### Security\_week4\_tu-20240924

说话人1 00:00  
If we have the main things architects the maps you is the same x map into the cycle case according to the alphabet, then they are hidden, right? Each single by dates as to the same single side of x and basically, we also knew that there was a special subset of the substitution suffer, which was the shift cipher, where we make the limitation of a bit like this, shifting the side effects of a bit with regards to the plaintiffs alphabet. In the first question, basically, the equation says that we have a cedar cycle. It gives us the cycle takes, it asks for the plane. This is and we are told that the most common plain text makers in the plain text are e and I we know from what we talked about frequency analysis. The main issue of institutional cycle is that the action or the behavior, statistical behavior of the main text is not changed when we go to the cycle text.

If we know that the most common plain text is eni then we can go through the psychotics, and we can go look for the most common psychotic figures, which is l and h we know that l and h must be e I the other thing that we know is and what the question follows beginning with a shift cycle, we know that the subtext alphabet is just a plane that shifted relatively to the planets.

Therefore, we should also know that h should probably be the e and l should be the line because l is better than h and l is better.

So I say the e is not good. And from that, we can make us a petition of it. Lsihz is a constant shift of three, and the validation comes, iai saw, I conquer, right? And they say by judaism. Okay. Question two. And this gives you a little bit more basic practice with the substitution suffer, encrypt the following matrix using the substitution center alphabet given, right? Using the given up a bit, the subjects becomes ehyllehd some interesting things you can just see here, as of the frequency analysis stuff that we know. We see that the same happened in the plantings that you're also happens to decide what they say.

So we have the e is starting in. It just happens in the alphabet of maps to the e so we have to eat beginning in. We have a double a as well. We see that the pattern does not get broken out in any way. And then the second one, if we are interpreting the time case, j is equal to sy we have two ns, then epric so basically, it becomes submitted. So that's straightforward. Substitution platform. Next thing is the 100. So we know that the 100 needs a key that is random and equally. As the papers were interesting, we encrypt and encrypt by using an x or so we take the plaintiffs, the x or the key to get inside of it. We take the side of this. We explore it to the key to get the plaintiffs. We talked about one time. We said that it has a very nice security properties, because it's the one cycle that's theoretically secure, right? Because if somebody with infinite resources would force all the secret keys, then they can still not determine of any certainty while the great message or had loss, right?

In terms of a work example, we're working with the reduced alphabet here. We can give you a table to map some of the letters to a binary value. It's not doesn't have any certificates. It's not ascii or anything like that. It's just something for this specific exercise. And we want to ensure to where hello with the one time at acde we take the plain text, we can write it down. We can write the binary representation of the bank is done. So we get the binary representation from the tutorial table. H is in 011, and everything else you can get from the mapping table as well. Then we have a one one, fabcdae let's get you divide everything done, and then you can do xo we remember the xo function. It's a binary operator binding bit, x or vibrate bit. If growth is zero, then the answer is zero. If growth is one, the answer is one. If one of them is y and the other one is zero, the answer is y zero is 0 = 01 is 0 = 1, - 0 = 1, and - 0 = 1.

The first side of the fixed value is h what I said last week, whenever we explore anything by zero in this game, the same value back. The second one, e and e zero, and zero is 01, and zero is one, 00 ~ 00, ~ 1 ~ 1. That gives us f for the l 1011101000, one, and 101, and 0 is 1. It's gonna be good, one of them, but our side of the expansion is basically h if ji okay. From the question three d we are using the cycle test. We have been the previous mission, part a and we encrypted with a different one point path. So instead of using abcad using it or be done, and we need trips saying doing xo the h is 011. It is 0101, 00011010 is 11, and 1, is zero, negative c if we do the entire encryption, now we get a different word, which is polite.

And that, as you mentioned, lost family nature. This is the secret of the strength of long time.

In this case, we have a very small possible alphabet, but if we had this same case, sorry, but then we had this soccer picks. Hhik essentially, we would decrypted with all possible combinations of the one I had alphabet. We will also find all possible 5 meter combination of paintings. This is going to have a lot of five letter words in it. That is going to sound like a valid message. All right. So I realize it was hello, and now we made flight. But it could also have be any other language message, including the correct one, including the other. But the attacker is going to sit with basically every single possible message. Any one of them could be the real message. None of them is gonna be more equally likely to be correct than any of the other. So basically, the attacker is not good enough. And that's the basic principle of why syria can be secure. We'll basically get all possible messages back. As a result, the fact that even if he is able to brute for search for the key value, he will still not know that hello is specifically the one that is correct, because it could also be any other part.

Okay, so one disadvantage of the one time bad report was key management. He said that even though the 1 time kind of theoretically secure, it is not practical to be used. All right? Because every single client becomes sending message, the key must be equal and make the message. And it must be new, and it must be rather, right? If I were to go online dominating b and then it would be like a 400 bias. For us to use 100 ad, the key must also be four gigabyte long. Right? Then the streaming service must give me the one time path, because every single time I download, it would be the one time path is going to be different. All right. The one time guide itself is not as long as the movie, and they must somehow give it to me securities and no one else knows what it is. Right? If that streaming service provider has a way to give me that one time pad in a secure way, then they should probably just use that same method to give you. Right?

So in other words, it's very difficult to actually use one ipad, right? Unless it's a very short messages, really fast, but for modern data, it's pretty much useless. Right? What I did it for us, which is good, is that it's sort of people thinking about one and one of the soccer should look like. Right? They say if we know the scheme cider, it's going to approximately have everything. The one time tag had similar benefits, but maybe not all of the drawbacks in terms of us being able to practically manage the key, but still have an encryption and encryption structure that looks quite a lot similar.

What they say when the streamside curve had a short key for the sender, the same short key from the recipient, which did not change every single time. The message was said, all right. But the sender and the recipient would use this key and some algorithm to make basically something that looked like a one time pattern, a random sequence of primary values. They were then x or left to the main things to make the cycle test. The recipient will create the same sequence of wondering ideas, because using the same algorithm and exactly the same key, because it generates the same sequence, it can explore in the subjects. It will recover the plaintiff. So what we can answer the thing is we have a short key. We generate the xp of one compiler apply, or is it be a new random value? That's an equally matrix. We explore that we don't talk to fix the recipient, also make that 100 using his key in the algorithm, and it can extort the size of this to make a claim.

This is not as secure as what I have, right? Because basically, this is not a short length e so an attacker can search for the as long as short term p and if they find a short term p they can make also the same issue. Right? In other words, it's pretty much now standard if I can find the key of the screen cipher. Yeah, ok so quite easy. We have secret key in my key screen. So p 39 days to make sockets, recipient has a secret key. Next snp street, x or the side effects ok right?

So the last question asks, if you are renting an apartment, you are using a banking service to pay your rent. And the banking services use an extreme software to encrypt the message between you and the bank. And the format of the message is the market to pay, the account you want to go if you go to enable pin number or maybe a one time password to authorize the transaction. If your neighbor has exactly the same landlord, which means they pay to the same account as you, they can intercept your message and then modify this message. So the money goes to them instead of to the diamond.

What is essentially asking you is there's an attacker with some known blankets. We have a scheme using a streamsider candidate attacker with some known blankets, modify the encrypted message without necessarily attacking the streamside for itself. In other words, the actual algorithm like rc four, or knowing the key of that stream zone. The answer is, so we know that the cycle picks. We basically need the account and the amount and the password exhort to the p stream. This notation here needs concatenate. Is that our students always ask me completely something difficult, so this is concatenation. Our definition is used as an operator for streams. You want to add streams together.

Sockets is a kind of happening to the amount, implemented the password, excluded the key stream. If the hacker knows that can't value, then the attacker knows that over here, we have the cycle takes, it corresponds to the account. The attacker can take that with the cycle, takes x or it to the account number to get the piece of history back that was using encrypt this account number. Then the attacker can take that t stream, x or it to its own account number. Right? And that would give us a new socket fix, which is the actors account number, amount, and possible. And we send that to the bank, the bank will be transferred amount to this modified, accountable.

If we want to think about, then why do we need, in addition to confidentiality service? If we are using extreme software, we have to I think that we also need take the ok the origin of education. And this is actually very important. Whenever you're gonna encrypt anything with the stream software, stream software is and then it's not very easy to decrypt the data, but it's actually very easy for people to modify the plaintiffs. Even if I didn't know anything about the matrix, if I change the value of the ciphertext, from a zero to a one, from a one to a zero, if there is simply a decrypt, that plane takes split is also benefit. Right? It's very easy to waterfall.

So whenever we use a stream software, we must also have integrity service At the same time. And when we get to almost the last lecture in the course, when we talk about wireless security, we'll see that this is exactly when they first make a WiFi standard. It's the thing that they did not do. Right? They use the scheme cycle to encrypt the data, but they have no integrity and people showed it was very easy to on the fly change. Why? Right? In terms of looking at a workout example, if we have the fact, if we know there's a legitimate account number 154, we want the actors account. Number 5674, we're sitting 6,500, and then is 9141, right? So this gives us a message of money account. Probably it should be fun. We have some history, which is 01234567895, which is supposed to be random, but we pertain to the chat. We take the plane next. We exhort it to the key street, and we get outside the next. Here are the subtext values and the corresponding binary values.

Then hacker notice that these four digits in the middle, 5753 is the citation that come from. It's this zero. It's this one and this one. The factor takes this socket, takes value, exhaust it to the known plain text, which is 1234, and recovers the key street. You also not see it as part of the cigarette key street, 01000101, 01100111, right? Except the street exhorts into the attackers account number and gets the new cycle things. And then it takes the new attacker sockets, replaces the old sockets and gets a new encrypted message that new interpretive message, if we decrypt it by exploring on the original history that gives us the new account number, the original possible.

And if we send that message off to the bank, now the bank will basically cost for that money. Is that kind of 567? Right? So very easy way from 1 to 5. It seems like for encrypted data, right? Without going to without attacking anything in this library. So the important bit to remember is easy to modify the editor would be using stream software. If we're using stream software for confidentiality, we also need additional services other than origin indication or integrity sense. That is everything for the tutorial. Everything I will put everything at this Wednesday.