### Security\_week8\_lec01-20241029\_14:08

说话人1 00:00  
And then you break it, because it's so they said, instead of napping, they say from 40 to 100. They left from 75 to 99. Right? If you've got 60, in this case, you did quite good. That is the average that probably gives you ad something in that direction, right? Then something about 70, starting within a minus. This is not a this is just in history. I just to calibrate yourself on what happened for this, actually, the average with a little bit longer than to see. That's it. Some people still did very well with the higher grades. I I really think it was the possibly a slight problem with wisdom create. And I think it produce some people as a list. If I probably there, like, I don't think it's entirely only white ball, because I used to face it before and people were not confused, but I can understand how people can be complete.

As such. I'm going to count the letter on the part of the c five, then 560. Right? That is just the average of resistance to 66. We are acceptable for. And I explain what the problem was, the question of create later, right? And it's just like, ii think it's just an english thing where I was expecting a certain thing and some people from what I expected more, again, spend some extra time trying to do it. Most people try to do it. It didn't really take a long time to do it. So it was like maybe wasting a couple of minutes on it and then giving up, but then so leads you probably lot of 5 % minutes trying to do it. I I guess I break we will also post everybody's friends canvas as the people who are not here. You can see this. Let's just remember that we are marking it out of 55 out of this. Just to remind their funded the actual way, the 4th grade works, the problem said, why is 10 %?

The second problem is 10 % in the midterm between me. And then they were exam is 60 years, right? So the good news is that the average for the problem stage is very high, right? Way, too high, way around the average. Right? So if you met them, right? Is not that, right? Maybe something happens. That doesn't mean your final grade will be back, because you probably did ok from c one. You can still concentrate and do really well in your problem state two. And then your exam could be okay.

For example, the problem state why? If you would like on average and you got around 70, you got 70 again for the second problem set, and you only got 50 % in the better. If you get around 75 of the exam, you can still get it very good. Right? It doesn't mean things are over loss if it happens not at all. Right? If you really consider like a bread, then you can talk to me.

I will also make announcement later today on canvas. Having you, we showed us mark which question of the midterm as everything you have to be concerned about that question, you can ask a specific or you can ask me. Okay. Let's talk about the questions. The first question relates to one time pass. Right? And then questions. Question one was actually very well answered is the average of the situation was 55 very good performance. The idea is that you're just going to do status. One contact will be cutting me to give you a student number, to instruct our message, and you can use the table to basically convert between these 80s and your student number to find the value.

Everybody will have slightly different answer. But if I just because you did number 12345678, the last 6 meters is 235678. I make that into the binding value. And then basically, I take storage on to the scientists, and I will get a result. I think I made a copy of paper on this, too. Is it for our person? But the top one is correct in this a 52, 85. I don't know you did not get it right. So basically, if you great for me. So you basically just make your own student number binary, you make the cyber face or the banking primary. You excellent to get up, engage your encrypted application. Okay? Then the next one, if you intercept a subtext of a five to a five b and the middle part of the main text is d and you don't know that as a character, if you don't have a lot of characters, but the middle of the characters.

So how do you modify the subjects? If the nerve pain takes part of the trip to 77 instead of b 77? Instead of pb so this is like the question we did in the tutorial two. Right? Remember that? Before a question where the guy tried to see money, he does the bank account number, and he tried to change it to his own bank account number. Exactly the same principle, you take the two a you can visit the binary, you take the db you can visit the binary. You take sort of, if you get, it is a private history, which is 93. And you take so that 93 in your maintained, if you wanted to be the student statements and then you have any subject a five p four, five p which is the receiver of the decrease. The middle part will change from dp 70.

They know in general, not that I expected you to do this, right? Because in the future after the sports, if anyone somebody was asked me like, but how can I do fine read? These are business directors may be buying these things. In practice, like we really thought actually like even if you have windows calculator considered to the programmer mode, I will do all of it for you. You can interface numbers and finding numbers. You can hear the decimal number, and then basically just do all the binary functions and the world. Ok so if you ever have to calculate it very fast or something else they need to do is mean some standard calculator. Question two, they were too mobile operation. The one is cfd the other one is on the road. I give you the three equations for the encryption, and I ask you to give the encryption equation.

This question was question two, was not that well answered, but I think it also has the most difficult questions. In the case. The last two questions asking about the files, and then that sensor data, those are challenges. It does otherwise. That be hard. Very so good to see you the standard software. Reasonably, your answer. Counter mode, c zero is the encryption of ivx or to d zero. C one is the encryption of iv plus one x or to p one. And c two is the encryption of iv plus two x over two. That means the plane takes is the encryption of iv explosion zero. P one is the encryption of id plus one, x over to c one. And p two is the encryption of id plus two x over to c this one is quite straightforward for c and b mode. C zero is equal to the encryption of id export to be zero. Cy is the encryption of c zero takes over b one, and c two is the encryption of cy explore.

In 2 months, the biggest problem came here. So some people instead of saying trip here would be tripped here. So what is the trip? For cdc mode? It's description if you actually be crippling something as anything storing it with the previous id on this previous artificial. For esd mode to have p zero, it's the encryption of id explore. D zero. D one is the encryption of c zero, so to c one, and p two is the encryption of c one, xox during the transmission, 1/5 of c zero is changed. The one that is changed. One box is lost to that equations. However, you have all right, and which one is the error complication? Less briefly explain the error? The error is worse for mode one, because one has two clock error, another one, who only has one here.

So the 2 clock error is one. P zero is equal to cyx or in the encryption of id that is ignore that of itself. I'll let it over here. E zero is the encryption of id export to c zero. C zero is incorrect. Then e zero is going to be incorrect. D one is the encryption of c zero. They sort of c one, c zero is incorrect. P one will be correct. P two is c one and c two that will incorrect. C zero, p two will be correct.

And then suddenly, for, if you look at the counter mode, you'll see that same time. There's only one block. There's none of the blocks involves c zero from 83 years transmission. So it's easier or wrong, easier. It's going to be wrong. And then after that, you want you can, I don't know why it will be placing this. During transmission, the entire block is lost. So which mode is better? If we go back to the decryption operation for this one, if c zero, cy and c two, and say it becomes c one and c two, and c three, then we're gonna have the missing block. We then gonna have an incorrect block, and then we are gonna have a correct block. We basically do it easier as the encryption of id takes off to see one, which is gonna be incorrect.

Then we're gonna do. E one is the encryption of c one. C one takes over to c two, which means p one is actually p two, but it is still correct. Then p three would be c two, xo to c three, which means the actual p three. But it's actually correct. So we lose a block, and then you will have one block incorrect. And then it will work. Right? For the second one, it is more complicated. If c zero disappears and we have c one, c two, and c three, all of the messages are going to be incorrect forever. The reason is because p zero is the encryption of ivxo and c one, but it should really be the encryption of iv plus one.

The next one were gonna say e one is id plus one, x over c two, but that was encrypted with id plus two, because we have the synchronized counter. And by using that log, we are basically lost synchronization. Right? So for the receiver, for the rest of the message, the whole state of the counter is always going to be great for one, in essence, for remaining loss. I will fix those big problems.

Okay? You need to encrypt customer records. Are they stored on a server? You regularly need to access and update these records, which of these modes would be more efficient to use? We can explain why it would definitely be mode two, because they might too, if we want to decrease, let's say, the first block of customer data, we just make the counter, we encrypt it, we explore it through the record, we get the faints record. We can update the plaintiff's record and then re encrypt it. And that has no impact on c one. For cfd mode, we can basically, they say we can encrypt iv we can extort it to our record c zero. Then we update the p zero and we re encrypt the new c zero. But now c one is defeated on c zero, and c two is debated on the new c one. So that means we have to decrypt and re encrypt all the remaining loss to make that update on that quality. Right? That was also in the slide, on the slide, in the note, in the next months where we discussed compromise, it is also explicitly mentioned there.

So the last one, you wrote a system where there's a hardware device that is used to create sensor data in factory. This we're basically using the same to data to control. So it's very time critical. Essentially, once we take this into reading, we have to upload it with the . one statement. Ok so we take a sense of reading every 1 second, and they only have one thing to the second offer. Your device can do an x or a 0101 seconds. Add a block site birthday 0 . 065 stickers to encrypt one book. You use one of the modes of operation to a and explain your answer.

You could use mode two. And why you should have realized this over two, you have one segment between readings. So actually, the device can go. I know, i'm making a reading 1 second from now. I would need to encrypt it very fast and sin. The device can be compute encryption of id encryption of id plus one, and encryption of id plus two. In the moment, we take the reading t zero, t one, and t two. You can do the three x source. You can say it means you are on the part. For the mode on the left, you cannot do things early and you cannot do things in parallel. Right? Because for to encrypt c one, we need c zero and to encrypt c two, we need c one. That means we have to get their readings. Encrypt c zero only once we have c zero can be encrypt c one. Anyone wants to have c one? We can encrypt c two. That means we have to do everything after one another. Right? And that will take too long a time and we will miss our final ..

So the answer is, what is it? So for question three, given e equals thirteen, q equals 23 and equals 19, rather than the equation for signing message, show your population and make it 24. So it is equal to three times q is equal to 15 times 23 is equal to 9. Phi of a is equal to d minus one. C minus one is equal for re is in the modular inverse of e modular yn you do the extended to the algorithm to explore the 13 × 19 + 17. 19 is equal to 1 from 17 + 2, 17 is equal to 1 × 2001. Then you work backwards. Why is equal to 70 minus 8 times 2? Which is equal to 17 - 8 × 19 - 1 × 17, which is equal ~ 9 × 17 - 8 × 19. 9 × 17 - 8 × 19 is 9 × 264 - 15 × 19 - 8 × 19, which gives you 9 × 264 - 1, 25 times 17.

So we apply what you like to 96 to both sides. And we get one more to 1996 is congruent to - 125. So i'm 17 more electricity. Or if I have one to the interest is negative, so we make it the smallest positive value, processing the modulus values at once. And we get a equal to one, 23. Right? Then the answer is just the signature is the message 1234, raised to the private exponent, more to this game, which is 299, and that was needed. Just write down the equation for signing the basis. Unfortunately, I think more than 80 % of you try to solve this equation, right? Which you were not required to do. I did not expect you to do it. I just ask you to write down the equation, but I can understand how some people get a little bit confused. That is why they tell us, because if you actually then started doing square and multiply to try to solve the equation, you could pay a lot of money, okay?

But apart from this question was also very well answered recently is actually also very well answered. It's like question one. So that's good. That means most people in the material job, which is great ok for question b you have an alcohol encryption system with probably why people behaving and equal to calculate the product ds what you should realize is that y is equal to g to the h one p there's no real way to calculate it, because p is only 11. The easiest way to do it is just to group for search. You have to try one in number until you get on the us right? The answer is seven, right? X is equal to seven. I see, is that very key to the white one? Pe to the two more pe to be what we have to get on the piw briefly explain the difficult problem you need to solve to do this. This is the discrete locker of the problem.

If you have bc and d it's easy to calculate a but if you have ab and e it's very difficult to calculate c and then why are you able to solve these very difficult questions or difficult problem? It's because the numbers are very small.

Remember, when we said when we worked with basic matrix property, the strength is, in the fact that the numbers are really big. If the numbers are small, we can solve the street operator problem quite easily. If the numbers are small, we can solve the factorization problem. Questions? Right? So basically, we need larger numbers for this to be secured.

Question four, what mechanism can be used on a radiation? Explain why it provides under mediation. The digital signature provides another creation, because only one person has a private key. And inside of this, right? That's the reason. Okay. Would you be able to use one of the block side? For words, in question to a construction back in a way similar to acbc mac? Briefly explain the answer. So this was also intended to be a very challenging problem for me. Right? So the answer is actually, no, neither of them was in a to be used to calculate a map. The reason for that is because both of them actually quite trivially allows the modification of the banking. Remember that when we do a map, we are sending the plane takes message together with the back. Right?

So we basically know what p zero, p one and p two is when we are doing the back population. Let's say for mode why we chose p two as our mac that on that tag is the encryption of c one, right? Together with the x or of p two. Right? But we know p two. We can x or p two, if you see two, and then x or any new p onto it that we want to modify that lost loss of paintings. Right? And we can do exactly the same with calculus. Right? We know what c two is, because c two is on that tag. We know p zero, p one, and p two. Once again, we xop two to c two. We will get this value, even though we don't have a key, and then we can x or a new plane takes on it, or any value that we want. But operations do it and definitely be a bad one anyway, because the 7 days between c two and you want to be zero.

The only one you can easily use, in any case, is the first one, which is similar to cdc mode. And then it's intended to be designed that every psycho fix the things on the previous main text, right? But let's go have the same issue about the law school. You can basically change the law school very easy, so it's not a very good factor.

Alice wants to say data involved and also provide data origin of integration of d so that can be modified. Alice involved only the message back to adn does this message achieve what alice wanted to do? It does not because it doesn't actually help bob anything. Bob gets a map of the message, but there's no way. So the message would be, right? The data be, but there's nothing that bob can actually do to make it work, right? Because bob cannot take a nap and extract the data from it. He's going to get his back. Value is going to say this is very nice and I don't actually have the data and I think is verified against this mac. I can also do nothing to this mac and try and extracting the usual state data out of it. Right? If alice and b together with the mac of d right, then it would be fine. Then we would be addressed, right? But just saying involved, the mac doesn't actually transfer any sort of data or message. People.

Then for the last questions, aes has a half 90 2 bit block size. Aes is one twenty eight one ninety two and two fifty six fifty. But they've lost eyes are all the same. They're all 128 %. But the secrecy means that encryption method is secure, because attackers cannot practically find the fedex with the computing resources that have available today. This is false. Why is being described here as computational secrecy when we talked about computational secrecy? The secrets in two places when we talked about one of that and the very first nature of the course, when we talked about why we wanted to give it here insecurity or insecure. Right? So this is false, because perfect secrecy says, even if the attacker has infinite resources, the system should still be secure, right? Like one time higher. Even if the attacker has all the primary resources in the world, it was supposed to be a recent person today. Isolated cryptography can be used to provide confidentiality. That is the origin of mitigation and repudiation. This is true. It can do encryption and his new initial signature, and the initial signature can provide focus on remediation and be bigger deal.

Then the point in that coin miners are saying they actually random number r and cohesive cars equal to the same number provided by the system. This is mostly guys the right integrating condition resistance of the hash function. This is false. There's already a different value, and the guy is trying to find a hash to that step given value. Remember, for provision, the guy has full control over both values. This is either more related to one radius or secondary in the resistance. If you mention either one of these, it would be ok we have given h of x we need to find an x that gives us the same as, but we are not a value that is gonna give us the same category.

And then the final one, this route for search requires an average six to the 2 to the 60 guesses. This is false with this as it is 15, and they actually estimate is to say - 1 is to I will fix the one of these more issues. You can ask what I was supposed to be the solution. I will post the solution from you on campus, so you can check it there. You can compare it again to mid term. If there's anything wrong with you, met them and of marking or you, if there's like a simple thing wrong, like the marks missing, you have exactly the answer in the solution that the mark is missing.

Then you can talk to the da that last question. I will put that on campus. If it's more complicated question, like you answered something, and it's not the answer in the solution, but you also think it should be correct. Then you are more welcome to talk to me and you can think about it. It is also a good solution. So that is everything for the listener. I think I just want to take the short like a few minutes, right? And then you can just think about you with them for 1 second, because I just have to move the nature slides to this, because we are trying to do the, according to the lecture again. And partly to work from this, I did not want to report the solution position for the rest of the next year. A private nature of what do you expectations, but I have to be 5 days ago and maybe it starts. If you just give me 2 or 3 minutes, is that ready? We can start to make sure. Ok.