### Security\_week6\_lec6Authenty-20241015

说话人1 00:00  
We started building a school of education. We said that we should have some confidentiality of the core hero of the alice's secret. There should be something at least only alice can do, so we said okay and alice can encrypt things. They would say, okay, that helps us against somebody learning articles, but it doesn't prevent it from using it from the bank. So then they said we needed to ask creation is also in the communications. All right. Let's think about some different ways to do that. So now we can think about it as a little bit more formal way. If we have others involved and they share the decay, go off and say no to others, alice can take the hat over. He has together with response. The safer is all back more.

So in other words, what we have is something that's only attached to this transaction. But at the same time, we have also only something that alice can do. So only alice can calculate this after the norms with ek because alice is the only other person involved that has this ek right? Normally, in protocols, lots of background things happen as well.

For example, alice has to tell them all this. I have others, I want to talk to you and then following that bottle basically challenge others with notes. But in general, we will be interested in the security protocols. We only keep the part that's actually relevant to what we tried to do. So there's nice setup or any niceties that happened originally, or basically they got it. Okay? So otherwise that we can do exactly the same thing, right? Bob gets in a non students. Alice can calculate the map of the norms using pk similarly, we have some freshness from the north which links it to the now for this transaction, we are doing a mac with ek which already only others tattoo.

All right. Then we can also or it was encrypt enormous and send it to alice that the alice is the only one that can recur this message, recover the norms, and send it back at all, and then finally walked in the city. And alice. He get encrypted and save it back. Right? So every time we now see it is something that gives us something we call freshness, something that makes it to one specific transaction listen to now, because bob is now using this noise. Next time he's going to use a different one, right? And every single time is something that only ads can do. Any others can calculate on that. She's the other one with the decay, or only alice could decrypt the dawns, because she's the other one with decay, or only alice get encrypted, not because she's the other one.

Right? So now we're getting the idea is something that only alice can do. And there is something that shows that alice has done that something now, right? Not yesterday or last week, right now. Right. So if there is a public innovations and assumptions, we can do the same thing with a tomato prefer. If we say that 30 brackets is encrypted with the public view of alice, and square brackets is citing the message in with the private key of alice, then what can we do? Bob getting trim are with alice's public key. Sorry, adam is the only one that can decrypt this message because he's the only one with the priority. Then he says, are that involved so many involved in same art? Alice been sinus r because he's the only one of the private pieces is that anyone inside is he sent it back before? So once again, there's something only alice can do is be true. Something only alice can do, which is sign. And alice is doing it on a number that is leaking it to the now. Right? Something that's gonna happen right now.

So now we get ready for 11. Right? This basically comes from the terminology that they use at the iso 9789 standard, which is basically the 50 patients said we stay where they define a lot of different options. When you do it, they said somebody else or people to each other. In any authentication protocol will have a claimant, will have a principle, and we will have a verifier. A claimant will basically tell the bearer fire that they are the principle.

I tell you that I am alice, right? I have the claimant, because I am telling you who I am. You are the verifier that you have not decide whether I am actually the person i'm claiming to be or not. And alice is the principal, because that's the person I am claiming to be. The others. If you think about it very formerly, the verifiers job is to make sure that the claimant that the principal is the same person, the person that they are talking to, how is it that there are others? They have to actually ensure that person talking to them is actually out. The main government indication protocol is any sequence of messages that goes between these two parties that is designed in such a way that is the laws that they require, because the concern will verify the identity of the failure, but we have 2 types of application protocol.

They can either be unilateral or mutual. Unilateral means there is a protocol when the protocol is finished. One party is indicated to the other in mutual indications. Both parties are thinking better to each other. So once the vertical is finished, this is then you gave the ball. What was it? Then you get to palace. Can you do that for indication? Alice has indicated involved, or models have indicated to us? Right? Basically, our protocol can only be messages going with each other, right? We're sending some data between others and all. I can then decide then somebody actually be the same thing. So before we were talking about, this is looking at the protocols, he said, if I want to make sure that i'm looking at this, it should be something that only alice could do, and thereby some be something that links the fact that alice has done it just now.

When we have those things back to security services, the first requirement is the message that I receive must have come from the principal, right?

If somebody sends me a message saying I am alice, the message that I receive should be from alice. It must be received from alice.

In other words, we need that is the origin of the implication. That is step number one. However, we must also make sure that message was generated recently or not. That is operations. Only if we have both of these conditions satisfied, and we say that we were indicated anyone. If I get a message, it says I am not as here are some proposed stuff. That message must have data origin of indication. In other words, that message I should be able to verify has been made by alice.

And secondly, that message must also have precious. In other words, alice has made this message. She has made it now right now during this person talking, then I know that the person i'm talking to is out. So we need both of these conditions. Right? Sentence of origin, of education. Last week we discussed maps. We also discussed digital signature schemes further. These will give you data origin of indication about assigns the message and send it to me. I verify the signature. I know that alice has made this message. It has not been modified. Right? Last week, we were sick people about encryption as a method of providing integrity. And we said, in general, encryption does not provide us with any degree to check. So I like to think groups of messages and send it to you. You just don't really know. That's what you receive is correct. Either in this special case, when we are defining protocols, if we give it some help, encryption can also be a third method of data, origin of information.

So how does that work? Encryption can check integrity. If the receiver had some way of knowing that the message made six. Normally, if i'm just sending the data, in general, it's very difficult for you to say this data is to rate a lot of records like six. Right? In authentication protocols, we can use something called the manipulation detection program, abc we can basically use that on the plaintiffs before the encryption.

Then when the receiver decrypt it, they can check whether this code is still correct. Right? For example, we had widen manipulation, detection code, which heads in that direction, and that was a hash. All right. Now, for example, if we take a message, we hash it and then we encrypted. There is cynthia, they decrypt it, and they get a valid hash value for the data that could be a way of seeing whether the data makes sense or not. Right? However, the easiest way to do this, we just have the receiver know the exact data that they should be received. Right? So any area that we're basically looking at things like this, right? Bob says monster alice encrypts bonds and saved it back to bob. We have freshness from the north, so that's something that's gonna be happening now. And our data oriented indication comes from the encryption, because alice is the only one improvement, decay, and bob already knows the answer you should be getting. Right? If have a sense of anything back and encrypt it and it's not been dance, you already said, bobble, rejected. Right?

So bob knows what the data is coming in. So if anyone modifies it, he decrypted, he will the in the context of the education protocols, if we allow for encryption to be set up in that way, it is an effective way of giving a speck of urgent impression. Right? I'd like to say good thing. How about depression? We have two common ways to generations. The one is nonsense. We sort of looked at them already when we looked at the various examples. This is called a challenge response protocol. I save you a challenge. You do something that talents, you send it back. The challenge is usually add on or regarding number. Okay? The first one, however, could also be a time stamp. Ii can simply take the current time. I can put that into my message somehow and send it to the verifier. So time stamps can be both logical or clock based.

So if we look at clock based, common sense, it's simply taking the current file in the message. Where was this message created? Send it to the verify. The only problem with this is is that actually the two parties to sit there and the receiver, the our favor and the verifier should have security synchronized box. If an attacker can come along with mace, with either one of the clocks, right? They can basically break the algorithm you have to think about. I also, if I can base with the verifier spot and said it by a day or make them a day slow, right? And did I have to send the message to that verify or like to send it?

And then I wait today, and then I sent it to that time. And I got to say it's fresh, because I just received this message from 1 second ago, even though it's from the data, right? And in practice, it's not so easy to provide such calls. Right? Synchronized class is actually a research area itself, not only for not ready for security with the networking people. They love doing boxing, pronunciation and research, because it's actually quite a difficult problem. How accurately you can synchronize them and they drove all the time.

Even if you have to watch this, for example, and you put them next to each other and you synchronize them in the morning, i'm pretty sure by the evening, one of them would be one of these statements fast or slow.

You can get some really accurate clocks like the ones they used in satellite receivers for positioning. Right? Like gpa satellites programs that kind of thing. But I put that very expensive. Are they very equal? And even they came to drift a little bit. So therefore, you need to have a way to synchronize them regularly. And then you will need to have security. Also, for everyone concerned. So you can do this security. So it's not impossible, but this is something that needs to be capable of. Right? So other things that we need to think about when we're gonna use cost based on steps is reliability. If I send a message to somebody else, this message does not travel instantaneous. It has to go to some network. It might cover or the encounter some congestion. Things might be delayed. Maybe the packet is dropped, and I try to be transmitted, which means not ever seen against it, like 5 seconds from now, rather than immediately. How do we deal with that? Normally, what happens is the receiver. Can I just say the message was seen one a second ago? So I consider expression. The receiver must have something called the window of acceptance, right?

And this means I will take any packet that I think was seen in the last 32nd for 15 seconds. So now immediately you have the cradle, you can say the shorter my window of acceptance, the more secure my system, because the shortest opportunity there is for reply. Right? Alternatively, the longer I commit, a percentage, the more reliability I have, the more messages I will, except is valid. And one state by another sylvia, even though they were subject to difficult conditions. Normally, artistic book is in the factory verify will set up with no acceptance. It will love all the messages that regarded that thought.

If it gets a visit from others, they say at 90199 9 o'clock and 1 second and its window of acceptance is 30 seconds. It will not take another basis from alice before 50 seconds, after 9 o'clock. Right? Because they will keep track of all the messages that comes in within that is done. Right? And if there's already a message from others that will reject, it, will only take a new message from others after 50 stations of the line. Right? The next way we can do freshness is using logical concepts. So logical concepts that these blocks, they use sequence numbers or counters.

If you are familiar with networking and you study ecp it's sort of something similar on ecp uses counters. You set up sessions be different. Parties make sure that all the messages are security. They're not reliably. And these guys, when we have alice involved, alice involved will maintain a counter, which signifies the number of messages that atoms have sent involved, and the number of messages involved has sent to us.

So the moment we just assume alice is sending both numbers, so they have a counter that counts how many messages others as stated before.

Okay? Whenever alice in the name is these two ball, this factor is increased by one.

I just have a number. And now, let's say number ten, it wants to send a message to bob, so it goes, I prevent it to 11. I put the 11 in the message and I send it to bob. Bob gets this message. He looks at this number. He says the last time I listened to you, a number of the number was, okay. My current number for how does it escape? 11 is larger than ten, it's fresher than ten. Therefore, I accept this means. Right? They involve increments these counter to 11.

Next time, alice was in 12. If alice somehow send for the message with the value eight, we'll say, but my current value is he dated. Now, getting a message from others with a this message must be all i'm gonna rejected and not accepted. Right? So whenever bob gets a message, he looks at the number that alice has sent. Then it's a fresh number. He says his own number equal to that number. The additional reason for that is also reliability. Let's say others sends the message 11. What's counter value? Is k right? But that message goes missing. And alice realize she has to see the game. That means she makes a new message equal to 12. We've all received at this time. You see, I didn't get any data, but 12 is still newer than ten. Somewhere along the line on this, each must have gone missing. So I will save my own comfort as well. And immediately, pilots involved is synchronized again. Right? So bob doesn't really care if the message is much bigger than his own number, but he doesn't care the the message number is smaller than his current number.

Okay? And then they might not ended up to the use of pakistan for the logical or hi guys is then nonsense. I just generated the random loans and says it's involved. All the business loans in surprise. Answers are a bit of an interesting thing, because sometimes they are random, right? But strictly speaking, a counter is also a loss. If I just increment a counter, every single violence in the next counter value matters, and my counter is very long and i'd like you to wrap around. Right? It means every single time I talk to others, I will have a new number.

This works perfectly well for some protocols, right? For other protocols, it would not work. Once again, if we go sort of and look at something simple, we look at this example here. In this example, aa counter would work fine, right? Boxing, the counter back into others. Bob says came to alice, bob, alice put things in the back before. Boss is 11 to alice encrypt 11 since the back of all, he's okay. It doesn't work here, because if I know what this is using a counter involving trips came and said to others analysis, in fact pain. Tomorrow I see bob is saving another encrypt. It wants to add it. I also know the answer is going to be here, because I know bob is using a partner. So in some cases, partners are okay. In some protocols you cannot use account. So it's more common to find that monsters are basically random numbers.

Okay? So on that aspect, that rapid number generation is also very important in equation security for generating nonsense and generating key values a little bit about when we talk about the management. But the basic idea is how you can do it is you can either generate them super randomly, or you can have true random number generation through random number generation needs a random, physical. Which most things don't have. It's actually very special to generate random numbers in that way. So generally speaking, most things are produced using pseudo random function. The pseudo random function is it produces something based on the formula. But if you just look at the result, you cannot be the next one. They look random, even though they've gone through here. We can basically use a very strong pseudo random number generator that will never repeat. Otherwise, we can just generate random numbers, store a value for all random numbers and make sure we need to use the same one. Or otherwise, we just use the random number to be really long. We generated rather than be accepted as a very unlikely chance that ever belongs straight through.

Okay. In terms of when we design a protocol, we can think about different attacks that we want to prevent. Right? The first and the most basic one is masquerade. Remember, we talked about masquerade attack. We said if the protocol is so broken, that somebody could just pretend to be others, then we are meeting with the masquerade, in fact, so masquerade, in fact, usually comes from a protocol that doesn't have proper data origin, education. In other words, it doesn't require alice to generate the basis. Anyone can just generate the basis. The next thing up is replaying that, right? Replay attack is prevented by creationist mechanism. If you don't have a big freshness approach, I did with my base concepts, logical concepts, or monsters, then your protocol can be vulnerable. The final impact is reflection. So reflection is a bit of a special case. Reflection happens if we do with the indication using symmetric algorithm. I want to explain this now, because it's easier to explain with an example.

And we'll look at an example later when we get a little bit into the program. When we want to make education protocols, how do we go about designing and analyzing protocols in general? Right? Generally, any type of cryptographic protocol has some assumptions. The assumptions are what are in place before we even start. There is alice and bob. They have secret, nice clock. They already have a shame, key or involved as a public private key. These are things that are already assumed to be there before we even start. Then we have the protocol flow. So basically, who is sending a message to whom when and what order we have the protocol messages. So what is being said between the two parties? Then we also have protocol action. If I send a message to paul, what is he doing with it before he's sitting here response? Why does actually happening after the messages during the messages are being exchanged? Right? So also, what we need to keep in mind is different aspects of the protocol.

Obviously, if we design a protocol, we have some security objective in mind. In other words, we want to be able to deliver something. We wanted to do something or achieve something. These security objectives will map onto a state of security requirements or cryptographic requirements. Then we have to go into the protocol. And after we have done, so we'll do final analysis. You basically check the assumptions in the following the messages and the actions to make sure that these objectives are.

Actually. So if we do a very simple example, let's say we define some security objectives. So bob wants to make sure that alice was the source of an electronic purchase contract. Bob wants the contract to be enforceable at the length of time, so he doesn't want to deny alice to deny that she has entered into this contract. If we map this down into protocol goals. In other words, security requirements that we need or security services that we need. We see that we need data origin of education, because bob wants to do verified in this message, actually came from others. And in addition that bob requires not repudiation of the message, anyone is not repudiation of orange. So basically, ball makes a protocol, and he says alice is going to seem to me a message and a map of the list.

In terms of assumptions, we now added involved as a shift etab in terms of message flow. That's why the message between others involved. In terms of message content, the message contains them back of the message. In terms of actions, once the message is received, bottle verify the validity of the mac. If the validity of the mac is correct, he knows it as has seen this message.

Then we do the analysis and we say everything looks from a functional perspective. Does it actually provides data origin of education? Because we have a map? Does it provide us with non repudiation? It's enough in the back for 500 creation. Why is there anything that can provide non repeat edge? Signature? Right? The signature, as I made the one private p only one private p inside, matt cannot provide another reputation. Our protocol plans. It can do half. It can do the data or even indication. But I cannot do that on you guys. Now we redesign it. So you say alice is going to send a signature of the message people. In terms of our assumption, bob has, alice has a public private key. The flow is the one single message. The message data is the signature of the message for the action is involved, verify the signature there.

Now we can do the analysis. We can say signature providers with origin of innovation. Very good. Aa signature also provide us with one application. Right? That is what we want. That was the goal that we wanted, and therefore offer the goal. Every single time we can, if you buy what the product wants to do, you can define it, and then you can check it if it actually works.

Let's look at some basic protocols. It doesn't have an indication protocols in the examples to be given the course. Basically, all of it comes from the iso line in 1907. These are actually real protocols that is being used for this b right? Not just academic example. In terms of notation, a and b are identified as the identity of palace involved. Ta is einstein made by alice, ra is a random loans generated by alice. Tab is this gft because involved, it takes especially anything. It could be. And one of the protocols is to find some picks. It is not for security purposes. It's if you want to exchange some, I think information between others involved have to say five if we say the curve on the score padx it basically means xa is encrypted, was to make a crypto are using dad if we do math dadx it means we are doing the map of x using this share secret ekb and if we use signature of x by a it basically means an xy with the private e of a right?

So that's the, as the first protocol example. We have alice and we have bob. Alice seems involved the following message, a 57, 95 others, the identity of all some other things that if you get involved in this, because we modify, although and then encryption of everything, with symmetric encryption of everything, using eab i'll give you a minute to look at this protocol, and you think about what is going on, what is the assumptions? What is the actions needed to be taken by others involved? Why is this an example for? Is this unilateral of each of the pensions?

Who is it taking credit to who? And why? What do you think for this protocol to work? Why does alice and bob have before it stops? They need a shared key, right? If that is the problem does not have shared key, the protocol doesn't work. Okay. Next, is this an example of unilateral or mutual indication? Is others are dedicated to bob? Is what was dedicated to alice or is bob and alice dedicated to each other? I think we can probably this. We can probably not say it's mutual, right? Why can we not say it's mutual? Why is it not nature? It is an easy question. Why is it not engaged with indication protocol? Because bob doesn't even say anything. Right? There's nothing for us to verify from both sides, but there's nothing. Right? So there's no way for us. You need to go. We can only put dedicate potentially alice. What are the two things we need to indicate us? The two properties? We need a message that only alice could have made, and alice must have made a message now, right?

So we need data oriented education. We need phrases. The data origin and indication comes from the encryption. Alice is the only one that can make this message. So she is the only one apart from b with pad so if bob receives this message, and he encrypted and he sees all the stuff inside, and he sees that alice has made or encrypted this message, he knows that this message comes from others that gives him the data origin of the equation. Where does the freshness come from? I suppose that alice has made this message just now, and he gets timestamp. There is a timestamp inside. So the timestamp gives us the creationist. The encryption gives us the data are limited indication. The two conditions are made. Therefore, alice is a dedicated before. Right? The assumption is a secret key that should be not involved. And there's only one action or basically recruits the message. Make sure that the data origin of integration is correct, make sure that the timestamp is actually rich. If that is operate, you will have any head out.

The second example, bob sends rather number rb rather loans, rb to alice. Alice takes rb to identify, or bob, there's the back of that and send it back, involve. Why do you? I'll give you half a minute to think about this. Once again, things which is dedicated to who is unilateral, mutual. What are the assumptions that we have? Why can we say that somebody who's indicated to somebody else? Otherwise, where is the data origin of education? Where is the patients?

So what do you think here? Is this unilateral mutual? Is one person getting a thing to get into the other one? Or are they both getting a thing to get into each other? Explain zebra. So bob sends random number to alice. So this message has freshness, right? Cause bob is sending a new random number to alice. So this message has creation. Very good. Does this message have been the origin of education? No, because there's nothing that is only both could have done this. Anyone could have done this. So the message that goes from wall to others as precious, but no data origin of education. So bob is not as any good. So that means and this is unilateral education. So evidence seems to go, in fact, rarb and b this map because data origin of education, because it's something only alice can do. Right? And inside it a not that is fresh, new, always use the new. So that means this message is fresh, right?

So now god has gotten from alice and message that early alice could have made with the bag and contains the freshness rb for the conditions are satisfied. So alice is a dedicated evolve. This is a unilateral protocol where alice is a thing better evolve. Why is this fall here? Where did this come from? Because we could have made it like this. And all the things would still be there. We would have freshness, and we would have that the origin of education, what does this ball actually do for us? So what is that is? Is it provides as an indication of the direction of the message. You can define this other way. If you put this identifier, could say this message is intended for ball, so the receiver is ball. Definitely, you could put a here, which means the sender is a right? But most common people use. And I think the better way to do it is a bit.

So basically, I made this message, the intended recipient of this message was born. Why is this important? Remember, I talked about the third attack released here. I say this masquerade is not like the origin of any equation. There's reply if there's no freshness, and the third one is reflection, what have we done? Wouldn't it be there? What happens now is for folks the matter be and he says I am ball. You need to identify to me. Here is my rather loans, rb at the same time, battery goes off and replace it the ball. So it is. I am palace. I want to talk to you, but first you need to dedicate yourself to me. Here is non rv but battery uses the same norms as the one that was used to challenge her, right? Being the honest person that he is in his memory about it. Answer, which is bob met with. Now its model balls and norms. Back with gave me it's actually valid response. It's the same time. Right? And then this response that bob sends back to battery is also the correct response that bob has expected battery to send back to him.

Basically, what happens is valerie reflects it back involved. Take your response back from all, and basically reflects back involved and basically use this ball to calculate the right response for her, which they need to say that involved battery can also do the same things. You can get this army from above and then go find a and say aaai am ball I want to indicate to you here is a random number. And then a alice will sit back to our map, gave the army, right? And then it will send it back involvement. But usually we don't assume that we assume that there is a need to find. Right? So this is hard work by putting the ball in here. What basically now happens is give ball makes this response. Balls response would be like that. And the response that involving states back would be like that.

So now the second message, this message here is no longer the same as the message at the end. I think as we kind of reflected, okay. Right? We look at two more examples, and then you can hear. Right.

Next example, this is non so on. The boss is not alice. Science is on and saying that before, right? In this case, who is it dedicated to who is bob is dedicated to others? Or is others is indicated to bob? If we look at the message that goes from bob to alice and has freshness, but it does not have data origin and indication, right? Because anyone could have made the city. If we look at the message going from alice to bob, it has freshness because of the norms. It has data origin of dedication because of the signature. It only had us to have done the signature. Right? Therefore, the man, bob has a message from alice is fresh, whether they are in a dedication. So analysis has been painted involved. In this case, there's no little identifier be here.

All right. However, it's probably also a good idea who did it, but theoretically, we don't need it, because we cannot retake this. Right? For example, if this was, instead, battery and battery would try to now do her, take with the reflection and say that, well, their response will come back, will be the signature of bob's name, rv ii reaching it. But basically, now you see that this response involved, his back is signed by him. And their response involved with the state back from alice is signed by alice. We don't have this problem with prediction that we would have had when we use symmetric of them, right? Because the signature already inherently tells us who the source of the messages, because the sender is also the sign.

Okay? One more and then talk about it. Right? So next one, alice sends the ball, pa the signature of pa and identified ball. Bob says to alice, pb the signature of pb and a okay. Is this a kind of unilateral only show authentication? Who is it dedicated to who? And why is alison indicated to bob? So the message came from alice to bob. It's a signature of a time stamp made violence. So can we say that this message would only have been made violence? Yes, but it was signed by alice, right? Can we say that this basic aspirations? Because in that time stuff, right? The bar has a message from alice and od alice to play. And it's great. Now alice is dedicated to bob, is bob is dedicated to alice. Yes, but the message is doing the same thing, right? And this has a message from bob. They call that sign, so we have data or intimate education. We have a concept that said that this is fresh. Therefore, work conditions are met, and that basically depends transform.

We're gonna stop there for now. There's still a couple of examples there, but we will do it after we have. And then, therefore, so what I want to do is the better with better. Next week is the term. Here are the deal. So today we did make sure six. Okay, no wonder. Today we did it for six, but the method is not going to be about today so that there was only the things we have done last week.

It covers lecture 1 to 5, so everything up to including integrity. Remember, for the number theory, you should be able to do our side of the volunteer development. Not long, not the theory. Only question. Questions, similar difficulty. You probably said one editorial, right? Of their idea of difficulty, right? Why you are allowed calculators, you are allowed notice that can be on your pc that can be happen. It doesn't matter. Okay? If I walk through during the quiz and I see anything that's not powerpoint of pdf then i'm not going to be happy. Right? So you can only have our point of pdf for your notes, right? Like you can keep it on your computer, so you don't have to send out everything, and everybody comes with like 400 pieces of paper.

During the quiz, I don't want to see anything as you find out wechat with her and your browser and all sorts of other things.

I need a powerpoint for the pda so you can be a nurse. The warning is, even though you are allowed to bring your notes studying for it, like it's a closing test, because the time is very limited. Right? You do not have time, every single time you go to the next question. You don't have time to go to that part of the notes. Readers study, see if you can understand and then apply it to the problem. Right? The notes are only there for you as a reference. So you should always be able to answer the question in your head already from what you remember. But if they so happens to be a little thing that you forget, you can look it up with your book in your record notes, right? If you refer back to the reference, every single question you are probably gonna struggle to finish the midterm. Okay? So that is fine.

The time is the method and then remember to check the campus. So remember that every week I upload those additional notes that goes together with the slides, and you can do from there what slides are important than which ones are not. So usually I arrive at the bottom. This slide is really important. You should probably study it. Or in the next five slides are very important, is this core stuff. Or I will say this slide is really only there for interest for you to understand. It's very interesting, but you probably not gonna get a direct question on this thing that. Okay, so that can help you optimize a little bit what you study during this week when you are studying, if anything is not clear, send us some email, and we are more than how happy to help you answer anything. Also remember your car pleasure. You don't bring the car pleasure, then. Some of the questions are difficult, not difficult. I you probably do like random calculations you get before you carry this in a way to talk. So rather bring on the top later and be happy. Does anyone have any other questions about the middle group? I prefer you die.

But maybe you can is okay. If you use the calculator as long as there's not a basic calculator, it's okay as long as you don't use an online one, and then it has to be a little half of the winner default one. That's probably the city can be scientific calculator and use the programmer to calculate some. No, you cannot. There will be enough big numbers. So that big number is like in the problem set. The rest of the numbers will be small. I need for rsa how the public to be held if there is a number. So you should be able to calculate it right now. All right. If you, for example, do the agency fitting algorithm, right? Instead of having our headlines, maybe like two dots, right? And number is small. So it should be easier. You might be able to do the matter for this. It's going to be as long as the probability.

Any other questions about the good? Everybody happy about the quiz? If you think about some questions, you want to ask about the quiz right there? Just talk with the EMAIL, and we can answer that one. It's 4 o'clock, so we can have a break. We can have the tutorial. Now. In this classroom, you can see where you start, and i'll start going to the oral solutions at 4:50. Thank you. If they got you, what they do is actually it's more you can do it. So it is very important. Yeah, I'm not happy. So we need to.