### Security\_week6\_lec6Authenty2-20241015

说话人1 00:00  
Right? In that case, we want to be the mom, but as long as you generally on ., it's okay because there can be no absolutely correct answer. But most of these articles that you read is not going to give you the exact means. You have to think a little bit and think which one is more likely. So at the end you're making like a guess, but it's an educated game, right? It's why they have some logic to mind. So I cannot say, you guess wrong if the answer is not there, as long as its logic is correct. Right? So there's actually a lot of interesting places to get cyber security stories. So sometimes you read it in the newspaper, sometimes you can read it online anywhere. But generally, there are also some other resources. So I think the violin that sort of goes worldwide is something called songs. So songs is like information security, almost for executives. What they do is they take everything that happened in a given week in terms of cyber security, and they tried to date it down to like easy to read short story like a short item.

And this is these people have this attack. These people discovered this new problem right here is a new vulnerability that people are talking about. They basically, there's still a dog break it down into a small, easily readable paragraph. And then once a week, they send an email out to anyone that subscribes to the newspaper to basically give them these short information pieces about philosophy.

And then sometimes they reference you to longer more detail things, but that everybody can just keep up to date with interesting things that happen in cyber security. Right? And then there's something similar also by the uk government. So they have these updated, great reforms like things that have happened software that is not secure, various types of things that people might want to do it more. So it doesn't give like detailed information, but it gives you like a little bit of overview of what is going on.

Right? I think that into question two, so question two combines a lot of things together. Mostly, it's a taste of mode of operation alongside her. We want you to see what happens actually, with some of these box office work, and you have errors if you do the encryption. But we can't really ask you to do this or as so we just give you a simple substitution. Sorry. Then there's the preparation. So we want to encourage you. We are keeping for the same ages twice with cbc mode. But using two different I ds, we ask you to come to mode.

And then finally, for the cbc mode, we ask you what happens if you have that error? And what happens when you have a lost law for the first one. So you have to encrypt the message for alice that you walk back for as message to binary sequences given the alphabet there, right? Then you can put it into this binary representations of these eight, 4 bit binary strings, right? And every single time you're gonna take one string, you can why don't you have this thing? So the only thing is another way tricky is you have to keep track of strings and nature at the same time, because sometimes you have to do the by receiving manipulation first and then map it back to a character to do the substitution.

Sorry, right? The substitution separation is simple. Ship cipher would be equal for the first encryption, cpc mode with id 001. We know that cpc encryption, c zero is the encryption of ida sort of one. Cy is the encryption of c zero, xo one. This means that the encryption of id which is 0011, and e zero, which is alice. Now it's for other support. The first letter is d it's 0001. The first extorted together. It's zero, ay and a zero y and ay and a one. Is it zero? Then this maps back to c if we do the substitution software cooking the c it increase with air. Then c one is c zero and x or to p one. It's if x or to o we put the f here, we put the out here. We can so that we together, which is an l and it made for the l if you was, then we give you a second, the same until we run out of bank next.

And the final side of this is foc is the in ei what the second question in us is, can you do the same thing with the different id right?

And then supposed to illustrate that with cpc mode, the current cycle takes the things not on the only of the current plane takes, but also for previous banking study.

What we should not see is that even though we are interesting exactly the same message, which is $4 by recruiting it with a new id the resulted, soccer takes is completely different. What it was before. So before we had, this subject takes foc if we into the iron, now we have odfidedna right? The cycle takes is very different, even though we are basically encrypted. Is that right? Then encrypted with counter mode, the method is the size of the system mode is different.

Here we are encrypting zero, because it says there is the first counter value is zero, the initial value is zero. We encrypting zero, xop one, xp zero, sorry. Encrypted is 0 %. Encryption a we encrypt a to d and then basically, we extort that to be, which is our expanded, then the x or 00110001. When we explode it together, we get ac the first architecture is c the concrete mode. And I think the same of c zero, c one doesn't depend on c zeros. We instead encrypt the counter + 1.

All right? Which is the same as encrypted b together with banking zero, we encrypted be then x oriented zero. You guys? Ak right? It gives you everything, and I values ckgka for dne it now becomes a little bit interesting. Because it said, if the most significant bit of ckp becomes an error, what is the recovery? Plain text? Previously, what we had was the worst significant bit of c three because of the f if this is 0101, basically it becomes a 1101. So basically becomes again, right? Then p three is c two x or the description of n which is equal to I before, is c three x or the description of b that's nx or o d the fedex is now bodidice what we can see is the first three letters was sort of correct.

The next two, the p three and p four are incorrect. Right? That would be expected to happen. If we have a bit. There are two blocks will be wrong. And then after that, everything is correct again, right? A is turned into ai the alice turned into ab and we still have the ice from alice's name at the end ok so these two blocks are incorrect and the rest are fine. Then the final one, if c three is completely lost, the receiver doesn't realize this. So it basically processes c four, c three, c five, or c four, c six, 65. See, if there is a lot of p three is equal to c two, x or encryption of c four, there's within c three, there's even as another users in c four.

Now, plaintiffs three becomes an end. When it takes four users, c five considered c four. So the fedex becomes I basically, what the fedex now does is your dod and then you have bias. Right? What happened here is, obviously, we're gonna have one day spandex block because the receiver received while they expanded law. So we can't have the same amount of fedex loss, because once a year, right? One law, only one law had an error. We have more of this correct. We then have an incorrect law that should have been an l but it is m and our a has disappeared all together. But after that, one blocking error, basically, the last part of palace's name is correct. That's an interesting thing about cdc mode. Even if we lose a block, it's still read, synchronize with the same inherent, right? You're gonna have one block in error, but then afterwards everything will be fine here, right?

So for the number theory, the number theory numbers were quite large and sort of that way on purpose. So you could really struggle with it. So once we give you easier, shorter numbers to do with rsa of the moment, then hopefully that should be straightforward. So we ask you to use a student id as x is your idea to see this idea. Why is the least significant conditions? Basically, x is the most, the y is the last four digits. If you see the number, then x is, you want to see the number. The first one is compute, what do you want to the y what? 18,805 with anyone need to calculate? Phi of y so this is the four digit number. They would likely to find the greatest of divisors. He did number, this number, then five integers, x and z the next time just give the number five z times this number is equal to the greatest form of divisor repeated number. That's why I think we have a 1 billion is best to calculate.

Then finally, there is choose any prime number of z that is smaller than x calculate x to the x more c so I will put the solutions online, so i'm not gonna regard everything for you.

And I also know that which student number is, which I just had to choose one. I chose to see the number on top of her. This is an example. Right? But the basic idea of the square multiply is that now we have the least significant for regions, which is y 840. That is our exponent. We have to first decide what the values of two is. That is going to give us this exposure. For me, 1,008, hundred and forty is 3 to the 4 + 3 to the 5 + 2 to the 8 + 2 to the 9 + 8.

And then we have to do all the squares to the largest one. I'm going up all the way to two to the 10. I have 41 squared, which I didn't calculate this. 1681. And then I have 41, which is 41 squared, all squared. I can just use my previous answer. Right? And then I keep repeating this until I get to 41 in the car, then, right? And then basically, I collect all the terms that I need again. So I need 50 to the 4th term. So I need this one here. 6581. I need 2 to the five. So I need the 14386. I need it into the end. Start with the 138, and 6, and I need the 2 to the 9. So the 15 for one here.

And then finally, I need the two to the k which is 1295, this one here. Then I use my calculator, I can multiply this together. I can do this one for the reduction. I gave 5,776, okay? For the modular inverse, the important thing to remember is that if we have opposite number, if the last four digits of your student number was a prime number, you are very lucky, but it's most likely to be a composite number. We need to factorize it first.

For my chosen student number 1840, I confess, see that it's divisible by 4 to 4 times. Right? And then basically, it's divisible by 5, twenty three pounds and then 23. Now there is a lot of five once and there's a pretty feet. So my a 1,840 is 2 to the 54 × 5 × 23. That means 5 1,000, 840 is just the phi of this term times the phi of this term, times the phi of this term. It's phi of two to the four, which is 2 to the 4 - 1 × 2 - 1. This is 8 × 1. And then for a prime number is this prime - 1, because it's five to the r zero minus five minus one, basically to the power of zero, 22, - 1, and then multiply that. I get 700. Im fine. Okay. Then the greatest common device error to calculate the greatest common device that you have to use the algorithm.

Right? You can basically do it both ways, right? You can do the one to their production, or you can also write it out in a different way. So there's two different ways of slide showing, right? In essence, the more useful one to end up with is the one in this format. If something is equal to something times the second number plus remainder, this will help you do the next question. But if you decide to do the recursive, greatest common advisor with the modulus, that is also fine.

And remember, the middle number becomes the number on the left. If you remain there, becoming the number in the middle, and then 488618, forty two four eight eight six one seven, 07 + 153, then 48861707 is equal to many times of 1,008 + 34, 36,000, the energy 7,001, then the brand is covered over.

And then the next one is 133 = 3 × 34 + 31. We work it on, but we basically have 31 people who came down + 1. It doesn't happen if the greatest common divisor between my student number and this number is one, could be that you get something else, and that is 55. Right? If you don't get why you can't calculate them 1 ~ 30/1, it might be the next question doesn't ask you to be the one to do this. This ask you to find a combination of your students number and this number after they broke it.

So then it's equal to the greatest one divided, even if you grasp on the bible five or six. It is something else. It would still do it. I think it's one. It is fine as well. You're gonna use the extended, you fit it algorithm, which means you have to look back. Y is equal to 51 - 10 × 3. Then we go one up. We see that three is equal to 34 - 31. We substitute day for three, and we multiply it up. And every single time you multiply it up, you actually do the calculation to see if this equations don't equal to one, right? If it's not that you multiply are incorrect, then we substitute for 31, then we substitute 133. There is up to 2, 448861707. Then finally, what we should have is we should have an equation in this form. Something comes to student number plus something else times. They give a number like this, other number. And that is your final answer. You don't have to do anything wrong. Right? It's just asking you to solve, if we were using this to do more delivery this, we were lucky enough to have a greatest on the body of one.

Then we'll take them more to the reduction of both sides. One of these terms will be here, and you'll end up a lot of interest. We got it. But it's not asking me is that yet just ask me to solve the equation. If something comes to see this number, but something given number is equal to the greatest of the process.

E was the modular interest equation. There's a smaller number. Once again, we do the extended video algorithm, basically do the video algorithm to find the grades from the divisor, which you should find to be one. All right? And then you do the working back exactly like with the previous question. And then you get to one o seven three eighty one × 108809 - 4008993 thousand nine hundred 291452. You do the modular reduction of 291452 of both sides. This means this third disappears. You basically have 11091452 is equal to 170 81 × 108809108291485. And then you can see, and I think the if you want this value here, if you want it, that one times the number modular reduction is equal to one more number of equations.

Okay? Choose a prime number. Is it so that it is smaller than x calculate x to the x one, z one plan to do this is to think about the possible hero. They choose the modulus as a prime number, which is as close as possible to your student number as you can get. My student number, I think, is the problem number 48861833. And then I know that this number is the power of five of this number would be congruent to one.

So that means that basically disappeared from an idiot with an additional to the a then it's a small enough number. If you just multiply out interviews. The other smart way to do this is simply to choose as two. Anyone choose as two? Okay, people try to say this, too. That would also be correct, which means you get this ceo either my student number is odd or even. Even if it's zero, if it's part of line, then you can solve it as one line. Then that would be the easier way to do it. But if you did it a long way, congratulations to you. It's a very good. Okay? And then it's possible. Or if you just decided to do square and multiply also extra, congratulations. It would be very, very long like that. That's it for number theory. So there's some basic equations about how the laws of the online is giving you a chance to work through those very small numbers.

For other law, we have a private key, we have a prime, we have a generator, we have a private key is equal to five computers, the public py encrypt the message n equals six with the right number equals seven. Verify the calculation. So this basically decrypt the citation to make sure you get message out.

And then finally, what security service can provide using of the mall after the showed in the class notes. The public key is just g to the x one p it's 3 to the 51, 13, and 9. Out of all, we have two parts, architects, a and b a is equal to g to the r one e equal to seven one thirty is to be re. B is equal to the message times g to the x to the power r it is equal to 6 × 97. Modular 30 is equal to. Then it will be the description. A is equal a to the x point of b which is c to the 513 is equal to nine. And then the message is equal to b times the modular emails of a modulo e which is equal to two times the modulo inverse of nine modulo 13. We can see that this is just three. 3 × 9 is twenty seven one zero thirty is 1, two thousand three one zero three. The games are right, which is equal to 6.

And then the last part of the question, given that rsa can do everything, the idea of this question is, if you think about what alcohol can come to, for the algebra encryption algorithm, we serve in the slides, we can only provide from potentiality. We can only improve information. There are other signature schemes based on alcohol, which I briefly told you about in class in lecture five, but that is not what we discussed, or the encryption and not the one you are doing here.

All right. So this one can only provide us with compensation is nothing else cannot always also sign like our sentence.

And then what did they help them? Consider? They have the exchange of people 30 and d seven. Alice takes x equal to five and more xy equal to 11. Why does the sheer key and explain the weakness of the phenomenon how you can fix it? At to the x mark e 7 to the 51 to the 15 is 11, be to the y is equal to 7, 11, 1 to the 15, which is equal to two. The k is g to the x to the y which is equal to 11 to the power, 11, 1 to the 15. You looking at from a perspective, you can also accompany these dictators. And you see it's the same, but the shared key is equal to six.

And then for the weakness, I remember we talked about the matter in the middle attack. So if three d comes in the middle, she basically makes a key with alice, and she makes it said that he was involved and others involved. And then she's there. So the easiest way to solve that is just to add something to origin of the equation between others involved. And you've now lived about two ways to do that. Either. They can sign the data, or they can do a map of the vector. The easiest way to do this is, alice will say, d to the a mod e and then back using the shared key of others involved of g to the a one p is involved in something similar.

So g to the b one p and then back using the sharing pad of g to the d or dok and then basically, that would ensure the treaty cannot get from the treaty dot coms. And then she sends back g to the e to others. She says g to the t to four, there is no way for her to generate back ad of g to the t one, e but she doesn't have this shared key between others involved, right? So she cannot make this map a better than if you say, kind of sciences. It was okay for the sciences and it was okay to give you exactly the same salt, same solution.

Then the final one, you are the owner of online talking in there and you find switches and diamond programs and you have the internet. You basically want to prevent people from modifying the software. So you want to put it back on it. You choose to implement an aspect. The programmer tells you that he's implementing it in this way. The hash mac is equal to the hash of ek are calculated to the data. Explain why this is not secure, and then suggest how they should implement it. In terms of suggesting how they implemented. This is not the same format as we talked about. But remember, what we talked about in class was that we should hash with one e together with a higher message. And then we should take this hash result and hash it with another e to make on that. This part is only the first part, right? You have the e to get rid of the math. The problem when doing it like this, is that it's simply that I give you an intermediate value. Right? I calculate the hash of the message, and the message has two message blocks.

Then I asked k first followed by acid in one and in two. Right? I take my ivi take my e for simplicity, we just assume that the key is a block, and then they made it all, but it doesn't matter even if it's amazing doctors over the nancy doing multiple messages. But what happens now is he gets fit in together with iv we get a hash output. We hash this result together with the next message, go up and get the next hash result. And we have to get it with a two to give us our final hash. And we said that with our software, the biggest problem is then very simple for her attackers, just to add messages to our message. Right? Somebody could add another block to the message and to create a valid back value themselves, even though they have the key, you can just take off as values and hash it together with the additional message block to give themselves a new value match value.

Why does this work? Because the key case already has the beginning there. No matter how many extra blocks that attacker puts on, and simply adds on at the end of the hash by taking our house value, and continuing to hash takes from boston to the hash value, that hash value will be back. Right? Because the only time we need the key is right at the beginning. And we have already done that folding. If we were to implement the hash in this way, it's basically, it's very simple to extend the message to, however, long we want as an attacker. And so then update the hash to be ending. Got it. Okay? That is all the solutions. I work with the solutions on campus, with everything else. Right? And if you have any questions, feel free to ask any of me of the dns and we will lock it on campus, we will try to release your marks back to you by the next one, then.

All right. But you also not have the correct solutions. If you want to study for the victim, I would just add one thing for most of the questions in the problem sets, apart from question one, which is one is quite open. So we have more blocks for different things, or question two onwards. If you make a mistake, you will get zero, not for the entire question, but for the particular little question of some questions you did. The reason for that is for the problem state, you have a good book and an incident amount of five. So it's very easy for you to take your answer many parts. So from our perspective, the only challenge there is to be careful and do it correctly.

I cannot give you a method mark, because you can do things and notes what the method was. And then you have like a very long time to apply great. So early challenge is doing it, correct? Right? So for the men, for the problem sets, we're not going to do make the market. So it's either correct or incorrect for the quiz or for the exam. If you do a calculation problem and you make a little mistake, we will give you lots, then we will do make it long. Then we will say, okay, I see that I have the right idea, but he made it finally to say, because in those cases, you might not have a book or you might have very limited time.

So there's additional challenge to that. Right? But the problem says you have all your lives. You have a very long fee, fine with it. So there are many things that are really challenging agreement, correct? But don't worry for the quiz in the exam. We will give you made it more. We want more in the exact same one. That is the solutions for the better. Then I don't know. At the beginning of the file that should be an announcement, which I have in mind that the one I pop it over is busy at home. I'll put that announcement in here, right? And then i'll talk about it after the break there. But it was essentially something about it for real and also the mid term. So i'll talk about that in a second. Part of the forum is easy. I haven't had anyone complaining or anyone saying anything. So I think we're gonna keep with the single tutorial. We do the single tutorial from 4 to 400 ok so that's the easy announcement, but I would try and tell you things about the winter.

Now i'll fix the slide, and then i'll talk to you about winter. Thank you. That section, but for the tutorial today, only one session again, but that seems to be working well and no one complaint to me it. So that's okay. For today's lecture, it's basically, I started a new section, of the course. Last lecture, we look at the loss of the mechanisms, the low level, but we look at hash functions. We looked at max. We looked at digital signature for a hash. We said that a hash has a known algorithm, but there is no, therefore, anyone can calculate it. So it cannot provide integrity by itself, but it has the date if the followers actually be modified. So not if somebody intentionally modified the technical stuff there for that, for the hash. We also discussed the security of that function. We said we estimate that if it needed, you find a condition on the hash. And remember, we talked about that birthday problem, and we say that roughly what we need to estimate the security of the hash, where n is the name of the hash output, should be the square root of two today, right?

It's due to the end divided by, right? And then for the mac, the difference between a mac and a hash was that the mac needed to eat. So not anyone to calculate it, right? We can go, max, in different ways. We can use it with a hash function, or we can also use it in cdc mode. We could build a mac using cdc mode. For a mac. We don't have long repudiation because there's at least two parties. We generate the map, because in a symmetric system is at least two parties with the heat. So therefore, if somebody sent me a message, I cannot either say you are the only one is able to give you that message, because it would be multiple people giving me that message. Ii could have generated that message as well, right?

And then we look at digital signatures. It's an asymmetric crypto mechanism. 1 % inside with a private key. Many people can verify with that person's, probably. And we look at the specific version of rsa in more detail. At the end, we look briefly at some others for interest. And the rsa one is the important one. It's the argument it isn't that provides one recreation, right? Because any white person degenerate this. Once again, we talked about ashes with digital signature, as we said, digital signature, at least a matrix. It's based on number theory, will be one of their expectation. When we do the popular induction, we cannot actually sign a message. It's longer than the one. Instead of signing the message directly, we first hatched the message and then we signed right? In both mac and digital signature we used to have. But the hash cannot really provide anything by itself. It's a helper function for the other two. As I said, today signifies a change for the course, because we've done all the lower it preferred to be able to discuss.

After now, we'll be talking about mechanisms or tools, or how we can do certain things. Today was basically move on and start moving on to what we can actually do with these things. Otherwise, I quickly build protocols to provide us some other security services sectors of education. That sector is all about the education protocols, and then discovered sign of three and sign of four, the station of and security analysis of security nation.

So we're talking about, indeed, the same patient. Okay? What is the dedication in authentication? Somebody wants to prove their identity to someone else. So alice wants to prove her identity. Or it might also be dated to say that all actually wants to verify alice's identity. Right? At the same time, bob, I also want to show alice that he is in default, right? In which case we do, usually the information we do both of them at the same time. So while confidentiality and encryption is very well known, so if you ask anyone who doesn't study technical things and know anything about security, you ask them, what do you think security is? They'll immediately tell you encryption, because encryption is so easy to understand. I want to find my data. I want to be encrypted. And the infection is very big. But what people don't realize is that people also use the same dimension all the time, right?

And then when you pointed out, there is something like that's correct. Whenever I go online, I enter my username and password. There's lots of things I use every single day. I go to the cash machine or I used to go to the cash machine. I went for money, I I have a credit card. I want to pay with that credit card. I want to pay with my phone. If I scan my phone, if I scan aqr code, the first thing that happens is the receiver will verify whether that thing is a faint, whether the phone is a faint, whether the user is there.

If I go on any type of npr or under drive or railway with a smart card based ticket, I don't know how to have the one upon the octopus card. Every single time I use that to pay anywhere, it does nothing before we do the dedication. First, because it has to basically determined whether I have a legitimate card. It is best prices. Right? So I think the occasion is happening all the time, even though we don't always need that it's happening. Right? So in terms of communication, there are different things. Today's lecture is more focusing mainly on authentication of things, not necessarily people. We'll talk about with the indication of people later or something. You have, something you are something. Today is an indication, is possibly more in terms of machine to machine communication based on proposed and different keys.

Okay? When we do an indication on, let's say, the standard loan system that is not predicted to anything, and it's completely physically secure, then that could be relatively simple, right? That's it most of the time. This is what we need. Right? We need to do an indication over the public network. In other words, when we doing this with education, attackers can each drop on what we are doing? They can even replay some messages. They can modify some messages. All right. So basically, we need to have a protocol that can be secure, even though those attackers are around us. All the time. For example, if I want to enter into a building, I have my id card next to the door of the reader. I'm gonna put my id card there. Maybe it's gonna ask me some additional verification I in the pen or presenting my face, and then it's gonna let me into the voting.

If we want to have an analogy of an example of the difference between physical and network systems, we can think of a network system almost as a building that's just there. I scared. I entered the thin. If I don't get it, I could miss iran for as long as I want from attacker, I can miss around with everything. As long as I want. I can try 1,000 times. I can put a little thing there, today's other people's transactions, anything. It's not to take it. Right? On the other hand, if I want to go into a very sensitive building in the front of the building, they might be the turnstile that I go into. And the turnstile will be watched over by a security guard. If I come there with my id and I put it down and the machine beats, and the next be, all right, set by taking around, taxing the thing. The god is immediately going to come up to. And say, what are you doing here? This is not allowed.

And then if my thing looks a little bit wrong, it's probably going to take me away for the police. That perspective, because there's additional physical security in the system. Right? I don't have as much freedom as if I had the chance to miss around for everything. That's the same as whether we have a network system versus we have physical security system. The same happens if we have a fast machine like an atm I will put my card into it. I will put my pen into it. This machine basically protects this transaction. It's very difficult for somebody to observe that what happens between my card, the machine. Similarly, if I start doing strange things or I get the 30 correctly, too many times, the machine will basically keep the car and not give it back, right?

And then I will have to go to the bank for additional variation before I can get it back. That's why people know what is your people's credit card information. They would probably put a hardware into the machine. It's called the ship. It's good. It's like they will insert it into the real hot spot. It's really thin at the front of it. They'll make it here like it's part of the machine. So when you put your credit card in, it's not actually in the machine, so they're still stuck in this device. And then the device realize the information between the machine and your car, and in that way also reports everything. It goes between the private machine. Right? And additionally, they'll hide some sort of camera somewhere that watches your bed, which is why my sketching machine is not having fancy things where you cannot see what is entry? European.

All right. All of this comes from a specific reason. The same reason. You now have special fashion seats designed in a way they sort of ask the things going on. We cannot easily insert any additional hardware into the machine. Right? As they give an example. So how do we do with education over opening? So let's say we have alice and alice wants to access and read her email. Adams has a username and password. Adams seems the username and password to the email server in plain text. This is bad idea because anyone that each drops this message.

Now forever often pertain to be alice because now I have alice's username and alice's password and I can pretend to be alice. So returning to the others is called a masquerade back. I can simply pretend to be someone else. Right? Then we can say, we don't want that to happen. We know that is bad. We want to fix it, so we don't want others to sit there using them across within plaintiffs. What we'll do is will count others to encrypt areas of them as possible. They say using public encryption. So the email server will send. And the public key is the certificate of email server. So we can verify the civil server and email servers and gentlemen. It will come to alice. Alice will use the email servers, probably keep the encrypted username and password. Our alternative artists can see refusing them together with the hash of the password, the email server. The email server also stores as its password to see if it's better. Email, et cetera, will hash the password. It keeps. I simply compare it to the hash of the password at the same.

Now we have the eavesdropping attacker we had before. They can't actually do anything. They don't know what Alice is possible. It is. They don't even hear what Alice's username is. They cannot just take colors is used as I am a password and log into the EMAIL server has done. In that way, we basically taking away the basic masquerade of time. Either is this system secure, and if not, here is dumping line, does this system work? How can I log into talents in this system? In this system, I don't need analysis using our password. I just need this basic. Because this message, even though I do not know what we're using them as possible, is containers are using them as possible. So I report this message, or I report this message, and I send it to the EMAIL server tomorrow. It is also going to lock me in the time, right? And this is called a relay a replay of that. Right? I record something Alice made today. I replay it to the server tomorrow, and because it has a valid use and then impossible, even though I don't know what those are, the server is going to log in.

Now, we've given the confidentiality, but it didn't entirely work. So what works? The final way we can design it to make it better. Again, replay attack is that we can say every single transaction need some kind of unique aspect, something that makes it to having happened just now. So I cannot record it and use it again, tomorrow or later today. Right? How would this work? The EMAIL server will make a random number. This random number, it could be called enhance. It basically means number will be used once, right? And send that to others. Right? Alice will then do something to our possible encrypt that hash, whatever. But when doing search, you will also do this loss and send it back to the EMAIL server ok this could be encryption. It could be hatching. It could be signing for 30.

Okay? The EMAIL server knows the value of response with. It is better than this value that goes back. However, I cannot replay the message anymore, because if I report this message and together tomorrow, I go to the EMAIL sooner and I say, hey, I want to log in. The EMAIL server is going to give me a different aim, because every single time anyone asks people in, we get a different name. And the correct answer would then have to the evening we try to have, I just have a correct answer for the whole day. Therefore, I cannot log in as far as so in short, to prevent the replay and masquerade the parsley and use it like detail is heated. We have something that's new every time or something that's fresh every time also concluded nearest. So let's take a break. So it's the o'clock. We can take 10 minutes break, and they will get back. All right? Thank you. You need to have a in the circle me, too. You did that is the findings as a final. If it were to be given, think we are talking about that this moment good enough. So is going to be.