### Security\_week4\_lecture\_2-20240924

说话人1 00:00  
Is multiplication. And finally, the addition of the right key, which is simply an xo right? We took it through this. Each one by one, the bias substitution is, once again, just a simple lookup table. So we have a lookout tables for encryption. Then in this case, an x box is a substitution box, but there is a lookup table for encryption. We have another inverse is also for the literature.

For example, we can see that we have zero and zero. The mapping is 63. If we would go to the six to the three, you will see that it maps down back to a zero gate. Right? So quite simple to implement one thing to keep in mind, though, is that in the standard, the s box and inverse is false, is given. Right? And they are chosen to be of a certain format contains the numbers by the designers. If you decide to make your earliest walks with your own random numbers in it, decipher will not be secure. Use the x box. And in this as well as given in the sand, it's not just some random numbers. And we put into the box. I have some of me very carefully chosen to have some important quality. Right?

So for this example, i'm not going to do it in class, but if somebody is really interested in how the cycle works, you want to work out one single around yourself. I have given the examples at the beginning of iran to say, is this one on the right? And after the substitution box, the same should be the one on the left. If you want to go through and see that everything works. And remember, this is the first one is ea after 87. He's not creating. So there you want to take it out for yourself. You can just follow this example and take out your answers. The second transformation that happens is the third row. Once again, just like the substitution, the shift row is very easy. The first row of the matrix is not going to shift at all. The first row of the matrix says the same. The second row that I think is going to move one to the day. Three is gonna move here, two is gonna move here, the one is gonna move here, and the zero is gonna move around.

Then in the third row, everything is gonna move there by two. The three is gonna move here. The two is gonna move here. The one is gonna move here, and the zero is gonna move here. The last one, everything is gonna move around by three. So one is this, one is basically here. This one is in here and is zero. Then here. The very simple rotation of the matrix. Right? Once again, it will be example, and you wanna take it with the numbers so far, so good. We can't expect everything to be so easy.

So now we get to the one transform. That is a little bit more tricky, and that is the miss follow. The next column is basically an object matrix multiplication over a finite field of order eight. And this appeared useful for the daily mail to make sure that if we multiply, the answer is not larger than any of the values in the finite field. Once again, this year is used for whether he was given. So he promised make it what it really want. Ok in terms of matrix multiplication, if you remember, sort of high school or undergraduate matrix. If you're looking for this one here, it's basically this row multiplied by this point two times this value must be up to this value plus one times this value plus 1. This value, if this value.

That's the matrix multiplication, what do we mean by finite yield? Ok as I said, this is not really a critical force, but we still trying to expect a little bit towards you. In fact, the basic idea of a finite view is that we have a finite field of a given order. As usually we have a finance view to the end as a order of a a is the order is eight. But to expand it, begin to go a little smaller. We can work with a finite field over three down here. The basic idea of finite view is that I have a number of values that I can work with, and they are all within a step. And if I add, subtract, multiply of the five in a certain ways, the answer will also be within the same. If we have a finite field of order three, basically, we have 01234567. Those are eight, the ideas, right? And whether we add, subtract, multiply, or divide, our answer should also always be within that range.

Okay? One of the first things that we can do when we think about finite fields, if we can basically each finite field has, basically, there's two to the elements to the numbers. We can define it as polynocles. We are all the polynomial sizes, format of a to the a minus one times h a a a minus a a to the a minus two, one, 230 a dot a one x plus a zero, where a is always the value of 01, depending on whether the corresponding bit of the value that we try to represent, the value of. Is it zero or one?

If we look at a very simple example, if we have a five to the e to the a we should have e to the c sorry, we have a a four elements. We could be polynomial, and the polynomial is going to be a two, a squared plus a one, x plus a zero. I guess that this polynomial basically represents a boundary value. Right? The total number of values you can have is eight. And it goes from 000, to 111. If we want to represent 000 as a polynomial, it means a two is zero, a 10, and a 00. The problem is just be zero. All right? If I want to represent 111 is the quality of zero, that means one times x squared plus one times x plus one, which is nk squared plus x plus one.

If I wanted to do 100, it would be a squared by zero, x plus zero. It would just be x squared. These final numbers are just sort of a way to represent binary value or binary. They should take up as and how to break expression. It's not all that pretty obligated with one another. Addition is also privacy. So we have to follow those together. We treated almost like a simple expo. If we have two of the same part of the meals added to each other, they will just cancel out. We have h squared plus one plus h squared plus h plus one, a squared plus a squared. This cancels out. 1 plus 1 cancels out, and you have lived with an x if we have a squared plus a squared plus a squared, two of them will cancel out, but we still have an x squared. Addition of these four number is quite easy, where things become slightly different and difficult is with the multiplication.

All right. The moment we got to multiply for the news together, it's very easy that we can engage something that is outside of e we get in a larger number that we should. Hence, we do that once alone with the irreducible polynomial to always limit the size of the answer that we didn't get to stay within the final field. Then we have exactly the same polynomial as before. All right? If we have ax times u of xa three plus one times x squared plus x plus one, this is the same as binary value 101, i'm fine, then 11. But this is why the number four. If we multiply everything up, and it's just simple, good of the right, you get h squared times h squared and h to the wall. Experiment of h is h two is three, x squared times one is x squared, one times x squared, x squared, one times xx one, and one and one. And we then added together. We get ace to four, ace to b plus ace plus two. But we are supposed to have any value that's not to the x two two, because that would be half a finite field to the degree.

So we cannot have these. If we do the one below, we now have to do the logic of this result, a squared plus x plus one, which is there be so for a number of order three, that means we have to factorization. We get x plus one times x to b plus x plus one plus x squared plus x if we do the one in the reduction, so whenever we have anything multiplied by the one to other, it has a reminder, and it basically releases zero.

And the x squared plus x ok essentially, what it has taught us is that x function f times function d which is 101, is equal to one, zero, because a squared a a is a one. There is no final zero. It is here to take one on zero.

This is just an example for there to be, right? In terms of as we do exactly the same thing. They're very useful for them. It's very the family here, there. This is providing me for. If you wanted to do an example of our list, I have done one for you that is work out. I'm not gonna work it out, also read it. And I ask for you, but if you are interested in our economist works, and they talk about policy that you are interested, how it works, right? You can follow myself.

So I think all that the beginning is just happening. Over here, the green rocker matrix multiplication. We have 87, 60, forty six eight three eight six and multiply it by 2311.

You basically have 3 × 80 73 × 60 + 46 + 50. Where is reserved at the top here? That is this decimal value and this corresponding binary value. If you want to represent 87 s as a polynomial, he first made it in binary with 10000111. If we write the corresponding for the w dot, this would be ah seven.

Now, x six, now x five, x four nine, x three, x two, x and in europe is this one. And here, right? That doesn't happen. And after that, you just want to point out, you cancel all the double terms up. And then you factorization and you do your election, you should have to get along here. Great idea. If you're interested ahead, you can take a look. If you don't see all of those, you can explain it. You think. Right? The last term function is the addition, right? We simply take a rocky, it was also 128 bits, and we a sorted to save matrix. This is also wants to be very easy. The add on key, the shifting and substitutional easy, the mixing. Here is a little bit more complicated.

In short, if you look at the overrun function, we have a say, the substitute each of the independent bias. We then shift all the roads. We multiply it for our mixed column matrix to the part here, the support from the production. And finally, we do and takes all right. So in terms of looking at how these things work, so the finance, new mathematics is maybe a little bit new, seems a little bit complex. But a lot of these things are quite simple. We are substituting the life. I we are just rotating. It may be thrown by black. We are just doing an excellent, right. If you have to know when code this, it will probably be reasonably easy.

That said, if you were to go and design this, it would be extremely hard. Right? So I can show you this slide, and I can explain to you how it is. Everybody has the substitution, is everybody has the rotation, is everybody can multiply by a matrix, everybody can do an exorcist. Those are basic mathematical planning operation. Right? However, you want to know why all of these things were, why the values were chosen in a certain way. Then you can go by the book, written by the designers of aes right? And I believe that book is about the elements of behaviors. Right? And it will explain to you all the mathematics behind why these specific functions are very good for creating that diffusion, cohesion. We talked about. Right? We break into the 5 point. If you have a good group of a is considered extremely good.

If we have to quickly study in 20 minutes, it is easy for us to try and understand. Right? It is therefore easy for us to infinite. Right? The last . is the designer, i'm going to say i'm going to study specific mathematics and topography for years and years and years and years. And then you get to a sense where you are a massive expert, right? We try to see this may be only a few people in the world. We'll see later when we talk about that functions, the same guy that design, he is also on the team that design to be keep the use of your hat offer.

Clearly, there's a couple of, if you think about the competition that this runs from the island is 100 proposals they got from people who are really, really smart, only four that are to be good. Right? This is required by people who with a split in this area, right? And only four of the proposals with the name.

So it is very difficult to design for anyone, even somebody that's experience, right? Which is why we come back, why we did already designed these results regularly. I will waste, I try to do it. He wants to send it. Okay. I'm not going to discuss the wrong function. In this. We also have run functions. We start off with a scheduling algorithm that's been expand a piece for us. Basically, we end up with, he said, it's 8 by 8 bytes, right? We set it up into words. Why do they do with doing with three words up 32 bits? Yi mei. Every single time we want to go to the next round function, we take the with three. We were there for a of one. We go by substitution, and then we will take.

So over the concept, the class is given standard that gives us a permutation that the x or the w zero can be the 74. 74 is an x equal to w 1 to 75. We find these will tell me if you don't say that means it's basically going to be the 77. Every single time we do the round, we do this round. Again, we try update. Okay? Right? So that's the end of the years. Right? Just to come back the space, we used to estimate the total amount of reform, say that we need to break so many decipher. The space is all the possible keys that you can have for any specific design.

There is a piece that piece of the space to do. Since when we have substitution father, the key space is all possible alpha, basically you have. So you can see it. B six factorial for a is to be two to the one twenty eight two to the 192, or 2 to the six, one time the size of the site for the figures on the side of the message. So the message was 1,000, as long as he said, to be in 1,000.

Then what does the key space for rc four? Rc four has a variable in size between, is it 14 and 2000? Okay? So that he spent the 82 to the 40 to 2,000, right? Okay? Which brings us to the next problem. I think that we're open and we talked about the wall cider, and the boss either has a fixed loss eyes. So gray is if I can create this, right? None of the data that we want to see is only enough to create this. It's obviously going to be longer. How do we actually use box offers to improve things in practice? All right. Should we have basically a new people in block?

Now that would be incredibly difficult to implement? Would be where is the why not? Essentially, should we try and improve each law independently? This seems like a very obvious option. We can just take our message clearly to have one, create the loss interval by interval to interval 34567, et cetera. Or should we do something smarter when we basically make the scientific dependent, not only on the current plain text, but also on other plain textbooks, in other words, should be changed together. If we are going to do multiple blocks, we also need to think about how to handle partial walls, because my basis might not be entirely exact, multiple blocks. At least the last one is quite easy to pick up. So we should just basically you had it. All right. We should basically turn, you should basically had everything to be a multiple one to be interested if we're using ideas or at least a multiple regular walks out. One. The way is it being for the long sideways between the intro, long message are called modes of operation.

There are lots of modes of operation, and we will discuss about three, and then we will discuss four. The first one is an electronic photo that was basically the encryption be trying infinity. We started this one is very seriously broken. Then we can try a cycle of chaining when we change it in the box together. Right? We will also look at counter code. The counter code is a slight, interesting environment, because counterone is both using a boss like her, but it looks a lot like his insider.

We'll look at the benefits of that we gave it. The first thing that we could look at is ecp mode. Our attention is as five context, is equal to the encryption of pk of 5 days of p and binding copy is the encryption using the pay of the size of the c ok so there are various attention when we could use. This is one attention, everything before the promise feedback. Our benefit, we can also have e on this for a rapid heat. That's another way for us, but it's the same thing.

When you see the mode, scientists, not one, is the encryption of some plaintiffs, not zero scientists. Not one is the encryption of scientific or one. And subtext of two is the encryption of the plaintiff's law, too. And the degree p zero is equal to the recursion of c zero. P one is the recursion of c one. And e two is the diversion of c two.

So we see each one of the laws are encrypted completely independently. One of the ways that this goes wrong is that the attacker can reorder the loss. We have a message that basically says how this likes for. This is like a all the way apply. I was like ball and really like stone. And then we assume that the device would be p zero, p one, p two, and p be as follows. We encourage everything and we have c zero, c one, c two, and c three. The only problem is treaty doesn't necessarily like this. She goes. And what if I decide that this loss to be c zero, c three, c two, and c one? Now how this likes all and truly likes? All right? And this was very easy for her to do this one, basically shuffling this type of baseball service. All right? So very easy. Right? Because this is every single plan takes off, this maps to one corresponding start facebook.

The second thing that happens with ecbd is that we encrypt the same plane takes twice. We're going to end up with the same architecture to be sitting there, and she sees that ci is equal to cj she knows that the two plaintiffs false police are the case with the same. Right? This gives her some information. She doesn't know what the plaintiff is, but it does give her some information. So this is a serious issue that depends on what we are using. For some cases. It does not matter in some cases where truly that they observe a specific action being painted, it might be more serious. This is related to traffic analysis. Sometimes people who give me a traffic happened not necessarily looking at decipher case or plain case itself. Right? So truly might be watching a specific bank. She might see a transaction coming from a customer, but she sees the source happy.

And then later in the day, she sees that the why is that person? Is it amount of salt? All that really does is keeps and watching. And next week, he sees a similar transaction, right? So she sees that some of the socket case values are exactly the same coming from the same customer to. This is gonna guess that most likely later today is gonna be another software for the company by the same company.

All so then she can predict if you have a situation like this could be a problem. Right? If we want to illustrate it in another way, right? We can improve alice. So here a it's like a wife in each of us, and we can improve this image using ecd mode when we encrypted with ecd mode. And then we find that the cyber fixed values back, he said the grace tale, he basically still end up with us. Right? You gotta tell us exactly, but we still have the patent. Why does this happen? Because the same plane takes, he says, the same side of it.

Why we have not done with if we use a funny total mode, is if you think back to our substitution side of the previous nature, is we now basically got the substitution sign for again, our alphabet is nice to be here, because I alphabet is two to the n where n is the number of bits of the block size. But we still have the same issue we had in the constitution side of them. Right? The cycle days is going to have the same happens and saves the single properties as our plaintiffs. Right? And obviously, this is not good. And we thought that when we discussed the situation suffers why this is not good. Why is a better way of doing this? So a better way of doing this is the cbc mode, where we try to make the current cycle, this block in not only on the current matrix mode, but also all other main base blocks that are found before.

We can do some change in cdc mode. We have an initialization paper, which is random, but doesn't have to be secret. Then we'll have c zero is the encryption of ida sort of zero. C one is the encryption of c zero, a sort of p one. And c two is the encryption of c one, a sort of p two, easier than the encryption of c zero. A sort of rdp one is the description of c one, a sort of c zero, and p two is equal to the description of c two, xo to c one.

We can see what we've done. If we can see one. It depends on t one, but it also depends on the previous operation.

If we do the same thing with others, as we did with pcp mode, and we see what the effect alice has not completely disappeared. Right? Because if we now improve the same underlying primary value for acbc mode, it's not going to map to exactly the same size of a term, because that's how it takes value. Not up to me. The things on the current place is very interesting, but also all the previous effective books that were included. It's much better at having stronger the agents of all the underlying factors if we calculate in some cases. Right? Often means secure. What is a good model? We already say this is dependents of the subjects depends on more than the current matrix. We want limited error proclamation. We look like air propagation. So if something goes wrong, I think he doesn't recover. We ideally want some kind of synchronization. If we want to recover from area creation. We want to many optimize some other things. So maybe we might be really reduced encryption. Maybe we want to incur a mind size only.

Now I concur degree, maybe there are some other things that we need to consider in terms of the wider impact losses that have fun in a time. All of this with feeling to what we decide is the best box on earth for us. Right? Then there's a transmission errors. We can have two final errors. We can only have transmission error. We cannot transmission loss or transmission error. If I sing for my message and I saved c zero and one of the bits of c zero, let's say, goes wrong. Bob is a different version of cer that is the constitution error. If I say c zero, c one and c two, c one goes missing, completely involved, only gets c zero, c two. That's a function of laws. Reverse opinion final, as far as this error propagation is, once we have an error, how long will this error affect all for? Is the current law gonna be incorrect that they involve start getting the direct bank this up?

The next couple of laws will be incorrect, and then all gets the great plaintiffs up will basically be The rest of the message of all destroyed. How long after we made an error as if error actually continue or propagate on? Okay? We look at that a little bit more detail shortly. The next mode of operation. We can look at this counter mode. And counter mode works as well as we will not encrypt the p zero. Actually, we will choose a counter value, the civilization, take care of the initial value. You can treat it as zero, you can treat it as 11. You can say if you did it zero, we script 0 and the x or the result of p zero 0 c one. Then we encrypt one, and we explore the result of p one, usc two, I group two, and we encrypt that to p two, usc two. We decrypt the receiver has saw this with the same in initial value in groups, one, in groups two, a sort of values in p two. You get p two in terms value. Keep seeing one to get p one. He took his value to see if you get, you see the interesting thing with compromise.

Now is we use a loss on her to encourage this value, but it actually acts like a speed cycle, right? Because if we look back at the speed cycle model, we had a key, we had a pseudo random function, or ec did right there. We will a so that history to the bank x there is a game to make the same, the street, a sort of the size of a table, try to make that this guy's rather than have a spatial pc then right there, we basically made apc generator with the block side.

It's actually a loss offer. It's a loss on the mode of operation. But we can argue that approximates, basically, it seems up. Right? People like this mode, for example, is this mode is very strong for if we story files and we want to read and write very quickly, we are going to be considered, as let's say, they say we have a database of customer, right? And every customer is encrypted as one box. So customer y is c zero and customer two is cy the customer v is cp our customer wants us to update the details. Let's say customer to us update the details. Now we have a feature c one. We decide the corresponding all state of the initialization vicar. We encrypt it, right? We x or into the c one value to get the p you get the plaintiffs. We then read it by text, we updated by text. Then we write it back in, and we explore into this value again to decrease. We don't need to update anything to c zero. We don't need to update anything, c two.

Let's say we try to do the same thing with cbc mode. Lets say customer one possibility to come to the opposition. You can operate on variables. The d curve is quite easy, because I understand I mistake the previous value, previous reports go on this, which is c zero. I hate to read the description of cyi have the customers radio that okay.

Now I update the customers report. I write it back to the file, and I interested again, I see one is equal to the encryption of c zero and the uq one. Right now, what else do I need to do? Now that i've updated c one, what else do I need to do to the rest of all? If I use dbc one? I have to then decrypt it up at a higher as far, right? Because originally c two, the patent of c one. But if I qualify c one, now I have to make a new c two with a new c one. And that means I have to decrypt d two, reading curve d two to a c a c sorry, with a new c one. If my file is very long, I would not be stopped basically re updating the entire race of the block from the point where I would like.

In that case, if we are just doing read and write, read, how can I have an advantage? Because if I have ap one, I don't have to update c two or c zero on the update c one. That is when I go next one on the show rangers, the cfd mode. So cfd is the worst a combination of counter mode, cdc mode, because we basically slowly changing, but we also essentially for the speed cycle.

I guess ic zero is p zero export to the civilization there. C one is p one export to the encryption of c zero, and c two is p two export to the encryption of c you see, we still have the speed size are like x or incurred with beaker. But the way we popular streams, in this case, decided because every time that he speaks the current clock depends on the side effects.

For 50 years ago, africa is the vision of area provocation. All right. If we went to compromise, for example, let's say we calculated c zero, cy and c two. We said that default, alice by c zero, cy and c two, he says that default. But on the way to block, part of c zero is corrupted.

So they start to say in c zero, why do you think does that have unfold in terms of p zero, p one and p two is p zero going to be okay or not?

Okay? Are there any? Right? Because if I say the c zero and the c zero is an error in the way, you use the incorrect c zero, micro p zero, p zero going to be incorrect. Right? What about p one? Is it be ok the other thing it's going to be ok because c one was ok e two is going to be okc two is ok right? About we look at cbc level. Same exercise. We take c zero, c minus c two on the way involved, c zero as error. What is box p zero? And it looks like is p zero going to be okay or not? Okay? Because the base on c zero and c zero, it was wrong.

Now we use wrong things to calculate p zero. P zero is great. What about t one? Ok about ok not ok right? Because t one, the base of c zero. What about p two? I'm not p two is okay, because p two is not actually the thing of c zero. Right? Now, the role is only using c one and c two to cultivate p two. Right? And both of those are great. Right? In this case, when we talk about error propagation, we say the error propagation is too long, because one error is c zero, makes p zero incorrect. It makes p one incorrect. But p two is not. We can look at this exactly different. Or if we look cbc mode, the basic idea of cbc mode is we have any of these initialization data. We explore that p it is a value, and we encrypted with pk the ideas are outside of things.

All right. And alice will catch this on the decks. She said it before paul currently has to create id cash. And along this way, c goes wrong. She thinks it correct. Id she disrupts the wrong thing. She exploded into the direct id that she gets in the correction. Right? And then it caches the c worker. If we look at it like this, it works as follows. Ci is incorrect. We decrypt it, which means this value is correct. But the cash value, the previous soccer they fall is great. But that doesn't really matter to be a sort of incorrect interacting to create the incorrectly. The recipient passes this law to decrease the nation of this law. The nation of this law comes in is correct. He cursed, right? Correct, a sort of the wrong thing, incorrect. If I pass it to ci plus one at the top, ci plus two comes in the curve that is correct. It's sort of the directing attacking us directly.

It works itself out in two iterations and two loss.

Usually, ii for example, I think the cbc or cab side pictures about in which everyone I don't know. You can do that in notes, but we should learn pages. I have a full written explanation of how similarity happens. And cap without doing the features here be, there's quickly talking what happened is in cfp is c zero is incorrect. We know p zero, p one, and p two will be correct. If I say c zero, c one and c two, and there's an error in c zero, what happened to p zero? P one? E zero is a pain on the head on the bed. He wanted on the pain. That's okay. P two is. Okay, good. So it see if he has a similar property, seap right? If you want to get really complicated, there's a slight difference in the way. Because I think in the cfp is a wild bit error and many bit there where cbc is a many bit error than 1 bit. Right? We don't worry about that in terms of propagation.

So this to end with the general discussion, we looked at all of this between 2 weeks looking at the matrix encryption. We looked at a lot of underlying construction of a a is if you are a big photographer and they didn't find a few of the things when you are interested in really secure systems, what are the practical ways you can make way to?

I do I know if I design a system where I would buy a system that I am using a good, symmetric side, the basic cipher analysis, you can do it under a minute, is the first thing you look at is the key source. If it decides to be sure it's bad, why does he stand here today? Anything shorter with the size of 138 is not. Okay. Right? Very soon when we get to two thousand and fifty, some people already say we have the larger. Right? Second thing is decipher has to be public. Remember, when we talked about the cost principle, the cipher is only considered secure if you can make it public. The only thing people do not know is the key and it still performs well. Right? Public science have been to public scrutiny and they have some additional quality that comes from them. Right? These things onto the third point, right? You have to consider if expecting the cipher comes from an open competition, or whether it's some propriety thing made by a company and is hidden from you.

If it's a standard and the standard is recommended for use, it's most likely ok if you have older sufferers that are not standardized, but they are public, and despite the public, no one has managed to break it for a variable five, they might also be, okay. But the preference is to have something in the sense.

The next thing that they wanted to ask is mode of operation. It's very common. If you read hamlet for security product, for them, not to mention anything about the cooperation. Methods I have to say. So if I operate his ability, great encryption, usually that means ads right? But if I using it in ecp mode, that obviously is not very good. And basically they believe this is not the ads but the way they use it, the follow up mission should always be, I really like the fact that you using as but how are you actually using it to interpret the data?

I think I have an answer that satisfactory. You should probably find another product where they can explain what they are doing. Starting with cpc mode or another war with boston, these guys, he says, right? People used to be effective on cyprus, a lot of operations, which we'll look at a little bit when we look at the data of the picture. Right? This is a short case study. We need to practice a long time ago in 1995 for them. So in spca conductor and what a spot from school, the life essay, and the logic as it was secure using a steam soccer called the one. It has a forty eight fifty and it was not a public, right? This part became very popular. And basically for the five europe, I think large parts of the us people use for access control, for traveling, keeping, and for both a system. The cycle must be secret, and it was secure for a variable part. Right? The question is, if I was trying to sell you the cipher product today, if I said probably uses that I have spot products of you, should you buy the system or not?

If not, why should scare you in this description that it is to you that you should not buy? Is this a public system? Right? Because it's kept secret for privacy product. Why do you think about the key size? Is the key size low enough? One of the days, it was a fifty six fifty that already have broken 1998. Very easily, the size is small. Cyber hit secret warning sign that we should not use this world. Right? What eventually happens in this product is around 2006 2007. Some students or a student project is easy to do. Waited, reading, reverse, engineer, decipher, and they made it public.

At the moment for poverty, people look at the side there and realize that the cycle was actually created me back. Right? There were various attacks to do as far as I think if you reported to transactions you can. But I think it is, here is the same. Okay. And overnight, basically a lot of these systems behave insecure. All right? Because these cards are not secure, right? And this happened over the city. People are relying on this product to do a lot of things. And there was a big issue about cross. In reality, it wasn't indicated because most of the systems are basically online systems. They keep a copy of the file in the back end. So if you went to force it, either modified it, I would be detected. But so people were not very happy that this happened. Right? How did they do it? Just to show you how easy it is to buy a computer business in your things, even though you think it would be quite hard, is they actually took the smart card and inside the smart card would be the great decision, the children.

All right. What you do is you put some acid on the package and the acid will dissolve the plastic and will resolve the protective nickel layer. And then you make the Top locking layer, the Top logic layer and maybe the second player are always deeper than x they basically connect parts of the city together. You can see a a lot to run across and then put the acid on again, we find it for a second amount and then you wash it away, which means that acid eats to the Top metal layer, you can be the same as a layer.

Then you can put a drop as the one again. Wait for it for a specific amount of five and then wash it away. It will be through the same layer and you get to the bottom layer. You can see the bottom layer looks different, and the bottom layer is actually your logic. These are maple substrate that make our semiconductor that make up the logic of the binary operation.

So basically, you have events, and you have 2 days and 9 days. Not 10 days, you have two. These are bad or you better. You can basically did. What they did was they wrote some computer vision program at the time to look at the photos. It matched specific patterns, and then see what equals. And then they used to talk to layers to see how these logic is, but basically connected together. And then they end up with a sign for diagram. This is a very standard architecture for a linear feedback should register base, as he thought, every part cycle, you basically shift everything you want, and you end up with one, the on the street, right?

And once they made, you get paid for decipher, then everybody has to look at it and decided it was really hard just to sort of make it. So we don't really say this one specific product was bad. They call me about security of obscurity as all around the time they did this, where people realize that this is possible. Other people started doing this with all the products of the plant. Right? Basically, exactly the same thing happened with a number of proprietary RFID the data system. So you have the Micro classic, you have the axp high tech, the microchip. It takes its instruments, these two significant responder. This one here is also quite interesting, because at the time it was used for a lot of interesting things, they use a different approach, a tested increments that follow the patent will decipher.

So it didn't say exactly how it worked, but they had the basic occupation. But they didn't know exactly what ever thought. So they sort of put their own little high computing cluster at the time the whole language can be able ones. They grew for search, for a certain combination of impact register values until they figured out what the cycle is not exactly.

And then once they figure out how it would be exactly, they also found out it was quite easy, right? If you basically resources is, I think it will be hours for a couple of hours. They want to think of this is that this one was at the time used for a lot of cars as the security for your mobilize.

And so if the tag is there on the feature of the car will start. But it is not a part of myself, right? And it was also used to buy fuel in the us they had some YouTube figures that they were speeding each of these cars driving around. I it would be, all right, this case for the ti we have similar issues, right? 40, 50 capacity of Micro, classical, 40, 8, 50. It was all the right. So one of these things broke because they're basically unsecured, because they were all secure. And aside for it, they were actually quite how they it's a reminder that if we want to focus on today, make sure you decide going on, make sure you have a open on the cyber and product. And that should give you some assurance that your products over time. Okay. We have the engage. If you have any questions, you can ask me here for real. So what are you doing for yourself? Not serious. I will put all the nationals and everything. And.