:03:22  
No.  
So this certificate will be, uh, generated by the Google right mission.

 **ASHUTOSH BHATIA .** 1:03:27  
This certificate will be generated by the Google and signed by a cert third party which is called Certification Authority for the group.

 **JAGADEESAN P .** 1:03:34  
OK, got it.

 **ASHUTOSH BHATIA .** 1:03:35  
OK, now I got this certificate and I'm giving this to you.  
This is this is for me.  
Let's say this is I am not the Google I am.  
I am getting a certificate from myself OK and then I you you I'm giving it to you how you will come to know that this public key is right OK what you will do you will see.  
OK, this is the public key.  
Your name is ASHUTOSH and now let me just see verify using the digital signature.  
Now digital signature is reverse when somebody signs this using the digital signature, he actually encrypts the using the private key.  
So this whole certificate he has actually signed using the private key and whatever value comes here.  
Put it here.  
Now I will use the CS public key to verify the digital signature.  
So digital signature has two APIs, one is sign and another is verify sign takes message private key OK and then verify text message.  
Public key. OK, yeah.  
Message and this this message and the public key so basically.  
When you are, when you are verifying you are, you are actually verifying that OK, give me the message.  
Give me the public key and then I will come to know that.  
OK, whether this this signature was correct and when you are signing you are using message and the private key so verify should give me this value.  
Should give me means the one second the there's a message and then there's public key, correct?  
So this is this, should we give?  
This should give me true OK if it is giving me true that so from a programmer perspective you can just think about these two things.  
Sign and verify technically what is happening.  
Signing is nothing but encrypting using private key and verifying is nothing but decrypting using public key in encryption you are encrypting using public key and decryption using private key.  
Clearly it's a very when it's just reverse.

 **JAGADEESAN P .** 1:05:54  
Yes.

 **ASHUTOSH BHATIA .** 1:05:55  
OK.  
So then I will verify now the question is how when did I get the public key off the certification authority?  
Because this person is saying that, uh, this is the certification authority I have used.  
Now let's say it could be possible that my Firefox browser is not having the public key of that certification authority itself.  
Then this could be a hierarchical certificate where it is you saying that this certification 30 public key.  
So this is CAA public key and that has been actually signed by another certificate authority call Service certification 32.  
Then probably I'm having the public key of certificate authority 2.  
So first I will verify this, then I will get the public key of certification authority one there will I will use and sign see.  
It's a verified digest signature.  
OK, so usually the browsers are having root level CS so you can have think about the CS like this.  
OK, so if if you have got it signed directly by this person, then fine, I will just use this public key.  
But if you have signed it using by this person, then you need to put the public key of this person into the certificate itself and then that is being signed by this person.  
And then if this person, he probably is not available, then the certificate should contain the public key of this person in the certificate which is signed by this root certification authority. Clear.

 **MANISH MEHTA .** 1:07:43  
So how many CS will be involved?

 **JAGADEESAN P .** 1:07:45  
So.

 **MANISH MEHTA .** 1:07:45  
I mean, I'm not clear about this one.  
Can you just explain?

 **ASHUTOSH BHATIA .** 1:07:48  
In this, this is something called public key infrastructure.  
OK, this is a very standard term Internet, so usually there are very in in Internet from the when you download a browser there are predefined public keys which you which basically they put it on some kind of repository.  
Your browser keeps on fetching from there, but there's those are very few, so there are some few 3-4 root certification authorities and then you have at second level you have hundreds of certification authorities, so you can keep on making certification authority.  
What's the problem?  
Correct.  
So it's like if my if my photo, let's say access signing if if this is the ID card for me and it is signed by X.  
Now I don't know the the person who is receiving AC.  
I don't know this person X, but then in that somebody has signed that.  
OK, this person is X and it is it's.  
It's basically, but it's a I got it signed by wife.  
OK, now I know why.  
Fine.  
So now I know why I can verify that this is accent that I can verify this is you, Eric.  
So there are very few root level certification authorities.  
So if you go and search in public key infrastructure, you will come to know that you need a PKI infrastructure for the distribution of public keys.  
So public key distribution is also not that much easy.

 **HARSH KUMAR .** joined the meeting

 **ASHUTOSH BHATIA .** 1:09:21  
It's not like it does not come free.  
Does it complete Internet public key infrastructure which is actually an extra burden?  
And then in I, OT and all the tasks that you can't have this kind of heavy certificates, then it becomes a problem that how you will exchange the keys and then it comes in an algorithm called Diffie Hellman.  
They feel Hellman key exchange.  
Have you heard about it?  
Elardo, which basically ensures that you don't need any public key infrastructure.

 **SOMNATH CHATTERJEE .** 1:09:51  
Yes, Sir.

 **ASHUTOSH BHATIA .** 1:09:55  
Magically, I can actually exchange a key with you without in between any third party without knowing any third party that.

 **PANCHAL MAHESH MAROTRAO .** left the meeting

 **ASHUTOSH BHATIA .** 1:10:03  
What?  
What is the key step is between you and me?  
Forgive me, I'm not going to teach the FLW when I got them.  
Because then this will become a cryptographic course.  
Is that fine?  
Because that requires math understanding.  
OK.

 **K AKASH .** 1:10:26  
Yes, Sir.  
So this is this is clear now my question in the same context in the can you go to previous slide so after the first message being sent and and keys have been exchanged.

 **ASHUTOSH BHATIA .** 1:10:27  
So in just yeah.  
Umm.

 **K AKASH .** 1:10:43  
So how would Alice know whether Bob had received it in in decrypted it properly and to rely on that key in future communications?

 **ASHUTOSH BHATIA .** 1:10:55  
Uh.  
The TLS actually maintains a session and it is based on TCP so that they are very much tied up.

 **K AKASH .** 1:11:00  
OK.

 **ASHUTOSH BHATIA .** 1:11:01  
OK, so there's a tailor.  
So whenever you open and first time, let's say you are opening google.com, the TLS comes into the picture.

 **K AKASH .** 1:11:07  
Umm.

 **ASHUTOSH BHATIA .** 1:11:09  
Tales maintains a session.  
OK, the the session means nothing but four different types of keys.

 **K AKASH .** 1:11:12  
OK. Yeah.

 **ASHUTOSH BHATIA .** 1:11:16  
Forget about four keys.  
You just think about one key because there are four different type of keys are used for communication.

 **SAMEER JAYANT DESHPANDE .** joined the meeting

 **ASHUTOSH BHATIA .** 1:11:22  
But let's think that you have maintained a key.  
OK, now let's say you are opening another tab with same same Gmail or same site.  
OK, then it will not actually create a new session.  
This is called the master key.  
OK, this is called the master key and then it will create a different TCP connection for every like SDP makes different easy be connection for every connection.  
For every connection there will be key derived from let's say K1K2K3.  
So for every correction, there will be a key which will be derived.  
So you are not actually because negotiation is a big process and it actually reduces the performance throughput performance.

 **SAURABH RAUTELA .** joined the meeting

 **ASHUTOSH BHATIA .** 1:12:05  
You don't negotiate the key every time, so for every new TCP connection you derive a new key from this master key, and then you use this key for every packet transmission within a TCP connection.  
OK, once the TCP connections are teared down, this is this has no meaning once you stop the close, close your browser this session is down.

 **K AKASH .** 1:12:20  
OK.

 **ASHUTOSH BHATIA .** 1:12:29  
Done.  
This has not done.

 **K AKASH .** 1:12:32  
So you mean after acknowledgment after Bob sends an acknowledgement, probably with the derived key or whichever key which is related to the master key to Alice.  
So keys are eliminated, you mean?

 **ASHUTOSH BHATIA .** 1:12:42  
Yeah, yeah.  
The keys are eliminated and it is actually so then the only the master key and the derived keys are actually stored in a session called TCP session mean TCP is holding that in in data structure because see whenever the packet is coming it has to encrypt so that is there and that's why all this security things come down.

 **K AKASH .** 1:12:54  
OK.  
Got it, Sir.  
Yeah.

 **ASHUTOSH BHATIA .** 1:13:03  
Now let's assume that somebody has hacked your OS, correct?  
He has direct access to your your OS.  
You can say data structures, so this is another problem.  
It's like that is computer security.  
I think when we talk about computer security, that means now unity have to whatever is happening within your computer.

 **K AKASH .** 1:13:17  
OK. Yeah.

 **ASHUTOSH BHATIA .** 1:13:25  
Whether your memory because you are actually storing things, playing in your memory at most crucial thing is the key.  
So if somebody is able to, you can say reach the RAM or like you can directly there's a process which can actually read the OS memory means OS maintained memory.

 **K AKASH .** 1:13:33  
Yes.

 **ASHUTOSH BHATIA .** 1:13:45  
Then you are ready have gone.  
So there are different aspects of security is that it's not like from there the key can be lost and all the things it's a crucial, but this is how the TLS folks should I move ahead.

 **K AKASH .** 1:13:59  
Yeah.  
Yes, Sir.  
Yes, Sir.

 **ASHUTOSH BHATIA .** 1:14:02  
OK.  
OK.  
Thank you.  
Have you argument?  
OK, so one fundamental principle I think I've already talked about keys and kirchoff law in this to maintain security key should be definitely secret.  
OK, but what about encryption and decryption algorithm?  
People tend to secure these algorithm or make secret secret.  
Just that's completely wrong.  
Encryption and decryption algorithms are actually always open and open standards.  
OK, so for example if you are if, if you if there's a lock in some door and and and let's say I'm a thief, I don't have key, but I I also don't know what is the internal structure of this this this log.

 **PRIYANKA SINGH .** left the meeting

 **ASHUTOSH BHATIA .** 1:14:52  
But in cryptography we see that has nothing means people can offline find out that how this log has been made.  
OK, so there is no point.  
The secrets cannot be kept.  
Log OK that especially when you are keeping the code secrets means it is better to have key secret because keys can be changed later.  
So if it is compromised you can change, but if your code is compromised and you are making it secret, are you going to design a new algorithm?  
Did it go to?  
You have to put it on the embedded hardwares then anyhow you have to reveal it.  
You can't keep the code secret all the time because it has to be on public commodities.  
That is for the purpose that see, you should open your code, your algorithm, encryption and decryption so that people whatever like adversaries can try it out and once more and more adversaries had tried out that this and Gorham is good, it is good for that particular algorithm.  
Otherwise, if nobody has seen it, and if there is a weakness in the algorithm itself, and once the secret is lost so we don't buy that path, we go buy this path that see this algorithm is proven to be secure.  
Years and years, people have tried cracking it.  
You don't know that every time and IST puts up a challenge.  
And I steak, what's up?  
A challenge for a DS and all sorts of algorithms that whoever breaks this are we will give you 10,000 or $1,000,000.  
That there's that challenge is always on.  
OK, so that is actually that is you are actually incentivizing people that please break it?

 **ASHUTOSH KANOONGO .** left the meeting

 **ASHUTOSH BHATIA .** 1:16:36  
OK, so now the some of the arguments I think are already talked about, but why you should not keep your algorithm secret and only the key secret is like keys are the smaller programs are larger.

 **NANDAGOPAL NAIR .** left the meeting

 **NANDAGOPAL NAIR** joined the meeting

 **VINOD S R .** 1:16:48  
He.

 **ASHUTOSH BHATIA .** 1:16:51  
OK, easy to replace a key, then the whole program, and infeasible to imagine a secret pair of algorithms for every pair.  
So it's like you are going to communicate, let's say in over the Internet.  
It's a peer to peer communication.  
Means anybody can communicate with anybody in future.  
Are you going to have this?  
This these are end node.  
Then you need N C2 algorithms are you have to have N, C2 pair of antonyms.

 **ADHARSH M** joined the meeting

 **ASHUTOSH BHATIA .** 1:17:18  
What you're trying to say, so algorithm will always be same.  
The only thing is that between these two pairs you will have key secret and that is only when they are actually communicating, correct.  
OK.

 **ISHAAN DEEP SINGH .** 1:17:43  
Yes, Sir.

 **ASHUTOSH BHATIA .** 1:17:44  
OK, so now I'm going to show you that see, the crypto is not only about the the encryption.

 **K AKASH .** 1:17:44  
Yes, Sir.

 **SOMNATH CHATTERJEE .** 1:17:45  
Yes, Sir.

 **ASHUTOSH BHATIA .** 1:17:51  
OK.  
The one thing the crypto can achieve is digital signature.  
We have already talked about what is the meaning of digital signature in principle.  
Digital signature is nothing but you have a content, you have a data and then you run this through a signing algorithm.  
Is nothing but taking the and the private key and generating a piece of.  
You can say that piece of code, piece of information you can say is message authentication code or let's say some people call it digest OK and then you attach this digest here and then you just send this to anybody.  
Now the claim is nobody in this world can create the same digest for this data.  
So your digital signature is is always like with respect to the day.  
Our classical signature, my signature, is always same, correct?  
No, the digital signature is is basically generated by a private key and get depends upon the data.  
So the sign that the digest depends upon the data and the claim is in this world until unless you don't know the private key, you cannot generate this data.  
That's all.  
So anybody who will use this whole thing, that is the data and the digest, what you are providing me and the public key this in the verification algorithm, it will return true or false.  
That means I will just use the public key to decrypt this and I should get the same digest which you are giving me and I will match and then done.  
This is what it's called verification. OK.  
And that this is how the digital signature works clear.

 **VINOD S R .** 1:19:51  
Keep it.  
I will put it.

 **ASHUTOSH BHATIA .** 1:19:58  
Now second part is basically girl anonymous communication.  
Mean anonymous communication is also very important that nobody should be able to know that that actually who is who is talking or who is communicating, like for example, uh.

 **THIYANESWARAN M .** left the meeting

 **ASHUTOSH BHATIA .** 1:20:16  
If if let's say I'm this is this is Google.

 **VINOD S R** joined the meeting

 **ASHUTOSH BHATIA .** 1:20:22  
And uh yeah, Alice is trying to search Google Now, and whatever Alice puts on let's say, let's say, just trying that tell me something about the quantum computing, OK, quantum computing.  
Now that Google knows that this person says this, isn't it correct?  
Is there any way that I can encrypt this so that Google does not know it but Google can still provide me the results which are encrypted and then I will decrypt and I will get my result?  
This is actually a very big problem for different companies.

 **ASHUTOSH KANOONGO .** joined the meeting

 **ASHUTOSH BHATIA .** 1:21:02  
Also, who are running cloud services means we want to run their their data on cloud services or want to take services for cloud services.  
Think about this as a cloud service provider.  
I I have a task data and I want to run one algorithm over.  
I don't have that much.  
You can say computational resources, so I submit this data here.  
You just computed me in and give it back to me.  
The problem is company don't want to submit their data to the cloud, correct?  
They don't.  
They don't trust Amazon that much.  
Is that right?  
Am I right that is the biggest problem by some companies?  
Don't don't actually take the cloud services, especially for their critical projects.  
Am I right?

 **SOMNATH CHATTERJEE .** 1:21:52  
Yes.

 **NANDAGOPAL NAIR** left the meeting

 **ASHUTOSH BHATIA .** 1:21:53  
Yes.  
So The thing is, is there any way that I just encrypt this data and then give it to you you perform computation over this encrypted data and send the result back to me which is encrypted result.

 **NANDAGOPAL NAIR** joined the meeting

 **SHILPASHREE H L .** left the meeting

 **ASHUTOSH BHATIA .** 1:22:12  
That means you yourself don't know what you've computed, but then when I will decrypt, I will come to another result.  
This is called the computation over encrypted data and this has a lot of privacy and anonymity issues.  
Yes, you can say this thing.  
This is hard.  
Have you heard about the homomorphic encryption?  
Normal modifying encryption.  
Have you heard before this term? No.

 **NEERAJ KUMAR VIJAY .** 1:22:40  
No idea, no.

 **ASHUTOSH BHATIA .** 1:22:42  
So I just give you very, very busy because see, this will actually become too much, but I think I just give you the basic of.

 **AMIT KUMAR PANDEY .** 1:22:42  
No.

 **ISHAAN DEEP SINGH .** 1:22:43  
No, Sir.

 **ASHUTOSH BHATIA .** 1:22:52  
This thing?  
Yeah.  
What are you there?  
Is it ice cream now?  
OK, the way the homomorphic encryption works like this, if I have data, what happened?

 **SHILPASHREE H L .** joined the meeting

 **ASHUTOSH BHATIA .** 1:23:10  
And.  
If I have data, let's say I have data E and I want to compute A+B which is equals to C.  
OK, I'm just giving you a very basic example.  
What I want is when you encrypt A and then you add encrypted B then you should you should get encrypted.  
See, so that when somebody is performing computation over this too, he does not know anything about A&B.  
But then he gets encrypted C and I will send get it back and then I will decrypt decryption of encrypted C which is C But it so does your encryption algorithm has this property.  
It is very difficult to means you can't say that when you are actually actually transforming A to something encrypted A and then you are transforming B to something encrypted B.

 **HEMANT ASHOK SALI .** joined the meeting

 **ASHUTOSH BHATIA .** 1:24:16  
But it is still maintaining this arithmetic property.  
You are getting my point.

 **NEERAJ KUMAR VIJAY .** 1:24:24  
Yes.

 **ASHUTOSH BHATIA .** 1:24:25  
This is tough because the point is it starts maintaining this arithmetic property.  
It is saying that it has a very strong correlation with your input values and that encryption scheme itself is not very strong.

 **SIMRAN KAREER** joined the meeting

 **ASHUTOSH BHATIA .** 1:24:38  
OK, that means somebody can then know about the A&B just by looking ENBEB because there is a for example I I give you one thing if A is less than B then encryption of A is less than encryption of B.  
Do you think that this is a secure encryption scheme?  
If encryption has this property.

 **SOMNATH CHATTERJEE .** 1:25:08  
No.

 **ASHUTOSH BHATIA .** 1:25:10  
Why?  
What an attacker can do?

 **TARANVIR SINGH SAINI .** 1:25:11  
No.

 **SOMNATH CHATTERJEE .** 1:25:14  
So one can easily understand that this is something related to any numeric values or like yes.

 **ASHUTOSH BHATIA .** 1:25:19  
All the orderings he can get correct and automatically if he know one of them based case and all, and basically get every information about what you're talking about.  
So you can just keep on encrypting the things and then so it's this is.

 **SOMNATH CHATTERJEE .** 1:25:31  
Yeah.

 **ASHUTOSH BHATIA .** 1:25:35  
You certainly cannot have such properties.  
However, it is shown that the homomorphic encryption, which is this homomorphism property not only for plus, but for multiplication, division and negation.  
You can have this properties.  
It's called fully homomorphic encryption, and then this is very famous nowadays that their standards are actually coming up that actually allow you to perform computation over encrypted data.  
This has many many many use cases.  
I talked about one use case, but this is lot of other use cases.  
OK.  
Uh.  
2nd is like cryptography well known.  
You already know that you can design bitcoins that are there have been the behind the Bitcoin and every other cryptocurrency is the digital cache, which actually allows people to anonymously.  
What means?  
Forget about all those government laws and all they're not talking about that.  
But digital cache is the one which can anonymous digital cash and cash equivalent and electronic equivalent cash.  
I'll leave it to electronic equivalent of your physical currency notes, which provide you the very similar of services like anonymity and anonymity in the sense that if I'm having a currency that means a node, and if I give it to you or maybe to to some vendor, the point I leave from that place, nobody can tell that who who from where this came and actually who is owner of that, the current Paytm system and whatever you are learning, they are completely centralized and they are lecture based centralized.  
They know they know each and every transaction, so the digital points and digital currencies are totally different concept than this.

 **NANDAGOPAL NAIR** left the meeting

 **NANDAGOPAL NAIR** joined the meeting

 **ASHUTOSH BHATIA .** 1:27:32  
This thing I think he mudra the Government of India has as it started.  
It's called CDC, Central bank digital currency, which is based on this whole principle.  
You can right now go and download the E Mudra app and then you can get some CDC in your wallet.  
If you are from Bangalore and all I think from there the bank services are already started so you can see I I don't know how many people will you get so that you can actually exchange with them the CDC but the CDC has started in India and we really that in one year this is going to be a push from every because this actually provides government much more control over this.  
So means actually just started with anonymity, but that's a different that that I'm not going to discuss.  
No government is happy with the anonymous people holding anonymous cashes.  
Uh, so let's not go into the much detail of this, but this is 1 application which actually came in.  
Then not only just encryption, yeah.

 **NEERAJ KUMAR VIJAY .** 1:28:34  
How to buy it?  
I'm saying how to buy it.

 **ASHUTOSH BHATIA .** 1:28:40  
How to buy what?

 **NEERAJ KUMAR VIJAY .** 1:28:42  
Not this digital currency in India and.

 **ASHUTOSH BHATIA .** 1:28:45  
You don't have to buy see when you start your wallet.  
You have to give your hard card and everything, and then your bank account and everything.  
And then in your wallet.  
So let's say for you, you just say that, OK, you threw UPI or whatever, you just get 10 coins or so.  
It's like in ₹5.10 which they have mudras and that denominations.  
So you can either get in that denominations as well.  
So from your account you just convert it into the mudra and then spend it in ANURADHA with somebody else.  
So there's no veganism of buying.

 **NEERAJ KUMAR VIJAY .** 1:29:22  
OK, OK.

 **ASHUTOSH BHATIA .** 1:29:23  
So yeah.  
Yeah.  
So that's a yeah.

 **TARANVIR SINGH SAINI .** 1:29:24  
So, so so how, how are they?

 **SOWMYA N SWAMY .** 1:29:25  
But Sir, is it legal, Sir?

 **ASHUTOSH BHATIA .** 1:29:26  
But but but yes, but yes, let's.

 **SOWMYA N SWAMY .** 1:29:29  
Is it legal?

 **ASHUTOSH BHATIA .** 1:29:30  
So CPTC CPTC is by government.  
So you are confusing with cryptocurrency and CDC.

 **SOWMYA N SWAMY .** 1:29:35  
OK.

 **ASHUTOSH BHATIA .** 1:29:38  
OK.

 **SOWMYA N SWAMY .** 1:29:39  
Yes.

 **ASHUTOSH BHATIA .** 1:29:39  
No, no, no, no, no.  
The CBDC isn't is it?  
Answer from all over the country by the government to the cryptocurrency.  
It is actually cryptocurrency was decent realized.  
OK, decentralized and the CDC centralized, but there were some use things like recent lies, but it was actually a kind of E cash.  
But then the Paytm and all what you use involve banking.  
So this centralized is based on cryptography, that is similarity with decentralized like Bitcoin and also it provides you peer to peer exchange which actually the ATM all does not provide.  
You let the bank involved, so that has borrowed some of the concepts of you can say the the crypto at the peer to peer gas and to reflect the the very nature of the currency that nodes Ital points.  
But it is centralized.  
It is centralized.  
The government knows each and every transaction that what you're making, OK?  
So it is centralized.  
That's called CBDC Central bank digital currency go to RBI site.  
They have already installed in startups.  
OK, what you are talking about, legality and all this cryptocurrency, hundreds of cryptocurrency, OK?  
Do it.

 **K AKASH .** 1:31:07  
Yes, Sir.

 **SOWMYA N SWAMY .** 1:31:08  
Yes, Sir.

 **ASHUTOSH BHATIA .** 1:31:09  
Please go ahead and read.  
CDC means India, US, Europe, everybody has a started their own and this is the future because let me tell you, I think I really do not want to go into the economics.

 **JAYARAM MUHAMMED .** left the meeting

 **ASHUTOSH BHATIA .** 1:31:23  
You have a PTM wallet or whatever bank account and this person is having bank account there.  
There is a bank is there if you go to the foundations of economics, you will find that when you are actually sending money from here to here, this person is maintaining his own lecture.  
Correct.  
Like it will detect money from here and this.  
This is not rupees which is actually promised by the RBI.  
So one thing, unless these ledgers are not verified that what internally they are doing, so this money is a promise of bank.  
This money is not a promise of RBI.  
You're getting my point.  
Means I can I as a bank I can keep on doing frauds even if I don't have money.  
I'm just keep on adding the values because I'm just promising you that I've done it that there are a lot of prods.  
Technically, when bank is maintaining the Ledger, it is his promise of a new currency.  
His you are.  
You are dealing with.  
You're not dealing with the rupee rupees.  
So if you go with the basics of economics and this thing, you'll come to understand that why all company, all actually governments are trying to push because they just want to remove this and now you are directly connected to the RBI through this.  
So the banks are out of the picture.  
So you got this point out like bank is maintaining your Ledger, which is his promise that I have given.  
It is not exactly the rupee of the currency equivalent of RB I promise.  
Because the RBI promises that whenever you come back to me and give me this ₹20 note, I will give you equipment amount of gold.  
OK.  
However, that also they are not, but there is a promise that I will give you something worth of ₹20 if you just want to surrender your ₹20 back to me and then in US.  
This has happened long multiple times when the during recession, people said that I don't want this.  
Give me.  
Give me my my, my, my equivalent amount of gold bag.  
Then they say, then no, no, no, that cannot happen.  
It will actually reduce.  
So there are a lot of things involved in this, OK.

 **K AKASH .** 1:33:43  
Yes, Sir.

 **HEMANT ASHOK SALI .** 1:33:44  
Alright Sir.  
But then if there's a CBDC is there and it doesn't have any endorsement of the RBI, then who will back it up?

 **SAURABH RAUTELA .** left the meeting

 **ASHUTOSH BHATIA .** 1:33:52  
CBTC has endorsement of RBI.  
The Paytm has no endorsement of Ravi, the the bank account has no endorsement of Ravi.

 **HEMANT ASHOK SALI .** 1:33:55  
OK, it has no.

 **SAURABH RAUTELA .** joined the meeting

 **HEMANT ASHOK SALI .** 1:33:58  
OK, OK.

 **ASHUTOSH BHATIA .** 1:34:02  
Because it is their lecture.

 **HEMANT ASHOK SALI .** 1:34:02  
OK.  
Yeah, but they're operating under Arabia and ultimately in India.

 **ASHUTOSH BHATIA .** 1:34:08  
Doesn't matter, but they're knowing farts.  
Technically it is.

 **HEMANT ASHOK SALI .** 1:34:12  
But that is because.

 **ASHUTOSH BHATIA .** 1:34:13  
It is by trust.  
It is not by design and it it is not by the privacy the the trust you what you are getting is by that, OK.

 **HEMANT ASHOK SALI .** 1:34:15  
Yes.

 **ASHUTOSH BHATIA .** 1:34:23  
The law is there, everything is there and all, but this is the problem that they are facing a lot of frauds.  
The bank frauds actually over out of the out all over the world are the maximum frauds as of now in the fabric country.  
Second point is why CDC is coming is like governments have already realized that.

 **ANUBHAB SAHU .** left the meeting

 **ASHUTOSH BHATIA .** 1:34:43  
See if we don't do this, people will keep on generating their own equals because technology allows them.  
So people will create silos like OK means Elon Musk will create own currency.  
The MSN will create own currency and then they will start running their own own currency within their ecosystems.

 **ANUBHAB SAHU .** joined the meeting

 **ASHUTOSH BHATIA .** 1:35:02  
We got technology allows them, OK, this is going to be out of the hand from the government if they don't control this.  
So anyhow, you can't stop.  
You can't just stop because the technology is available, so you should have an option of digital currencies, otherwise it will.

 **ANUBHAB SAHU .** left the meeting

 **ASHUTOSH BHATIA .** 1:35:22  
It will create a means that then people will start running their own economies and where and all you will go and catch them.

 **ANUBHAB SAHU .** joined the meeting

 **ASHUTOSH BHATIA .** 1:35:28  
It's very difficult.

 **HEMANT ASHOK SALI .** 1:35:35  
Mustard.  
Then it will be like different barter systems coming up.

 **ASHUTOSH BHATIA .** 1:35:35  
OK.  
Yes.  
So.  
So it's like a because of the technology means if you go to the US net, uh hearings, most of the hearings nowadays are happening in coming up the regulations about this cryptocurrencies and CDC's because they have realized that there's no way that we can actually shut our eyes and make the very strong regulations because even if we do that, uh people will do all these things.  
So it they're just able to find out a very good balance between adopting the technology.  
But at the same time, avoiding the threats during this technology, because if you adopt this technology, you can say just like this without any regulations.  
Then also your company your, your, your country could be in thread.  
For example, people will like in Africa, people use dollars instead of their own own currency, correct?  
They don't trust on their own currency, you know that.  
So what?  
They say that three, whenever you are giving them dollar, it's fine because I know that this has value.  
It this promise is more better tomorrow.  
My my government can simply say that no, it has no value.  
Can't do anything, so it's all about from where the trust is coming and that's why the South African government has made Bitcoin has the official that is the first country was made the Bitcoin as the official.  
So they send that, OK, this technology is anyhow established.  
Let's make this itself as an official guidance.  
So once those some countries where the trust is very less on government.  
Ohh I need help.  
People started using some alternatives so and also there's a problem like like in Sri Lanka and all people start accepting other countries currencies.  
So it's like it's a so.  
So open word that you you can't stop things so that the government has lot of challenges to basically handle all these things is these things are happening.  
OK.  
Should I go ahead?

 **HEMANT ASHOK SALI .** 1:37:51  
Yes, Sir.

 **SOMNATH CHATTERJEE .** 1:37:52  
Sir, I have one small question like from the last topic, we were seeing the homomorphic computation.

 **KUMARI MENKA RAUSHAN .** left the meeting

 **SOMNATH CHATTERJEE .** 1:38:00  
So this homomorphic computation.

 **ASHUTOSH BHATIA .** 1:38:01  
Hmm.

 **SOMNATH CHATTERJEE .** 1:38:03  
So when we are doing so, is it not like it will?  
It is much more time taking for encryption and.

 **ASHUTOSH BHATIA .** 1:38:11  
Yes, yes.  
Well, morphing computation technology or and you say that as per this as of now this is not first of all as secure as the classical encryption.  
That is one thing.  
Uh, that means the modern encryption scheme, because anyhow you are leaking some information, whatever you do.  
So the math and research is going on first thing and second thing is it actually uses the the concept of introducing a lot of errors in the data so that when you are performing computation, you're still works but you cannot do this.  
So there's a there's a concept of introducing errors, and then you actually make the data much more larger.  
So it is computationally inefficient, but that's a trade off the privacy versus I and then now people are looking for quantum homomorphic communication.  
So then that that computation part can be handled by quantum.

 **SOMNATH CHATTERJEE .** 1:39:12  
OK.

 **ASHUTOSH BHATIA .** 1:39:13  
OK, so now let's move ahead.

 **SOMNATH CHATTERJEE .** 1:39:13  
Thank you. Yeah.

 **ASHUTOSH BHATIA .** 1:39:15  
Another interesting application apart from this encryption integrity and all that offer offer you can say cryptography is to design some interesting protocols which you cannot achieve without the cryptography and one of them is like think about I'm giving you an example of you can say Nicole secure multiparty computations.  
It turns of thesis people are doing in the secure multiparty competition as of now.  
Mathematically, the secure multiparty computation can be defined like this.  
Let's say there are N parties.  
Maybe you can think about you people and everybody know your salary.  
Correct your salary is this one is X1 and this one is X2.  
This one is X3.  
This one is X4 and this one is X5.  
Now you want to come up.  
You want to compute a function of this X1 X 2X4 X Y5 that is called some function F from next to X5.

 **PRIYANKA SINGH .** joined the meeting

 **ASHUTOSH BHATIA .** 1:40:19  
Uh, so that let's say that function is nothing but average.  
You want to know the average of salary of of this group of people.  
But then the problem is you really don't want to reveal.  
Nobody wants to reveal their own salary.  
OK, so you want the average of this and nobody wants to reveal their own self first you think and tell me what can?  
How can you do this?  
First, you assume that there is a trusted authority.  
OK, let's see.  
One possibility is you just everybody gives X1 X 2X3 X 4X to this the trusted and RT will actually compute X12.  
This thing calculate the arrest.  
Give back the result.  
OK.  
But then see you contact, accept any trusted guard because you have revealed the X1 to extend to him.  
So now the next question is, can it be possible means even I talked about homomorphic correct, can it be possible that you sent afford to the tested party like you sent encryption of X1.  
You sent encryption of X2 and then encryption of XN and then you should be able to compute the function that whatever you want because this is in general it's called secure multiparty computation.  
That means and there is a theorem in cryptography which says that in a distributed system, which says that if you can achieve this using a trusted third party, you can always come up with a distributed protocol.  
That means the end parties get involved in certain kind of communication so that they can.  
They can come up with a single value or they can perform some computation F on the secret values which are being which are actually holded by different parties.  
OK, so this is this this you can also think about as voting.  
OK, so let's say this person votes.  
There are four two parties, zero and one.  
This 40 this words to one and then I want to calculate just the maximum of like how many votes a particular party got.  
So if zeros are more party A1, if one has more party B1 Now you don't trust any third party because for this computation, but you just want to have a secure communication between yourself, you don't want to tell your each other your values.

 **KUMARI MENKA RAUSHAN .** joined the meeting

 **ASHUTOSH BHATIA .** 1:42:49  
That what is your but ultimately I should come up with the Maxwell.  
OK, so secure pointing wanting computation has many like in blockchain.  
Because in blockchain you do the computation in all computation in public, but at the same time you want the security that you don't want to reveal that.  
What is your value?  
So in in auctions, so there are many, many, many, many you can say applications and scenarios where you need such kind of the.  
Yeah, you can say such kind of.  
Computation where you want to do secure multiparty computation, and I'm not going into the detail of like there are multiple algorithms, but just to just to talk about.  
Like if you want if I say give the give you if I give you this problem as a puzzle.  
Let's say there are three people they want to know each other's salary.

 **DIVYA JYOTI MISHRA .** left the meeting

 **ASHUTOSH BHATIA .** 1:43:46  
OK, they are ready to communicate some message to each other.  
What is your solution so that nobody knows each other salary but at the same time they come to know the average?  
So this is this could be the most basic thinking, but this whole thing is based on the cryptography and then yeah, there are protocols there are there are libraries, so don't think it like this.  
Just know when there are libraries, Python libraries, you can you can do secure multiparty computation and everything is there.  
OK, it's not like so any any idea?

 **HEMANT ASHOK SALI .** 1:44:26  
So like we can have some dummy user and with him some dummy salary.

 **ASHUTOSH BHATIA .** 1:44:31  
No, no.  
Let's forget about it.  
I have already proved that if you can add the user, these people can do it.  
So this is the fundamental theorem.

 **HARSH KUMAR .** left the meeting

 **ASHUTOSH BHATIA .** 1:44:38  
So that means there is an.

 **HEMANT ASHOK SALI .** 1:44:38  
OK.

 **K AKASH .** 1:44:39  
Umm.

 **ASHUTOSH BHATIA .** 1:44:40  
There is a way to do it distributed manner as well.

 **K AKASH .** 1:44:44  
Sir, each one can ask a approximate range.

 **ASHUTOSH BHATIA .** 1:44:50  
OK.

 **K AKASH .** 1:44:50  
Do everyone and based on that approximate range, we can perform several calculations and get to know the average or.

 **ASHUTOSH BHATIA .** 1:44:58  
I would call it will it?  
Will it be a great?

 **K AKASH .** 1:45:01  
No, no, definitely not the accurate, but.

 **ASHUTOSH BHATIA .** 1:45:03  
What is the all working for accurate?  
So let's say this one is X.  
This one is having salary called Act this win.  
This one is X1, this one is X2.  
This one is X3.  
Let's say I just decided that this is starts.  
This will add some random generator, random number R&X 1 + R and give it to this.  
Get next two.  
Come to know what is this excellent space?  
You can we come to know what is a celery.  
So let's say this is our no, but it does not know.

 **HEMANT ASHOK SALI .** 1:45:36  
If he knows are then only.

 **ASHUTOSH BHATIA .** 1:45:40  
Now I'm just giving you X1 plus R1.  
I'm not giving you.

 **HEMANT ASHOK SALI .** 1:45:45  
Then you don't.

 **ASHUTOSH BHATIA .** 1:45:45  
So how will you and act now?

 **HEMANT ASHOK SALI .** 1:45:46  
You cannot.

 **ASHUTOSH BHATIA .** 1:45:49  
The X2 will generate another random number R2 and then it will generate random number R2 and to this person it will give X1 plus R1 plus R2.  
And this person? No.  
Sorry, not not this.

 **K AKASH .** 1:46:09  
So is it a game theory you are talking about?

 **ASHUTOSH BHATIA .** 1:46:11  
This is X2.  
No, no, no, no.  
This is not game theory.  
This is 1 simple protocol which will explain you that how a simple secure multiparty computation in a distributed can happen by exchanging the messages in a particular way.  
If this is giving X1 plus R1 plus X22X3, does X1 has any way of knowing X3 BSB CC has any way of knowing what is X1 and what is X2?

 **SOMNATH CHATTERJEE .** 1:46:45  
Umm.

 **ASHUTOSH BHATIA .** 1:46:46  
Correct.  
Then she will add X3 in it.  
So this will become X1 plus X2 plus X 3 + R correct?

 **ASHISH KUMAR BHATTACHARYA .** left the meeting

 **ASHUTOSH BHATIA .** 1:46:59  
Now, does X1 is having anyone any way of knowing what is X1?

 **SOMNATH CHATTERJEE .** 1:47:00  
Yeah.

 **ASHUTOSH BHATIA .** 1:47:04  
What is X2 and X3?  
It knows X1 and R.  
Correct.

 **HEMANT ASHOK SALI .** 1:47:16  
Yeah.

 **ASHUTOSH BHATIA .** 1:47:18  
Then it will simply minus R from here this will become a X1 plus X2 plus X3.  
It will do divide by three.  
This is the average.  
It will communicate average to each other.

 **ASHISH KUMAR BHATTACHARYA .** joined the meeting

 **ASHUTOSH BHATIA .** 1:47:31  
This has a lot of flowers and there are a lot of attacks means I'm just giving you a very basic protocol to make you understand that how the secure multiparty computation then then actually the problems will start.  
What if this is a broad?  
Is it what if this is a broadcast channel?  
That means when you are communicating to this also this person is also listening, then this is broken, isn't it?  
Correct.

 **PRATHIGUDUPU SAI CHARAN RAJ .** left the meeting

 **HEMANT ASHOK SALI .** 1:48:03  
Yes, Sir.

 **SOMNATH CHATTERJEE .** 1:48:04  
Yes.

 **ASHUTOSH BHATIA .** 1:48:05  
So I'm not going to that detail, but this is this is I'm just giving you the glimpses that cryptography is not only about encryption.  
It has many, many many applications other than the encryption means which are kind of think magical to to this the cryptography in the math is is usually whenever things look like magical, the cryptography has answer now.

 **SHILPASHREE H L .** left the meeting

 **ASHUTOSH BHATIA .** 1:48:32  
Uh, yeah, this I anything I already talked about privately.  
Outsourcing computations?  
So you have let's say search query you are giving it to Google but Google should not come to know that what actually search encrypted Sally should come.  
So this is what is called one thing and then one of my favorite winners in the actually I also work on is called 0 knowledge proofs.  
Anybody heard about it?  
This is very like very high.  
You can say lots of mathematics, but it's a very magical concept.

 **NEERAJ KUMAR VIJAY .** 1:48:58  
Yep.  
Yeah, I have heard it and use some papers, but yeah.

 **ASHUTOSH BHATIA .** 1:49:13  
Can you?  
Can you just explain in a layman word what does it mean by?  
What is the meaning of 0 knowledge proofs and this is now the reality.  
Now the zero knowledge proof.  
Three years back was like a concept, but now you have libraries and you can achieve it very easy.  
So is there anybody who can explain in just a simple language that whatever alternately we are trying to do with by zero knowledge groups?  
So you don't know this provide give you any simple then let's say this is take this example.  
Let's say you you know you have been given an an integer which is actually the multiplication of two prime numbers.  
You know that if I just give you N, it is very hard to find out two prime numbers because based on this, the whole cryptography RSA algorithm is dependent, correct?  
If somebody breaks this, then your cryptography is broken.  
So this is a hard problem.  
OK.  
If I give you N it is hard to find out what is that and is the composite number my.

 **BHAVANAM NAGA SAHITYA .** joined the meeting

 **ASHUTOSH BHATIA .** 1:50:28  
After getting multiplication of two prime numbers, if I give you P&Q it is simple.  
You just multiply and get N, But if I give you N it is hard to find what is P&Q OK.

 **BANJAM DEWAN .** left the meeting

 **SOMNATH CHATTERJEE .** 1:50:43  
Yes.  
Is.

 **ASHUTOSH BHATIA .** 1:50:45  
First of all, why I'm saying it is hard to find.  
Can anybody give me an A simple?  
I will order that I give you NI telling you I'm telling you that this is actually a multiplication of two prime numbers.  
You give me an algorithm.  
What you will do just a layman algorithm, let's think about why it is hard.  
Otherwise it you won't be convinced.  
What is the algorithm that could be a simple algorithm?

 **HEMANT ASHOK SALI .** 1:51:05  
It's more like factorization, Sir.

 **ASHUTOSH BHATIA .** 1:51:10  
How we will do now?

 **NEERAJ KUMAR VIJAY .** 1:51:10  
This week, that prime number is 2 prime number of two large integers.

 **ASHUTOSH BHATIA .** 1:51:10  
Give me the algorithm.  
No, you mean the steps I am giving you an let's say this is a function.

 **K AKASH .** 1:51:33  
Sir, probably divide a the number with the prime number.

 **ASHUTOSH BHATIA .** 1:51:34  
To yeah.

 **NEERAJ KUMAR VIJAY .** 1:51:34  
Like.

 **K AKASH .** 1:51:39  
I know.

 **ASHUTOSH BHATIA .** 1:51:40  
But see to get the next prime number itself is a difficult is a function problem.  
Means what is the next prime number?

 **K AKASH .** 1:51:49  
Ohh.

 **ASHUTOSH BHATIA .** 1:51:49  
This is the there is a list of prime numbers, right?  
This is a prime.  
This is a prime.  
This is a prime the prime numbers are very funny.  
They don't have any specific correct, so that helps with the problem, it's.

 **K AKASH .** 1:51:56  
Yeah.  
Yeah, Sir.  
We can get the factors and if we get more than, let's say two prime numbers, we have to do just combinations which will bring us the in.

 **ASHUTOSH BHATIA .** 1:52:08  
See.  
No, no.  
Uh, let.  
Let's see.  
Very simple why you are making so things like so complicated US start let's say for I equals 21212 under Root NI just go up to this point OK.

 **LAD HARSH AMIT .** left the meeting

 **ASHUTOSH BHATIA .** 1:52:30  
Fine.  
Then I will say that OK.  
Uh divide and by eye, and then you will get some some value.

 **NEERAJ KUMAR VIJAY .** joined the meeting

 **ASHUTOSH BHATIA .** 1:52:43  
But let's say, let's say you get X OK.  
Now if first of all one second, if I is a prime number, OK, if I is a prime number then you divide north by I and if it divides properly then whatever next you get let's say J then that means I and J are those numbers prime numbers which multiply which achievement correct?  
Because the factorization is always unique for any number.  
So if N is a prime, that means I, I and NYIJ.  
That means I and J are those pairs, correct?

 **AMIT KUMAR PANDEY .** 1:53:27  
Yes, Sir.

 **ASHUTOSH BHATIA .** 1:53:29  
So then you just and then why I'm saying that you just have to go up to route end.  
Because see means ultimately either of P or Q will be.  
That will be one number which will be less than equals to root N means is there any doubt in this?

 **SHIRSH GUPTA .** left the meeting

 **ASHUTOSH BHATIA .** 1:54:02  
Either means either pay and you both are same, correct?

 **ASWIN .P .** 1:54:03  
Sure.

 **ASHUTOSH BHATIA .** 1:54:06  
Are one baby listen another will be higher means.  
Why?

 **SOMNATH CHATTERJEE .** 1:54:13  
Yes, yes.

 **ASHUTOSH BHATIA .** 1:54:14  
So you're just going up to root it and then you will certainly find it some, some number which will like basically gives this.  
So what is the complexity of this algorithm?  
They are going up to root and if N is an small N bit number, what is this rooted?

 **NANDAGOPAL NAIR** left the meeting

 **ASHUTOSH BHATIA .** 1:54:38  
If N is in bit root number, then root N is how many bit Nomura.  
And bike OK?  
I asked when bite door and minus one.

 **SOMNATH CHATTERJEE .** 1:54:48  
It.  
In by two.

 **TARANVIR SINGH SAINI .** 1:54:53  
N by two.

 **ASHUTOSH BHATIA .** 1:54:54  
And OK, so now if N is this number in RSA, is it this is a 2048 bit number that means N by two is 1024 bit number and that means two is to power 1024 rounds.  
You have to go forget about it.  
No supercomputer, no quantum computer.  
Nobody can do this in all light years.  
Correct.  
So that means am I clear that this this isn't a hard problem now, there are lots of misheard problem because I'm making the number of bits in very large.  
OK.  
I mean, I'm not saying that you are.  
You're just trying to find it for when an equals 200, then.  
OK, fine up to ohh.  
I'm up to 10.  
There is one number I would just iterate it and find it.  
What's the problem correct?

 **K AKASH .** 1:55:55  
Here's a so you are making the encryption is longer.

 **ASHUTOSH BHATIA .** 1:55:56  
So.  
Yeah.  
So this is actually standard 204 in bit is actually as of now for RSA.  
OK.  
Do you use and large?  
That's otherwise that is not secure.  
You use enlarge.  
This is how the RSL algorithm works, and I'm just taking the example from RSL once.  
However, zero knowledge proof is a broader concept.  
I will explain.  
So the idea is that you know the answer to a hard problem.

 **DURVASULA DEEPIKA ANNAPURNA** left the meeting

 **ASHUTOSH BHATIA .** 1:56:29  
OK, not let's assume you know why.  
Do you know?  
Because see you if you yourself generate a random pee and then you you basically P&Q and you multiply, then you will get some N and now you are saying to somebody that say I know the factorization of N so it means that you only generated this and nobody if I just if I give this end to somebody else for him it is very hard.

 **SHIRSH GUPTA .** joined the meeting

 **ASHUTOSH BHATIA .** 1:56:54  
This is the same principle, but we talked about public key and private key pair generating public key and private key pair is simple but for given public key, finding out the private key is in hard problem which is based on this hardness and similarly getting public key from from private key is same thing.

 **DURVASULA DEEPIKA ANNAPURNA** joined the meeting

 **ASHUTOSH BHATIA .** 1:57:16  
So that's the crux.  
OK, this this factorization is the crux of RSL.  
Gotham means every five years some good researcher comes up and says that.

 **C RUKMANANDUDU .** left the meeting

 **ASHUTOSH BHATIA .** 1:57:26  
See I have found very efficient algorithm.  
Then everybody says that no, no, there is this flow that flaw.  
So this is a kind of bread and butter for the researchers that if I you have, you have cracked it, the whole cryptography you you just stop using banking accounts and everything because the day this is broken somebody comes up with a good algorithm.  
Uh, so smart way of finding out this then then then.  
Now think about something else.  
OK, but fortunately mathematics there are many other hard problems which are not broken, so they will simply shift to some of that.  
Let's it's a mathematical problem, OK?  
Should I move ahead?

 **SOMNATH CHATTERJEE .** 1:58:06  
Yes, Sir.

 **HEMANT ASHOK SALI .** 1:58:06  
Yes.

 **ASHUTOSH BHATIA .** 1:58:07  
Now yes, yeah.

 **TARANVIR SINGH SAINI .** 1:58:08  
Also one more thing.  
So.  
So let's take an example of over 2 Windows.  
So basically there, but it it is like when you're authenticating to some other site, it's not telling the source that what's the username or the password.  
So can we?

 **ASHUTOSH BHATIA .** 1:58:23  
Yeah, yeah, yeah.  
So this is one of the one of the you can say application of 0 knowledge.

 **TARANVIR SINGH SAINI .** 1:58:30  
OK, OK.  
So it's basically not revealing that and just telling that he knows that, OK.

 **ASHUTOSH BHATIA .** 1:58:32  
OK.  
I yeah.  
So I I am coming to that one.  
So the idea is, you know something, you know the solution to a hard problem?  
Mathematically, password cracking the password is assumed to be a hard problem.  
OK, so doesn't matter.  
You know the solution to a hard problem and to your authenticator this could be the authenticator.  
This person says that let's say let's say this is your username and is your username.  
So let let's try to understand in your context what you have given.  
I generate the PNQ, I get NI give N to the server and I say that tomorrow whenever I want to authenticate to myself to you, server will throw me a challenge that see give me the factorization means no not give me the factorization.  
Prove me that you know the factorization of N without giving me the factorization.  
That's the crux.  
So I will be able to convince you that I know the factorization without giving you the factorization is called 0 knowledge proof.  
I'm not conveying any knowledge to you because as of now, what is the password base you ask the password?

 **NEERAJ KUMAR VIJAY .** joined the meeting

 **ASHUTOSH BHATIA .** 1:59:51  
I give you the password, but that means you are also having the password, isn't it?  
When you are authenticating me by taking my password, you are having the password so server if the server is compromised, I'm gone, isn't it?

 **SOMNATH CHATTERJEE .** 2:00:10  
Yes.

 **ASHUTOSH BHATIA .** 2:00:11  
So can't I have mechanism that you just ask me?  
I will convince you I know the solution to the heart problem in general, or I just convince you that I know the password without giving you the password.

 **ASHUTOSH KANOONGO .** left the meeting

 **ASHUTOSH BHATIA .** 2:00:23  
That's the correct soft zero knowledge proof, so I give you a very you can say the basic example from where this zero knowledge proof is started and I think with this I will end OK the the this will actually show you that how the zero knowledge will works.

 **ASHISH KUMAR BHATTACHARYA .** left the meeting

 **ASHUTOSH BHATIA .** 2:00:41  
That means how I'm able to convince you that I know the password without even telling you the password.  
OK, so let's just take The Cave example.  
Very famous cave example which we teach in cryptography.  
There are two people.  
OK, The Cave entrance is here, and then once you enter from the crease here and then you reach at this position, then you have two parts either.  
You can think about like the password is fully just simsim or something.  
Now two parties are there.  
A&BA claims to B that I know that password of this.  
But B says OK, tell me then it says no.  
I will not tell you, but then how do you convince me that you know the password for this?  
That means you know the the magical word which will open this door, and then here is the the the process which will demonstrate that without communicating the password to be a is able to convince B that I know the password.  
OK, that's the basis of 0 knowledge proof.  
So let's see how it works.  
First, A will go here and reach here first.  
A will go.  
It will go here and reach here and then he will decide.  
It will take a decision.  
Either it will go decide or it will go this side once a S goes decide and it disappears.  
OK, let's say it reaches here.  
Then we will start and come here.  
OK.  
Then we will start, we will start and come here now.  
Here, let's assume that we can shout and we can listen that come from the right side or come from the left side.  
So this is actually a challenge from B, so B will throw a throw a challenge to A to come from either left side or right side and that he will decide randomly.

 **ARUN R .** left the meeting

 **ASHUTOSH BHATIA .** 2:02:50  
So that means B does not know what is going to say till this point I'm clear.

 **SOMNATH CHATTERJEE .** 2:02:59  
Yes.

 **ASHUTOSH BHATIA .** 2:03:01  
Now, what happens if, let's say the the A is here and a knows the key he says come from my right side.  
That means they will simply go back and go from here.  
OK.  
But if you're saying come from my left side, he will open the door.  
Go from here and come back from here.

 **ASHISH KUMAR BHATTACHARYA .** joined the meeting

 **ASHUTOSH BHATIA .** 2:03:19  
So if he knows the key, he will always be able to come from the right side.  
From there, the ABI is asking him to correct.

 **NEERAJ KUMAR VIJAY .** 2:03:30  
Tracking.

 **ASHUTOSH BHATIA .** 2:03:39  
Is that correct?  
But say something.

 **SOMNATH CHATTERJEE .** 2:03:49  
Submit if B knows knows the correct.

 **ISHAAN DEEP SINGH .** 2:03:51  
Yes, Sir.

 **SOMNATH CHATTERJEE .** 2:03:55  
Means a key.

 **ASHUTOSH BHATIA .** 2:03:56  
If it knows the key to the door, he will be able to pass the challenge thrown by me every time.

 **SOMNATH CHATTERJEE .** 2:04:06  
Yes, that is true, yeah.

 **ASHUTOSH BHATIA .** 2:04:07  
Correct now, but he does not know the key.  
What is his probability that for a particular time he will win?

 **ISHAAN DEEP SINGH .** 2:04:20  
.5.

 **ASHUTOSH BHATIA .** 2:04:22  
.51 by two now.

 **SOMNATH CHATTERJEE .** 2:04:24  
Yes.

 **KUMARI MENKA RAUSHAN .** left the meeting

 **ASHUTOSH BHATIA .** 2:04:24  
I will repeat this process, let's say 20 times.  
If I know the key, I'm very time I will be successful.  
But if I don't know the key, what is the probability that every time I'm successful 20 times?

 **SOMNATH CHATTERJEE .** 2:04:41  
Yes.

 **ASHUTOSH BHATIA .** 2:04:43  
What is the probability?

 **K AKASH .** 2:04:45  
If you don't know the key lesser than I mean 20 maybe.

 **SOMNATH CHATTERJEE .** 2:04:45  
No.

 **ASHUTOSH BHATIA .** 2:04:51  
One by two raised to power 20.  
Correct.

 **HEMANT ASHOK SALI .** 2:04:53  
Yeah.

 **ASHUTOSH BHATIA .** 2:04:54  
So that is like one by two into one by two into one by two, correct?

 **G PHANI KUMAR .** 2:04:56  
To me.

 **TARANVIR SINGH SAINI .** 2:05:00  
Yes, Sir.

 **SOMNATH CHATTERJEE .** 2:05:00  
Yes.

 **ASHUTOSH BHATIA .** 2:05:02  
Which is miniscule.  
That is based on this probabilistic fact that if you don't know the key, it is difficult for you because it is nearly impossible for you to win this game every time.  
So I will do this challenge response means challenge a random challenge because you don't know what sequence are will ask.  
So you can't prioritize side that.  
See, this is called the there's a concept called Witness and challenge.  
I'm not going into that detail, but the idea is that in prior you don't know what is, what is the path you're going to take at night.  
No, not not this party.  
Not that party, and that is the crux.  
That's the I actually can convince you that I know the key without in without dealing with the password.  
OK, so I maybe I will give it another example.  
Next class there there's a class.  
Maybe you can also go do it on your.  
Another example is I can convince you that I know the answer to a Sudoku puzzle without telling you the answer.  
OK, so you can think about this is in general I can know.  
I can tell you the solution to a hard problem without telling you the solution, so I haven't actually convince you.  
And then there's a mathematics.  
OK, so with this I stop.  
If you have any doubt I can just take one last question.

 **JAGADEESAN P .** 2:06:28  
Uh set up without knowing the password.  
How you can come in the right side.  
So I mean, what is it?

 **ASHUTOSH BHATIA .** 2:06:35  
Without knowing the password he will take like see means if you if you ask me to come from the left and by chance I was in the left I will be I will just come from the left.  
I by I know why do I need this so my probability that I will actually win this one by half?

 **ASHISH KUMAR BHATTACHARYA .** left the meeting

 **ASHUTOSH BHATIA .** 2:06:57  
I I can still win the game with probability half if I don't know the game correct.  
Because by chance you ask, B doesn't know.

 **JAGADEESAN P .** 2:07:05  
OK, B doesn't know whether he doesn't.

 **ASHUTOSH BHATIA .** 2:07:08  
Correct.  
That's the.  
That's the B doesn't know.

 **JAGADEESAN P .** 2:07:09  
He doesn't know whether you went left side or right side right, OK, because of that, OK.

 **ASHUTOSH BHATIA .** 2:07:13  
Yes.  
So second thing you try to understand on your own that Sudoku thing I gave in general in mathematics, if there is any problem there are N number of hard problems in in crypto in mathematics.

 **NEERAJ KUMAR VIJAY .** left the meeting

 **ASHUTOSH BHATIA .** 2:07:32  
OK, another problem is called graph isomorphism.  
I don't know whether you have done discrete math or not.

 **GANESH NAGA RAJESH H .** left the meeting

 **ASHUTOSH BHATIA .** 2:07:38  
Graph isomorphism means there are two graphs and I want to know that in some in some way these two graphs are similar, and if the side number of nodes in two graphs like you can think about stop Facebook graph like relationship graph and I just want to know the the there is any other graph which is very much similar to this graph.  
There is a definition of similarity, but I'm not going into that.  
And the citizen that isn't mathematically hard problem to tell that there exists a mapping between the nodes from this graph to that graph which shows that yes, so your problem is to find a mapping and that is in the hard problem.  
So how can I actually convince that I know the mapping without telling you the map?  
OK, so this is actually useful in many, many cases.

 **SHIRSH GUPTA .** left the meeting

 **DURVASULA DEEPIKA ANNAPURNA** left the meeting

 **ASHUTOSH BHATIA .** 2:08:25  
For example, if Facebook is giving a problem to to a Google saying that solve this almost whether these two graphs are homomorphic or not, and then the Google finds out the mapping that say that yes, it is yes.  
But then the Google will say to the Facebook that yeah, now I know how Facebook will say that.  
See how do I trust you?  
First you tell me that that.  
What is the solution?

 **NANDAGOPAL NAIR** joined the meeting

 **ASHUTOSH BHATIA .** 2:08:48  
But the point I give you then you will say that OK means OK, this is you also know the solution.

 **SHIRSH GUPTA .** joined the meeting

 **ASHUTOSH BHATIA .** 2:08:54  
I don't want to reveal the solution first, I just want to say that yeah, I know.  
So for graph isomorphism also you can use the zero knowledge proofs and not only this in DEEPTI Graphy sorry blockchain, there was a die hard need to use this zero knowledge proofs to basically say that This is Money you owned by you and all and each and every company has now started this knowledge proof and specially in blockchains.  
So this is actually a way to this is.  
Yeah, you can think the magic of math and the all.  
So there are protocols and maths there.  
I'm not going to do that detail, so OK, thank you.  
I thank please try to run that script and I will post the the lab one which is which is going to be evaluated.  
You have to complete the lab probably in two weeks.  
Uh, and then I will provide the how you can submit it and if somebody is facing any difficulty in doing the lab, no issue, you can ask me.  
Only thing is that you can take each other's help in understanding the question, but not not just taking the answers or taking.  
That means you have to execute on your own, but you can take the help to understand that is not a problem, but you have to execute on your own.  
Means at the end of the day, if you submit somebody, others that I'm just going to give zero, then I'm not going to discuss anything more than that.  
OK.  
Thank you very much.  
Thank you for joining.

 **GANAPATI M. KUNDAPURA .** 2:10:28  
Sir, last question, uh, previous session recordings are four hours.

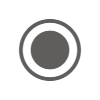
 **ASHUTOSH BHATIA .** 2:10:29  
Yes, yes, yes.

 **GANAPATI M. KUNDAPURA .** 2:10:33  
Or three hours long.  
Can you stop the recording after the session?

 **ASHUTOSH BHATIA .** 2:10:36  
Hello, like uh.  
OK.  
Let me just discard this and then let me go here and then, uh, recording more recording.

 **PAVAN KUMAR S M .** left the meeting

 **ASHUTOSH BHATIA .** 2:10:46  
Trans Skype.

 **ASHUTOSH BHATIA .** stopped transcription