cs915.m4a

说话人 1 00:00
Final exams in 2013 and 24. Iii think that boss some of them are trivial. Us is included for you. Again, spend a few minutes just to go through different questions. You can very quickly start with these ones. I prefer short, brief and quite answers over lengthy and natural experiences. This highly recommend is this before everyone to base one on my excuse on governance system? When I do have some classes and questions related to the second total ok because you call this in some of all the lectures. So some students have the tendency to provide more explanation about what you have been asked for. We have to see it, but I do not recommend it to you unless you are quite sure what your own hands. Because in some cases, maybe very cases, some students get confused, so they thought and answer the right question.

And then they are so many more stuff or not. You will use someone. Let's say, if the question is, for 5 months, I I I I might be the one for 2 months, depending on what you wrote and how many marks I don't know.

So what we need to do here, we need to answer this question. I'm gonna answer no more. We must be able to get very high the difference between democratic tools that we covered in class.

So namely, we solve cushion techniques of the property totally harsh functions. Why do we need them? And where do we need them? And signatures of I believe this is it. I don't know what people think on the one's website, because I wasn't quite sure what or why this happened. We usually have asked time, but these problems have been more important. Tmd us. Is it to score down e it was the end when she is. So ii will find the exams. The past papers are available here. Now, if you click on the ceiling, and then these possible absolutely from 20, 2004 and 2023. So you can look at these two exams that is true. If you are cs 45 students, this one is missing. Ii don't know why. That's why I provide the need for cs account for the company to receive.

I want to go over the last exam because I think there good example in a similar source, same logic. Definitely the content is not the same. Okay? But the largest substrate is, I think it doesn't matter. Do you have any questions so far? So my we got these. I will give you something. Because I know this won’t be increasingly the most of you, a global example going on. And also be that gives you some indication on what mistake I don’t know. Yeah, it’s gonna make sense about how we can do on this conference or which section you could skip for when it was important dot com.

And then for those bonus.

Right now, if you keep away from this example, you can expect to be hard like what you said have done in the course. Byebye poisse with this one. And so let’s get started. What i’m going to do and I will probably be to be history. And this form will write some notes here, probably. Then you want to expect for what you expect from it. Can you see the question? But before this, cctv ppt msn. Working. I know you haven’t. I went to the material and because for the more billions for the month, or in case remembers anything, you can just suggest, goodness, that’s fine if you are wrong, but that’s okay.

Same chord with the summer 2025. For all the exam, you should finish it. I want to take one on clothes. That’s it. All.

The first question is something you will have, something is positive or will change it. I heard come from is about specifically for the top and you all the faster you have to do, which is one very be useful in certain manual software. Isn’t it debate and stubborn?

We have to answer these questions. I will give you some minutes on how you provide an answer.

If you have, if you have talking about some deputies, you are asking for the 1/2 of the past have good neighbors and input and the output, and use the function that you have your involved for this all group, remember, is you are done and use this notation that we want to remember. Index on and all index part. Could anyone tell us what these letters stand for? An xr and r and xr for memory? Anyone? So you have a question that we have it a message. I won’t think of it. What happens here? Music, that’s ads for ds is based on possible number. You remember it on numbers? Ios. And around very good, we have rounds. So that will only divide the message in two blocks, let’s say, over 64 bits each. And then each block will be valid to use the left or and boss. I’m going my english growing again, but let us do the good question. And it's only interesting.

So c left arm, let's see, ok and drive on. So all this on. So we have this message that if you want to draw that spine and control like this, this is the block going into 2/2 left and right. Ngo. We have this new function here. This is that the function here. And it's going to make a secret view. The index, I let's say, and you would have rather export function with export. One course is going to actually to become the left port. So this is one wrong and the price of the structure. So I left + 1, and they lift power. So this one will be used. This one's going to apply as a function that takes the pkrn right? Or so invest in our group. And that's going to output the result of we don't come to write for from those following so that we can call on consensus.

You can find the in terms of it, found it and you keep the company business.

So as long as you provide us with diss us, I can do it growing this thing, left eyes, left for becomes early on. Sorry, so anybody, so you understand what's happening. So they will export next. So it's not the first. Yes, it's an excellent.

Let me use a different color for this population. It's not just addition. It's an export operation for this one. Excellent ok exclusive operation with the function outlaws, which is the wrong function applied to the wrong part of the input. Isn't the eastern tables, then we swap, keep swap. And so depending on the global grounds, eventually get in the wrong message. If you do this time index, I really see themselves.

Let's put up the the same question. The fine state natural is known to be convertible. What do you mean by this? You could use this mathematics equation or equations expand more. It is in groups. So it's not a very complicated. And do you have any idea why possible networks are reviewed? So what do you mean by this? I on the problem, yes. We can use the same structure to decrease the message. Excellent. So we can use the same as a structure to include and be used as. And this saves you a lot of time, and no need to have another piece of power to resolve to to include the message. You can use the same algorithm. Let's see how it works.

So what should we do about it? So let's say i'm repeating the message like this for cctv, ktmgisoemeineticenico cftc. An enemy has to be how do you have the message broke? And in the private sense, we have sort of the problem of secrets are, so we have to do. But the relationship is going to be which one. And you can write that normal. It's not a he is, if I want to go backward, you follow these others.

Byebye. What I want, then I if you have evidence I plus one, it's going to satisfy the relations of underwriting. Let me do this how it was one equal to all of this stuff. Yes. I move on. And our index 5 + 1, something right here, equal to, or who can tell us about anyone? How did you compute the examples? One? Yes, very good. And I so that you can write it this way. And next time, x four, xoki products, x four. That's all the function that dates for the key way in the store in the organs. Assy. Now, when they said to do, but now what do you want to do? Because we have the subjects no more to recover index on.

The government gets our model in this higher and higher index. Eat for me. So you want to compute projects are, let's start. And this is the answer you can see here on the all index calling, the simple end is one o if I want to open an index of people who are yes, r index I plus one, because we have put the bankers on this one and xo with one. This is on very good.

So export, when you can explore the same, I let's say you explore the message and itself, you get what? Youth. You are going to export one with one. It was or zero is zero is zero. It's our comments here, because I export our power + 1 with this function. Also x for this second part of the equation with the same function. We passed the show. And the trick here is for x four, the x four or five plus one with fo so fo k index r and r index r but that not have our next on it, but that part of it I would like to see ngo iphone ppt. So you just understand how the these groups and how all these symbols and things work. They will be.

O in a question like this, let's say instead of putting li plus one, like straight and I plus one, what's the ri and then say that on the r it's gonna be possible, correct? Because we know the value of our next part, which ends the next time cost is a system. Ii do we need to explain that? No, I if someone people gets replace all of these parts are in the full figure who's to get more. That's how it doesn't. I I this is not just for you, former step because of the father given elements across one and all index across one, we can be covered putting this on. And following this. I just it was a good question. And as an advice, also, in case, so for this example, I for this question, you got to be I so how is if anyone talking about because of that, or some order mostly by court, you can trust me.

How do you remember little bits? Some things about the first structural already years? Can you get some fucking answer? Yes? What do you think as normally possible? You can still get some modes. Even impression me. You can, if you remember what's in good news. If you don't work with the technical details on continuing the equations out of all these marks, if you are able to explain why you are doing, remember that some being known on disease, and later on. So at any stage, you might be able to get something often, except in a specific case, when you are used to be coming experiment and so on.

This could be a more check our team, try to do less for memory, Understand the concept and provide us through. Thank you. And that group solution based on your understanding of the boss. Now, for questions that bs has 60 norms, all the odds are the same except the last one. I'm hope you brought it out. I want to explain the difference in one ppt and providing doesn't quite as it could be more about korea. People were talking about how much people would like.

And then it's very simple dreams course. Instead of one such wrong, so called one wrong, we have to draw the we are not for one to just one, and then we lost do you remember? What was the last round? Is not similar to the previous 2 months? Anyone? And then there is a compute, ii hope so. Remember, we have left, right? Let's say I start with that. That's zero with that one. Let's say i'm gonna talking with that one. Okay. And then we swap. So then the simplified restructure he was in nana. Is it? I byebye. Then we have the almost 16. I don't know, 16 or his name. So we have swallows. And last one, what do you do? Remember? 1 month, bs. Leander. It was very good for every twice, because excellent. Here is what you just risk. You ktv. One rule was in here. This is. So eventually you get that 16. So we get left 16.

And then so if we swap uc ev ev ep ep, just the highlights what happens if we have swap the loss. And this, we have gotten left 10, 16, and 4, 16.

Don't do this one because of the encryption. We have possible. So again, these reports that's wrong. Modify this on just the loss. And instead of swapping as 15, the output, the last song you would like this. Here I want this. I don't. And this one now, you never understand what when you get seven, 16, even and borrow 16. Okay? They all 16 and 16, and then feed it to the encryption, same as is that this? So you have the swaps also accepting the loss, found. And that's it becomes straightforward. Yes. And how many are also encryption? We need more so 16 months. For the encryption, we start with. Please open your book. So we start with the left, one, right, one, for the encryption. Hope it would be all 16, right? 16 and less 16. And in the description, we start with all 16 and 16, eventually, we will end up if you reverse this. Course is exactly the same. Cctv. Nana, what is it? So let's check the loss of the question.

If you are getting the block side here on the short side, hoeo nasa. Hopefully someone is talking about it. This is ds and not ads is weak. Somebody suggested to use two ds so there is one po these cookies. And that's not only you have the message. Are you going to be if they want them? Are we good? Is it the best? He obtained long terms he of gave me again and we often from the first listen to the first time. Confession is deeply breaking this cycle should be good important. Finding both keys, k one and k two. And we know that the studio ps is going to fifty six fifty dispute. This is, in theory, so 56 starts to 50, 1,020. It's definitely from the roots forces. And if you want to try out all the possible keys, if you want to do, we have to the power 112 possible.

Some people found clever to talk against you, remember how we can practice here. See, what do you have any ideas to create this article? Is it would be impossible. Okay, so we have a very famous in resources, man, individual. It's like a natural artist involved on getting together. And you have enough apples don't talking to separate jobs. It is man doing this one very similar, great. But instead of a man in the middle, it's called neat in the middle. So i'm gonna meet the attack is going to ibm is then two payments. Each statement will have to the whole pieces and use all the possible. Because we can check as an attractive are going to about our rules.

Now go to then all the possible encryption of this matrix and using key k one and store the results in the table. Ok this is all the possible peaceful k one, because we don't know what k one is. You don't know how many possible do you have to the powers? 56. And now we stop, because that also has access to the subtext. You see, it's going to the same procedure in the gross order. So check the results for by going from right to left, and see what all the possible values we get in using the key in the random key pages apply to, partly once you get this table that has oversized 200, and that has 2 . 6 countries. Overall, we have neighborhood that we saw that all sides 2 × 246, which is the following 57, at least.

Now, recently, check for marching direct that table one, table two, it's not going to be a kind of a look of once you find and you will find a match and that which keys they were used. Let me go with. This. It's very simple. So let's say you have table one. And this table one has entrance here. Okay? These entries, you have completed them using some angle keys, so not all, which is, well talked about. This is app one, pp two. That's it. And then you have to put an index to the following pieces. Then we have also another thing here. You don't need to draw a table, for example, that's funny. And for these entries, and also we have, so i'm gonna say, what do you want? It's so ii normally then just won't get confused about k one, k two, k two, c these are numbers. Maybe I should have numbers on. The difference equals k one, k two.

So either you more risks, but kk something, and he can't write something or the more conclusion to your foundation since you're talking about the pka but that's fine. I will not tell you what it is done.

We are going to be a they won't. But here it is, not changed k one. Zhou, hu xin, they want to, they will be train one default o the organization i'm using here is, let's say k one one, k one two, et cetera, on the market elements. And here, what you can do is focus on pk two. Ok, eq into, et cetera. And the index going to be for scheme that came to up to k to also to the following businesses. So this is true when all these and all where is huge shape. So what behavior is? So it is, they do. And they do more is so they groups group or what do you do? Then? The mi led to the cio message, and then to do the socket, see? And that somewhere here, in this record is going to march with this once you find this marginal order, because only uk index r has been used as well as he came next chip.

So it's comfortable. You call do you have any questions? I think you want me to do the tables or just provide some explanation, because the question and I don't choose what to do. I don't concern. Yeah, this is question what the wrong? This one. Let's go to this one.

Id ios of keys, one secret in hong kong for our state, for example. Now, you will not be forced to do any technical complication or need to do have a good understanding. Like I say, technical about some specific examples in american example for me, to be able to know this team would, if you use, let's say, let's say you have others and teachers to jerry to help these and the public.

Remember that in rsa we have to start with a lot of numbers here to happen to follow. And then a few power land, which is going to be 2 - 1 + 2 - 1, use probability you can add on tv there's going to be probably. But the choice must satisfy this condition. We should be put on the fire. How can we get the probability? And what is for this country? Upm so the first part is begin, at least since the poverty. So I don't know, but I I maybe similar for me. So practically, we have include one more about that. So we one very good bye, man. So if you tell me this one, this is called the group. I you need to find that should be in the mostly inverse form. Multiple, byebye. I know, maybe you haven't advised, or you won't say. But if you get an evolution, pceoe power, that is something to do on, then you will not be able to acquire the extended in our land.

Gd all you have to do here. It just reminds us with this aspiration.

And if you have, let's say, ad close e ok so we start to find the deep that's as far as this condition. Using the extended degree in an argument, you don't need to go through the ethical details, just save the whole.

Remember that? D and e so the secret team and the public team should be inverse of each other. Id id early.

Ok. And actually, we have a hint here. In question, if you forgot about it, you have a hint here. Because he said that he wanted implementation as is going to our safety and you must pass for. So you can stop here. What do you remember about? It's really interesting things. So encryption, if I compute m to the power e over n what do you get? C multiply m by itself. How many times? E dots. And actually, it is probably that same. He is going to do this.

So if you can send on board, I want to send a message that can be read by others. I use her public key. They took the message ok so message and view and the kitchen pulses are we included using the public view of us, rcinaseder the sum of text is equal to mb the module n once honestly seems this c she's going to do what? She's going to decrypt. It isn't by applying what you can see to the problem in this part. And singapore v is equal to what is c it is m to the power.

You should be a basis for me n d here we have the ok which is equal to what? M to the power, ed and we know that ed is one, ok 10 numbers. We know that this value is actually, and this one, ed is equal to one. The message. So this is actually the message. So whether the modulus end, or when the rb is the rb what are the module stuff? Which you have to add? Iii still of each all the operations should be a computer models, module, and always, just to say some space, I if you, right? This is not and also for so that was not a long.

Nana. Ok. You haven't answered the question yet, by the way. And the question is about a semantic security, which used to be public school probably be interested in the system. What is semantic security? This is a memory question. The other example, you can use this rsa system. If you can build, it seems a bit option on the news of the pdn and supposing the price is £1,006 and the partner into sets with it, how can they modify the viable to be done that? We have asked to the option is required. We saw one example, I a simple example in the direction, because you should remember that the textbook rsa is not secure.

Before we read this answer, the first question, not the second one, but the first one about semantic security. Any idea what semantic security means? Anyone remembers what semantics really means? You could say that if you are in a particle, you get actually the software place. You shouldn't be able to derive the Information of the plane test. Okay? One way to say is the the soccer test of the public key inclusion system should be in distinguishable at home and the ground system should be ground, shouldn't give you any pain about the origin and ok even if we assume that the attractive has unlimited resources, are there in this place?

So in the TV we call what happens with wang tang pop. I know all the messengers say, and then you are you exploit with the secret team. If you are not darker and you only see the sockets, there is no way to tell what were the bits of the original banners in the states, too? Because it’s 50 % chance for everything to be equal to zero or. Okay. Let’s take a break and then.

imct, NASA.

Iphone