### Security\_week5\_lec2非对称加密-20240929

说话人1 00:00  
A all and hundreds of other people. All right? And analyses go to people in a company with 100 employees, which is one as we need to score 195 years as you will need a key for every single other person. Person. In that company. At the same time, they would all need to score another 900. And so on other 1990s, you talk to other people in the past. Right? So the number of these manage becomes very large. I really need a better way of management. And one way of doing this is simple as the management. The second way that we can use is probably key. So this is sort of originally made. I think the public key also be recommended. The management in itself is very complicated and we will have an entire nature on that later.  
所有人和其他数百人。好吧？对一家拥有100名员工的公司的员工进行分析，这是我们需要的195年，因为你需要为其他每个人提供一把钥匙。人。在那家公司。同时，他们都需要再得900分。等等其他的90年代，你跟其他的人讲过去。对的？所以这些管理的数量变得非常庞大。我真的需要更好的管理方式。其中一种方法很简单，就是管理。我们可以使用的第二种方法可能是关键。所以这是最初制作的。我认为公钥也是值得推荐的。管理本身是非常复杂的，我们稍后会有一个完整的性质。

But for now, we can just look at it in a slightly simplified way. So how does the same class be punished in 1907? Example as the management rather than alice storing the keys for everybody else? Alice and it was one key and that he allows her to go to some key distribution server, right? And similar involved business or keys for everybody else. He is sort of the key. They even open the key distribution servers. In other words, everybody in the system not only needs a small one. Why do you let it go to the distribution server? If alice wants to talk about alice talks to the server? And she goes, hi, I want to go to the ball. We need a key. And the server is, okay, take place a new key in cursive, alice using her key in cursive, involved using all ski and as of all, not as this new key or decision key, they can use to talk to each other.  
但现在，我们可以稍微简化地看一看。那么在1907年，同样的阶级是如何被惩罚的呢？作为管理示例，而不是Alice为其他所有人存储密钥？爱丽丝，这是一个密钥，他允许她去某个密钥分发服务器，对吗？以及其他所有人的类似业务或密钥。他是关键。他们甚至打开了密钥分发服务器。换句话说，系统中的每个人不仅需要一个小的。你为什么让它去分发服务器？如果Alice想谈论Alice与服务器交谈？她说，嗨，我想去参加舞会。我们需要钥匙。服务器是，好的，在草书中使用一个新的键，爱丽丝使用她的草书中的键，涉及到使用所有的SKI，而不是这个新的键或决策键，他们可以用来互相交谈。

And once I finish talking to each other, they believe that. All right, they can get about it. And next time they want to talk to each other, they will ask to celebrate it.  
一旦我和对方说完话，他们就会相信。好吧，他们可以得到它。下次他们想和对方说话的时候，他们会要求庆祝一下。

All right. So that is what I need to ask you, which is good. The problem is alison always needs to be online to talk to this additional server. I this additional several breaks, the same point of failure, and no one gets keys, and no one can talk to anyone else. Right? Public encryption is another way that we can do this. We can also see from this example of the difference between symmetric and asymmetric keys are. The app is, remember, as often as smaller than 70 and 70 of our size. It's the idea of having the matrix key in this system all has two keys, and they are not the same. The one key is by the key. He said priority within at all times, no. One else knows what the value of that priority is. Bob also has a public key. Bob has freely distribute that probability in any way he wishes to anyone that you wish. Right? And that will not impact on security. Right? What can be that probability to others or alice? And I have a probability and encourage a message for all, send it to bob involved in descriptive using these privacy.  
好吧。所以这就是我需要问你的，这很好。问题是艾莉森总是需要在线才能与这台额外的服务器通话。这额外的几次中断，同样的故障点，没有人能拿到钥匙，也没有人能和其他人交谈。对的？公共加密是我们可以做到这一点的另一种方法。从这个例子中我们还可以看到对称密钥和非对称密钥之间的区别。记住，这个应用程序通常比我们的尺寸小70到70。在这个系统中，矩阵密钥的想法是有两个密钥，它们是不一样的。一把钥匙在钥匙旁边。他说任何时候都要优先考虑，不。其他人知道优先权的价值是什么。Bob也有一个公钥。Bob以他希望任何方式自由地将概率分配给您希望的任何人。对的？这不会影响安全。对的？对其他人或爱丽丝来说，这种可能性有多大？我有一个可能性，并鼓励所有人发送一条消息，将其发送给参与描述使用这些隐私的鲍勃。

So how this house is going to be doing stage repairs are different for the management. Is it all can say I want to talk to alice or alice of all I want to talk to you. So I can say that's a problem. I'm gonna send you my public key. Alice will encrypt the key that you want to use, the public key, send it to all or will be created, rather than I have the cack they get the idea for su ps, probably by the key. Public key is anyone that means anyone can really improve message involved, but only one person will decrypt these messages. The guy in position of all priority, which is hopefully for.  
所以这个房子将如何进行阶段维修对管理层来说是不同的。是说我想和爱丽丝说话，还是说爱丽丝想和你说话。所以我可以说这是个问题。我把我的公钥发给你。Alice将加密您想要使用的密钥，公钥，将其发送给所有人或将创建，而不是我，他们可能通过密钥获得SU PS的想法。公钥是任何人，这意味着任何人都可以真正改进所涉及的消息，但只有一个人可以解密这些消息。这个家伙在所有优先的位置上，这是希望。

All right. Some of them do symmetric in terms of what we said. The attacker went such against this nature, be or the words of his message. Right? Even attackers here looks at the soccer decks. Right? Ideally, they cannot get the fedex, and nearly they cannot find the private key. But in addition, the requirement probably prepare is that the public key is known by everyone. So you should not be able to learn anything about the private key from the public key. Either.  
好吧。就我们所说的而言，它们中的一些是对称的。攻击者如此违背这一性质，或者说违背了他的信息的文字。对的？即使是这里的攻击者也会看着足球甲板。对的？理想情况下，他们无法获得联邦快递，并且几乎无法找到私钥。但除此之外，可能准备的要求是公钥被每个人知道。因此，您应该无法从公钥中了解有关私钥的任何信息。任何一个。

All right. In summary, as nature group purposes are very good, they are very fast. There is europe, but we need security exchange, ease. Then the model that works like better in distributing ease is acna to propose. And you can say it very well, because not everybody in the company is have a public private team there. And whenever they want to talk to anyone, they said that was probably they don't have to sit in a competition matter. That person can say the decision be, they can use hearing this combination, right? The interest here as a public key, there, a private key and a public key. The public key can be sent to anyone in any way, doesn't have to be different financial. The singer can use the public same messages. In other words, anyone can sing an improper message, but only one person can receive an e curve. A message is I only visited the curve is the violent position of private. That's the basic model.  
好吧。总之，由于自然组的目的非常好，他们非常快。有欧洲，但我们需要安全交换，放松。于是，更好地在分布中工作的模型就是ACNA提出的。你可以说得很好，因为不是公司里的每个人都有一个公共的私人团队。每当他们想和任何人交谈时，他们说他们可能不需要参加比赛。那个人可以说决定是，他们可以用听到这个组合，对吗？这里是公钥，那里是私钥和公钥。公钥可以以任何方式发送给任何人，不一定是不同的金融。歌手可以使用相同的公共信息。换句话说，任何人都可以唱出不恰当的信息，但只有一个人可以收到E曲线。一个消息是，我只访问了曲线，是私人的暴力立场。这是基本模型。

What is probability provides? When we look at a is a little bit is even when we look at the earlier version of c sovereign rc four, we saw a lot of very low level, binary shuffling, substitution, and deviation going on. And it was all about building nonlinear cycles by having non linearity, should not be able to characterize it as a mechanical equation. Right? How many teacher there is completely different? How many teacher there is basically mathematics? You can write down an equation for everything. Probably incur the security of probability of code is based on what is for mathematical library function. One way mathematical function is one that is easy to compute and find the answer. But once you have the answer, is very difficult to look back and figure out what the input to the function.  
什么是概率提供？当我们看A的时候，甚至当我们看C Sovereign RC 4的早期版本时，我们看到了很多非常低的级别，二进制混洗，替换和偏差。这一切都是关于通过非线性来建立非线性循环，不应该把它描述为一个机械方程。对的？有多少老师是完全不同的？有多少老师基本上是数学的？你可以写下每件事的方程式。可能招致代码的概率的安全性是基于什么是数学库函数。单向数学函数是一种易于计算和找到答案的函数。但是一旦你有了答案，就很难回头去找出函数的输入。

There are two famous problems or one way options. Why is that transition problem? And the sacred one is it is a sweet offer of the problem. So the accreditation problem was already talked very briefly about. Then I want to give you two prime numbers. I told them to multiply them together. You would be able to do that very easily as I give you x and y it's easy for you to calculate x times y and find z however, if I give you z and ask you to find x and y that would be very well. If I make it very big.  
有两个著名的问题或单向选项。为什么会有这个过渡问题？神圣的一点是，这是解决问题的甜蜜提议。所以认证问题已经简单讨论过了。然后我想给你两个质数。我告诉他们把它们相乘。你可以很容易地做到这一点，因为我给你X和y，你很容易计算X乘以y并找到Z，然而，如果我给你Z并让你找到X和y，那就很好了。如果我做得很大。

Similarly, when you screen longer than it's something that's similar, but working within the initiation, right? If I give you a and the experiment b and watch this in, it would be very easy for you to talk about it. But if I can be said and the base a and the modulus in, it would be very hard for you to populate the exponent eat. All right. If I very hard, it's not easy. I not impossible, not perfectly secure, right? When I had by combination invisible, it will take you a very long time to calculate what the correct value is. Right? The first algorithm that we will look at is rsi rsi is named after the papers, reverse senior and out a lot.  
类似地，当你筛选的时间比这更长时，它是类似的，但在初始阶段工作，对吧？如果我给你A和实验B，然后看这个，你会很容易谈论它。但是如果我可以说，底数A和模数，你很难填充指数E。好吧。如果我很努力，那就不容易了。我不是不可能，不是完全安全，对吧？当我通过组合看不见的时候，你要花很长时间才能计算出正确的值。对的？我们要看的第一个算法是RSI，RSI是以论文命名的，反向高级和出了很多。

All right. And if you want to think about it, I think rsa is probably one of the most famous is not the famous, most famous cryptographic algorithm. That is right, everybody, that's a discipline should have rsa and should have all the goods. Right? Rsa is in a way, very popular and very nice, because it's very simple. And in a way you can describe, it is quite elegant. It's a secure way to encourage messages. Is it a secure? Right? If you need to signature when we look at the next issue. But essentially, if you write it down, it's only 51. All right. You choose 2 times, you multiply them together, you calculate the popular readers. It need to be more generous when inspiration to curve, and while there is an integer. Right? Once again, very easy to write on the party. Where is it probably very hard to get to the stage where you can think of this is secure?  
好吧。如果你仔细想想，我认为RSA可能是最著名的加密算法之一，最著名的加密算法。是的，每个人，这是一个学科，应该有RSA，应该有所有的商品。对的？RSA在某种程度上非常流行，非常好，因为它非常简单。在某种程度上，你可以描述，它是相当优雅的。这是一种鼓励信息的安全方式。它是安全的吗？对的？如果我们看下一期的时候你需要签名。但本质上，如果你把它写下来，它只有51。好吧。你选择2倍，你把它们乘在一起，你计算受欢迎的读者。它需要更慷慨时，灵感曲线，而同时有一个整数。对的？再一次，很容易写上党。可能很难达到你认为这是安全的阶段？

All right. And you also have to think that they come up with this in the 1970s and a lot of people without, i'm not really sure how secure disease, right? Because why is it so simple, right? Which is also why when we talk to the next one about industry, stations remembered in one example from rsa the company that these people have started when they were trying to standardize and promote the use of ach program.  
好吧。你还必须考虑到他们在20世纪70年代提出了这个，很多人没有，我不确定疾病有多安全，对吧？因为为什么这么简单，对吧？这也是为什么当我们与下一个人谈论行业时，电台记得RSA公司的一个例子，这些人在试图标准化和推广ACH程序的使用时创办了该公司。

As I said, I would say, is incredibly famous. Recently, I don't like one that during the war for it in, I think, 2002. All right, the during award is, it's the nobel prize for computer science. The most proceed as far as you can learn the computer science. So things that one appearing prize before is basically things like all day oriented programming or pcpip or the unique operating system instructions and stuff like that. But I think these are designed the main code, the computer science. It is how many protocols that are also wanted during the war in 2050. I see very, very famous as a computer scientist, and there's a very large ass price like more than $1 million. Already, this was the interesting thing is that relations are one for rsa in 2002, and only subsequently after that time, when the uk government be classified, said the documents, then I think you realize that it might be some coordinator.  
正如我所说，我会说，是非常有名的。最近，我不喜欢在战争期间为它，我想，2002年。好的，这个奖项是，它是计算机科学的诺贝尔奖。只要你能学习计算机科学，你就可以继续学习。所以以前出现的奖品基本上是面向全天的编程或PCPIP或独特的操作系统指令之类的东西。但我认为这些都是设计的主要代码，计算机科学。在2050年的战争中，有多少协议也是需要的。我看到一个非常非常有名的计算机科学家，有一个非常大的价格，比如超过100万美元。有趣的是，在2002年，RSA的关系是一种关系，只是在那之后，当英国政府被列为机密时，文件说，我想你会意识到它可能是某个协调者。

So people thought about exactly the same idea, very similar ideas, roughly at the same time. But because they were working for government and they work with these excuses, classified government research, they couldn't really tell anyone about.  
所以人们在大致相同的时间思考完全相同的想法，非常相似的想法。但因为他们为政府工作，他们用这些借口工作，政府机密研究，他们不能告诉任何人。

So there isn't. Here I will be angry, famous. Most people never knew about, as you ask, why I was at the cost and I don't understand us, right? So maybe if they worked at a university instead of another man, and it would be very famous to decide rsas in terms of what rsa does. And these articles are very large part. Dsu you occupy them together to get in. And n is your public modulus. Then you gonna choose a value e the greatest on the divisor of a of e and phi n is equal to one. If you do phi n is this p minus one? This is only, if you remember about 585, 88, when you are, say, 58 and rsa says it's just e minus one times e minus one. He is in all the public exposure. So the public experiment together with the public modulus makes your property.  
所以没有。在这里我会生气，出名。大多数人都不知道，正如你所问的，为什么我要付出代价，我不理解我们，对吗？所以如果他们在一所大学工作而不是另一个人，根据RSA做什么来决定RSA将是非常有名的。这些文章是很大的一部分。你把他们一起占领才能进去。n是你的公共模数。然后你要选择一个值E，在E的除数A上最大，并且φn等于1。如果你做φ，n，这是P-1吗？这只是，如果你记得大约585，88，当你是，比如说，58，RSA说它只是E-1乘以E-1。他在所有的公众曝光率中。所以公共实验和公共模数一起构成了你的财产。

The next step is to compute the the e is the modular inverse of e module of ia so e times e must be converted to y module of I this is very deeply modular in this translation. And d is your private explosion or your private team. So do not have a public and private team. Your private key is basically your private exponent. You probably he has to propose a public exponent and a public modulus.  
下一步是计算E是IA的E模的模逆，所以E乘以E必须转换为I的Y模，这在这个转换中是非常深的模。D是你的私人爆炸或私人团队。所以不要有一个公共和私人团队。你的私钥基本上就是你的私有指数。你可能需要提出一个公共指数和一个公共模数。

So if you interpret assignment takes is the basis raised in the public experiment on the end. You decrypt, you take the scientific, you raise it to the private experience. You did a lots of reaction as to give you your reason, right? Very easy to understand. There is a lot to do. We look at a very basic example.  
所以如果你解释一下，任务是在最后的公共实验中提出的基础。你解密，你接受科学，你把它提升到私人体验。你做了很多反应来给出你的理由，对吗？非常容易理解。有很多事情要做。我们来看一个非常基本的例子。

If we have e equal to 30 e equal to 11, if you choose e equal to seven, use rsa to improve a is equal to n the first thing we do is we multiply pat together, which is 144. Five. N is this p minus one plus p minus one. That is 12 times 10, which is 120. Then we can do the master of english. 120 is equal to 70 57 + 1. So very much, that is the greatest on the visor between 7 and hundred eighty is one. So that will work up. Right? We can basically use the equation to do the ones that are in this. That means one is in the ground remains of 1 - 17, 7. That - 17 considered would be one that we need the smallest positive value to that. The easiest way to have it is just to add the watches value to it. So I understand people as hundred and twenty is 100 feet. So your private exponent and and modular english of seven module hundred and fifty is 1 hundred. Be right. And I have your public key as your public experience seven, and you probably want to design 43. Your variety is 103.  
如果我们有E等于30，E等于11，如果你选择E等于7，使用RSA来改进A等于N，我们要做的第一件事是将PAT相乘，也就是144。五。n是p减1加上p减1。12乘以10，就是120。然后我们可以做英语硕士。120等于7057+1。所以非常多，在7到180之间的遮阳板上最大的是1。所以那会起作用的。对的？我们基本上可以用这个方程来计算。这意味着一个人在1-17，7的地下残骸中。所考虑的-17将是我们需要的最小正值。拥有它最简单的方法就是将手表的价值添加到其中。所以我把人理解为一百二十是一百英尺。所以你的私人指数和7个模块150的模块英语是100。要正确。我有你的公钥作为你的公共经验7，你可能想设计43。你的品种是103。

The size of x is equal to the message to the experiment, e module, and state r seven, or to 143, Which is happens ok so in this case, this is an unfortunate way we chose another. So I said, use the numbers to show a funny result. Sometimes this could happen. Obviously, you should say I should not use the number, so this happens that you could do yourself, but it's also pretty hard. Then the message is equal to the subjects to the private exponent on the end, which is states the power hundred 3. What's the level? 143, which is equal to a right? You did it works. This is a much more complicated examples. You can work through this one yourself when it comes to this age where you need to calculate the monitor in this. Right? At the end of the normal theory nature, when I offered the notes for that to make sure there's gonna be forward examples. Two examples of square multiply, two examples of module in this.  
X的大小等于到实验，E模块和状态R7的消息，或者到143，这是可以发生的，所以在这种情况下，这是一种不幸的方式，我们选择了另一种。所以我说，用数字来展示一个有趣的结果。有时会发生这种情况。显然，你应该说我不应该使用这个数字，所以你可以自己做，但这也很难。则消息等于末端上的私有指数的主题，其表示幂百3。水平如何？143，等于一个权利？你做到了，成功了。这是一个复杂得多的例子。当到了这个年龄，你需要计算这个监视器的时候，你可以自己解决这个问题。对的？在正常的自然理论结束时，当我提供笔记时，以确保会有向前的例子。两个平方相乘的例子，两个模在此的例子。

So one of those examples of module in this relates to this question. It shows you how to calculate the modular inverse. For this example. That's the difficult part of our side, giving the marginally this. You calculate your priority. These are through this example. And we could act the other example or the modular in this example. What about the security of rsi rsa is based on the security of the factorization problem. The idea is that characterization is off. Okay, I heard people say, if we solving for unknowns, we usually think how much information do we have available? And reality for rsa we have more information available. It's only the attacker knows. There is a public market is in, and the public market is the product of e and q right? And then also now is in the public experiment and the greatest on the adviser of the public experiment, the phi of a is equal to one.  
其中一个模块的例子与这个问题有关。它向你展示了如何计算模逆。对于这个例子。这是我们这边困难的部分，给出了这个。你计算你的优先级。这些都是通过这个例子。我们可以扮演另一个例子或者这个例子中的模块。RSI的安全性如何？RSA是基于因式分解问题的安全性。这个想法是，人物塑造是关闭的。好的，我听到人们说，如果我们解决未知数，我们通常会想我们有多少可用的信息？对于RSA的现实，我们有更多可用的信息。只有攻击者知道。有一个公共市场，公共市场是E和Q的乘积，对吗？然后现在也是在公共实验和最大的公共实验的顾问上，A的PHI等于1。

Then finally, we know that is the size of xc is there any way so that you can find the index given there are information? So sometimes that is what they are able. However, people have discussed this rsa for them at me. Currently, the consensus is that to actually solve the rsa problem, it still comes down to factorization. For the attacker to win, the attacker must be able to factorize it. If the attacker is able to factorize in, the attacker cannot make file in, which means attacker that probability and calculate the file. In other words, the security of rsa pretty much for me to realize on how easy it is to track us to watch this.  
最后，我们知道这是XC的大小，有没有什么方法可以让你找到给定信息的索引？所以有时候这就是他们的能力。然而，人们已经在我这里讨论了这个RSA。目前的共识是，要真正解决RSA问题，仍然要归结为因式分解。为了让攻击者获胜，攻击者必须能够分解它。如果攻击者能够分解，则攻击者无法生成文件，这意味着攻击者可以计算文件的概率。换句话说，RSA的安全性让我意识到跟踪我们观看这个是多么容易。

All right? In terms of rsa security strength, you can therefore use a very complicated formula in trying to approach or approximate hard difficulties, in fact, prize any given. What's this? All right. It depends on the link of the market is similar to how we had. The brutal stage is the nations for was an entropy group of, we can say, as the rsa and that is sound, which it is, like our side is to factorize in. We can basically estimate how hard that is going to be. We got a radical medical equation. That's it. The effort is factorize is actually qualified. Rsa security company that was not about the use of public prefer. Every time there's people that is system was actually secure, you have to think about the fact that they have five versions, and they can't help people that is security group data.  
好吧？因此，就RSA安全强度而言，您可以使用一个非常复杂的公式来尝试接近或近似困难，事实上，奖励任何给定的。这是什么？好吧。这取决于市场的联系是如何类似于我们有。残酷的阶段是国家是一个熵群，我们可以说，作为RSA，这是健全的，就像我们这边是因式分解。我们基本上可以估计这会有多难。我们得到了一个激进的医学方程式。就这样了。努力是因式分解实际上是合格的。RSA安全公司表示，使用不是关于公众的首选。每次有人说系统实际上是安全的，你必须考虑到他们有五个版本，他们不能帮助人们，这是安全组数据。

And they basically said very fine. If you don't believe us, you will have a little bit of competition. You will give us a number of numbers for various sizes from rsa 129, or arsa 2038. We challenge anyone to try and factorize these numbers. Right? And they put out this competition in 1978. The first time that somebody was able to factorize rsa 125 was only 16 years later. Then. All right? And then rsa 155, we got a piece of the 512. But I should be characterized in 1999 576, characterized in 2000 three six hundred and forty was characterized in 2005.  
他们基本上都说很好。如果你不相信我们，你会有一点竞争。您将为我们提供来自RSA 129或ARSA 2038的各种大小的数字。我们要求任何人尝试分解这些数字。对的？他们在1978年举办了这个比赛。第一次有人能够分解RSA 125是在16年后。然后。好吧？然后是RSA 155，我们得到了512的一部分。但我应该在1999年表征576个，在2000年表征3640个，在2005年表征。

And then in 2007, I said, I think we made our point. All right, our system has not been secure for almost 27 years for a larger numbers that you should be using. Right? I think from now on it is not really a challenge anymore. This is simply writing for the quality to catch up as computing is faster. Basically, people back to us everything. All right. So after the price ended in 2007, people so managed to buy a price 768 and 704. Right? I think we have the numbers back on. There are a couple of systems today thats who were are as a or generally, people think that assistance need to be secure today. After 2030, you should be using rsi at least the p 5 and 48 to these are.  
然后在2007年，我说，我认为我们表达了我们的观点。好的，我们的系统已经有将近27年不安全了，因为你应该使用更大的数字。对的？我认为从现在开始，这不再是一个真正的挑战。这只是为了赶上计算速度更快的质量而编写的。基本上，人们把一切都还给我们。好吧。所以在2007年价格结束后，人们设法购买了价格为768和704的产品。对的？我想我们的数字恢复了。今天有几个系统，作为一个或一般，人们认为今天的援助需要是安全的。2030年以后，你应该使用RSI，至少是P5和48。

Okay. Everything is up to this interesting side discussion. What is the recommendation for sizes, for different types of group? The following was estimation by rsa labs. In 2003. They said for symmetric to be secure in the end of the year in 2010, you need an rsap size of 1,024. Similarly, is rather better to be secure for 2030. You need 112 % e right? In 2048 with our safety. If you have anything to go beyond 2,050, 138, and 3,000 72, this is rsas opinion. There are a lot of different opinions on this. All right? So is this opinion is, he says whose opinion is in his own opinion, is to be as our opinion, which is the german equivalent of us, is something to be academic studies on this. But if i've been done a little bit of this one in european union level, and it will come out of time, is that all of the keys need to be secure and how we should provide peace.  
好的。一切都取决于这个有趣的侧面讨论。对于不同类型的组，建议的大小是多少？以下是RSA实验室的估计。在2003年。他们说，为了让Symmetric在2010年年底变得安全，您需要1，0 24的RSAP大小。同样，在2030年也是安全的。你需要112%的E，对吗？2048年，我们的安全。如果您有任何超出2，050、138和3，00072的意见，这是RSAs的意见。对此有很多不同的看法。好吧？所以这个观点是，他说谁的观点是他自己的观点，就像我们的观点一样，这是德国人对我们的看法，是对这个问题的学术研究。但如果我已经在欧盟层面上做了一点，它将会随着时间的推移，那就是所有的关键都需要安全，以及我们应该如何提供和平。

And I really did I have this, you can do it yourself. It sure. I think these are as 80 sizes were quite accurate. A lot of people compare with these. Some people are a little bit more positive or negative about the symmetric besides. Some people say you already need 128 years today, and then we offer 2 thousand and fifty. You need a little bit longer. All right. As I said, it sounds different opinions about this. Everyone you can see from this and which is already very apparent is that how many people the key sizes are significantly larger than was an 80 people? I get to the equivalent table security otherwise, comparing good for searching of the entry key to characterization of rsa the size of this material that we use rsa significantly model, all for the others in a situation algorithms. Similar, you always eat very, very large number.  
我真的做了，我有这个，你可以自己做。它肯定。我认为这是因为80号的尺寸相当准确。很多人拿这些来比较。此外，有些人对对称的看法更积极或更消极。有些人说你今天已经需要128年了，然后我们提供了2500年。你需要更长的时间。好吧。正如我所说，这听起来有不同的看法。每个人都可以从这里看到，这已经很明显了，有多少人的关键尺寸比80人大得多？我得到了等价表的安全性，否则，比较好的搜索条目的关键字来表征RSA的大小，这就是我们使用RSA显著模型的材料，都是针对其他情况的算法。同样，你总是吃得非常非常多。

Then that presents with the analysis. You have to think that if you write code these days, most of the number of variables you use already are larger than 64 bits. You define a variable. Now I have to think that you are working with an offer that is 2,048 personal. That's a massive number you need. Very special number of libraries will offer you to implement. It is for all right. The other thing you can think about from a management district is the life of your data. So it's fine to say we wanted to start today. It has to be this long. But you really need to think about the data that you're interpreting and how long you want to be secure for. All right. If i'm suddenly interesting things today, but I want to leave it somewhere in the data store for the next 20 years, I should probably be using a longer key that i'm just doing some indications that are changing some data that i'm going to do by the individual.  
然后用分析来呈现。你必须考虑到，如果你现在写代码，你使用的大多数变量的数量已经大于64位。你定义一个变量。现在我不得不认为你正在与一个2，048个人的报价合作。这是你需要的一个巨大的数字。非常特殊数量的库将为您提供实现。这是为了所有的权利。你可以从管理区考虑的另一件事是你的数据的生命。所以说我们想从今天开始是可以的。一定要这么长。但你真的需要考虑你正在解释的数据，以及你想在多长时间内保持安全。好吧。如果我今天突然发现了有趣的东西，但我想在未来20年里把它留在数据存储中的某个地方，我可能应该使用一个更长的密钥，我只是在做一些指示，改变一些数据，我将由个人来做。

This, once again, feedback to how we think about security systems, what the threat is, what the capability of the factors going to be did. I factors would be able to do forces one hundred and eighties and 5 years from now. And I that would say 420 %, many years from now, maybe I would like to be 3 years old. So that means the future into the conversation will be from school data.  
这再一次反馈了我们对安全系统的看法，威胁是什么，因素的能力是什么。我的因素将能够做一百八十年代的力量，从现在起五年。我会说420%，很多年以后，也许我想要3岁。所以这意味着未来的对话将来自学校数据。

Okay, the next system living, there is alcohol, so the alcohol encryption scheme was small as a we choose a large p we have two states of numbers. Say, there. And then you must find, in terms of the notation, a is an element of s needs to choose a value, a random of cs right? And we also have the generator e to the one or pg to the one, pg to the minus one p is all equal. None of it is equal to one alcohol with a probability.  
好的，下一个系统，有酒精，所以酒精加密方案很小，我们选择一个大的p，我们有两个状态的数字。说，那里。然后你必须找到，根据符号，A是S的一个元素，需要选择一个值，一个随机的CS，对吗？我们也有生成元E到1或者PG到1，PG到负1，P都是相等的。它们都不等于一种酒精的概率。

Their priority is x rat is equal to x mod p sabg and p and y would be probably t it's would be a problem related arrest number r we go first part of the design of x a is equal to g to the r one p b is equal to the message times the probability rise to the random number one p he says two parts of the side of this a and b the degree we then say a is equal to a sh part of the party was ab the message is in b as the modular in this a module p we look at work example.  
他们的优先级是X，RAT等于X mod P，SABG和P，Y可能是T，这将是一个与逮捕数R有关的问题，我们首先设计X的一部分，A等于G到R，P B等于消息乘以概率上升到随机数1，P，他说这一边的两部分，A和B，然后我们说A是等于A SH的一方是AB，消息是在B中作为模块，在这个模块P中，我们看看工作的例子。

P is equal to 23 is equal to 11, is equal to six, intervals is ten. Random number is three. Probably the probability. Why is it in the 617, 20 3 is equal to 9? Incorrect. The first part of the scientific is even are three more than 23 is equal to 20, are 2 10 times on the message times. Probably he raised the rr plus the 23 is equal to 22. The bigger pay is equal to three to the six months of 2016. Message is equal to ￡22 and marginal emails of 16 marginally three is 0 to ￡22 30. I said I think the which is, okay, once again, I will give you a much more difficult example. You can go through it yourself. This part, we can calculate the ones that are inverse with the description. Hard to do that. This is the work example in the number of variation.  
P等于23，等于11，等于6，间隔是10。随机数是三。可能是概率。为什么在617，203等于9？不正确的。科学的第一部分是三个23以上的偶数等于20，是2的10倍，就是短信的倍数。可能他提高了RR加上23等于22。更高的工资相当于2016年六个月的三倍。邮件等于22英镑，16封边际电子邮件（边际3）等于0到2230英镑。我说我认为这是，好的，再一次，我会给你们一个更难的例子。你可以自己去看看。在这一部分，我们可以计算与描述相反的。很难做到。这是变异数中的工作示例。

There is one thing that we can discuss here. So you can probably see that if we look at the ball, it looks a little bit more complex in ourselves are saying that the one was there in this. If you do when you calculate to the private key from the public key, calculating the public private key relationship is what I need. You just need to do this situation. But if you need to know answering this, every time you do the description, right? That's it, I don't know, has a nice opportunity that people are really serious about theory. People prepare really nice.  
有一件事我们可以在这里讨论。所以你可能会看到，如果我们看这个球，它看起来有点复杂，我们说一个人在这里。如果你这样做，当你从公钥计算到私钥时，计算公钥和私钥的关系是我所需要的。你只需要在这种情况下做。但如果你需要知道答案，每次你做描述的时候，对吗？就是这样，我不知道，这是一个很好的机会，人们对理论非常认真。人们准备得很好。

So for us, a when we interpret the message, and the message says the same. In other words, we prove the same as it was. What happened to the size of x is it different? Or is it the same? If I group the same, like I if I group the same, it was what happens to this logic? It says the same, right? If my keys are the same, it says the same, because my only experiment says the same. And I probably want to listen to that. If I get you out of all, if I heard the same size, I if I heard the same thing is twice. It is designed to date the same, or it is designed to date different. They in deserve a year and save one. We choose a random number, right? Every time we heard we choose a new random number.  
所以对我们来说，当我们解释信息时，信息说的是一样的。换句话说，我们证明了它是一样的。X的大小发生了什么变化？有什么不同吗？还是一样的？如果我分组相同，就像如果我分组相同，这个逻辑会发生什么？上面说的是一样的，对吧？如果我的钥匙是一样的，它说一样，因为我唯一的实验说一样。我可能想听听。如果我把你全部弄出来，如果我听到同样的大小，我如果我听到同样的东西是两次。它被设计为日期相同，或者被设计为日期不同。他们应该得到一年的时间，并保存一年。我们随机选择一个数字，对吗？每次我们听到我们选择一个新的随机数。

If you read the number is utilized for calculating the first part of the subjects and the second part of the subjects, which means everything about the group, even if we could be the same right days, we end up with a different side of it. Right? Because some people quite like we might have a system where this is quite important. If you might send a lot of the messages that look the same are the same. And the actor is able to like you observe what you do, and you don't want to match the soccer base equation interaction. Right? What happens in the security of all the law? All right? People can be animal is from a which is g to the r mod e that africa needs are or from e to the ace of e which is why the africa is x or alternatively, the attacker from a and y is d to the ryd and d to the xyd they compute g to the rxy easily understand the disregard of the problems. And we know that those problems are like all. I should not be able to do that. And for the last one, this leads to the different order.  
如果你读到这个数字是用来计算第一部分科目和第二部分科目的，这意味着关于这个群体的一切，即使我们可以在相同的日子里，我们最终会得到不同的结果。对的？因为有些人很喜欢我们可能有一个系统，这是非常重要的。如果你可能发了很多看起来一样的信息，其实是一样的。演员能够像你一样观察你所做的事情，而你不想匹配足球基本方程的互动。对的？在所有法律的安全中发生了什么？好吧？人可以是动物，从A是G到非洲需要的R模E，或者从E到E的ACE，这就是为什么非洲是X，或者从A和Y的攻击者是D到RYD和D到XYD，他们计算G到RXY，很容易理解对问题的忽视。我们知道这些问题和所有问题一样。我应该做不到。对于最后一个，这导致了不同的顺序。

Then we will discuss a little bit later by some senate to be equivalent to the discrete model In terms of the discrete order of the product that we remind ourselves. Basically, if we have given d to a one p we can calculate why quite easily. But if we are given why in a we cannot calculate a very easy, right? This is similarly hard to the factorization problem. The reality is, if the modulus p is very large, they solving the discrete order of the problem would be very large. So in practice, pe today is larger than 1,003 workers long. Because I think it for this recovery, the problem, it's not context. Basically, an attacker needs to root for school exponents from zero to be - 1. The answer will be minus the easier, the more difficult it is. Right? This is another difficult problem. We said that one of the security issues or security options of all of us in the development problem. Development problem is that we have equal to x of p and d to yyd and we find e to the x bar of e if we can solve this, and then you can write parts of, once again, similar to the rsa for them, where people say about this, some different things that you can do, but it's pretty much a lot of accusation we could have discussed on the program.  
然后，我们稍后会通过一些参议院来讨论，根据我们提醒自己的产品的离散顺序，来等价于离散模型。基本上，如果我们把D给一个P，我们可以很容易地计算出为什么。但是如果我们给出为什么在A中，我们不能很容易地计算A，对吗？这与因式分解问题同样困难。事实是，如果模数p非常大，他们解决问题的离散阶将非常大。因此，在实践中，今天的PE大于1，003个工人的长度。因为我认为这次复苏的问题，不是背景。基本上，攻击者需要对学校指数从0到-1进行寻根。答案是负的，越容易，就越难。对的？这又是一个难题。我们说我们所有人在发展问题中的安全问题或安全选择之一。开发的问题是，我们有等于X的p和d到yyd，如果我们能解决这个问题，我们可以找到e到e的x栏，然后你可以再写一部分，类似于他们的RSA，人们对此说，你可以做一些不同的事情，但我们可以在程序中讨论很多指控。

I think, as he said, I decide a different problem.  
我认为，正如他所说，我决定一个不同的问题。

But at the end of the day, you still have to break the discreet over the whole. You either have to find y or you need to find x to be able to calculate this, you need to find x and then raise b to the rx you need to find y and raise a to the power of y is it all the problems are really different? On this remark system, we experience in the loss of religion stressed that if you have an algorithm for the development year, strange is slightly special.  
但在一天结束的时候，你仍然必须打破整体的谨慎。你要么找到y，要么找到X来计算这个，你需要找到X，然后把B提高到Rx，你需要找到y，然后把A提高到y的幂，所有的问题都是不同的吗？关于这个备注系统，我们在失教的经验中强调，如果你有一年的算法开发，奇怪的是略显特别。

We cannot use it to encrypt information rsa and probably we interpret this year. If it happen is a key exchange. So it's an exchange price of a symmetry proposed. The last alison ball to make a new share symmetry. What happens here is alice will choose a a choose a random value b alice will do you need a more piece in all of the g to the be what he said to us? What will get the g to a one p raise it to the power b that will be the g to the 81 p and alice with agp one p raise it to the power a and I will also give her g to the a or p now, at least of all, has the same value, g to the a or p they can use that as a basis of operating a new, symmetric. It's passive attacks. This is the 55, because we're an attacker about 80 to a one p they must either calculate b or a from this exchange.  
我们不能用它来加密信息RSA，可能我们今年会解释。如果发生，则是密钥交换。所以这是一个对称的交换价格。最后一个艾莉森球做了一个新的共享对称。这里发生的是Alice将选择A A选择一个随机值B Alice将你需要在所有的G中再加一块才能成为他对我们说的那样吗？什么会让G变成1，P，把它提升到B次方，这将是G到81，P的幂，爱丽丝用AGP，1，P，把它提升到A次方，我也会给她G到A或P现在，至少，有相同的值，G到A或P，他们可以用它作为操作一个新的，对称的基础。是被动攻击。这是55，因为我们是一个攻击者，大约80比1 P，他们必须从这个交换中计算B或A。

In other words, they are solving the problem, which is equal to this part of the problem effort, right? To be able to calculate besides either if government has problems with active attack, so passive attack is equal to listen. They see these two messages and they want to find the secret key. The development is vulnerable to active attack, especially matters of attack. What happens in the manner of the attack? Alice wants to look at. All of said alice is deeply able to be people, a team to the table. He is wrapped by treaty with a response to g to the team or b that is alice. This is only the ball. She actually agrees a new key g to the 80 more p with judy. Right? Or it's amazing from who he thinks is alice, who is actually three d all right? He says g to the b or t back, that means he agrees on a deal of three d that is g to the bd or b I ever said the key g to the at and what has a key to the g to the bt I just think she's going to grow up, involved in.  
换句话说，他们在解决问题，等于这部分问题努力，对吧？此外，如果政府主动攻击有问题，那么被动攻击就等于倾听。他们看到这两条信息，他们想找到密钥。开发容易受到主动攻击，尤其是攻击事件。攻击的方式是什么？爱丽丝想看看。所有的人都说爱丽丝很有能力成为一个人，一个团队到桌子上。他被条约包裹着，对团队G或B的回应是爱丽丝。这只是球。她实际上同意了朱迪的80多个P的新密钥G。对的？或者他认为谁是爱丽丝，谁实际上是三个D，这很令人惊讶，好吗？他说G对B或T回，这意味着他同意三个D的交易，即G对BD或B，我曾经说过关键的G对AT和关键的G对BT，我只是觉得她会长大，参与其中。

She's talking to us, but in reality, most of them are talking to judy.  
她在和我们说话，但实际上，大多数人都在和朱迪说话。

I I really exists, right? So alice with a group missing to the wall, three will take it read and send it all re interpreted with the king of all. What will have a response to alice? What was in the back? Because the gvd reading a paper really like it really can change it. And then basically send a new message encrypted with d to the ad backgrounds.  
我我真的存在，对吧？于是爱丽丝带着一群人走到墙边，三个人将这一切读完并送回与国王一起重新解释。什么会对爱丽丝有反应？后面是什么？因为GVD读一篇论文真的很喜欢它，真的可以改变它。然后基本上向广告后台发送一条用D加密的新消息。

Basically, I will and the only way to solve this, if I think you could add data or is an indication to the business, right? So very much I don't want to look at and a good security. We will see that a lot of practical or actual systems use if they were, but they all add the origin of information remains to from the. In other words, you have to take this message is possible, and this message is not for us.  
基本上，我会和唯一的方法来解决这个问题，如果我认为你可以添加数据，或者是对业务的指示，对吗？所以我非常不想看和一个好的安全。我们会看到很多实际或实际的系统使用，如果它们是，但它们都添加了信息的来源仍然来自。换句话说，你必须接受这个消息是可能的，而这个消息不是给我们的。

All right? So in conclusion, symmetry versus publicly proposed.  
好吧？总之，对称与公开提议。

So it's an entry photography. Alice involved should trust each other because they all the same city. If I have it is dishonest and shares it with everyone else, then this is the right the first party seems to be honest, keep the secret. He probably take a progress, leave. The communicating parties did not trust each other, because this is the ball as public private key there. What is the early person that has his private key? And he should trust himself to keep this here.  
所以这是入门摄影。爱丽丝应该互相信任，因为他们都在同一个城市。如果我拥有它是不诚实的，并与其他所有人分享它，那么这是正确的，第一方似乎是诚实的，保守秘密。他可能进步了，离开了。通信双方互不信任，因为这是作为公私钥存在的球。最早拥有自己私钥的人是谁？他应该相信自己能把这个留在这里。

All right? We need this public key to, that's not matter. Right? The major key, both the keys for the sender and receiver is the same probability. There are two single keys. The public key for the sender, the private key of the severe. Another symmetric key security. If this offer is good, the best approach is good for research. Probably the best approach is basically solving these mathematical long way functions. I did a discrete organism problem, or the factorization model. In terms of encryption, symmetric key encryption is faster. That's why whenever we want to really a lot of data, we want to use symmetric encryption. That's why in practice, in other systems, the key management is most likely that probably he could go. Your actual ball encryption is always on the symmetric encryption. The reason for that is because probably is much slower, because probably the security relies on the size of the numbers and also inherent your exponentiation explanation. Despite how wonderful the square multiply other than is the other day that is the chinese reminder there, but I think those things are so much lower than just running for people for years.  
好吧？我们需要这个公钥，这不重要。对的？主密钥，发送方和接收方的密钥是相同的概率。有两个单键。发送方的公钥，严害方的私钥。另一个对称密钥安全性。如果这个提议是好的，最好的方法是有利于研究。也许最好的方法基本上是解决这些数学长程函数。我做了一个离散有机体问题，或者因式分解模型。在加密方面，对称密钥加密速度更快。这就是为什么每当我们需要大量数据时，我们都要使用对称加密。这就是为什么在实践中，在其他系统中，密钥管理最有可能是他可以去。你的实际球加密总是在对称加密上。这是因为可能要慢得多，因为安全性可能依赖于数字的大小，也依赖于你的指数解释。尽管前几天的平方乘法是多么美妙，这是中国人的提醒，但我认为这些东西比人们多年来的跑步要低得多。

I started this is extremely large because the larger they stories are the most secure. This is all right. So probably I question is relatively inefficient, much. So you don't want to be involved encryption. The matrix sizes are much smaller, right? To be secure. And so the public key prepare, we need to choose our keys to be part lost. And some examples it is. It is 4067 to finish variations for is index for public key rsa all the more people stuff. It's all example, the public key.  
我开始这是非常大的，因为更大的故事是最安全的。这样就可以了。所以可能我的问题是效率比较低，多。所以你不想参与加密。矩阵的尺寸要小得多，对吧？为了安全。所以公钥准备好了，我们需要选择我们的密钥来部分丢失。还有一些例子。它是4067来完成公钥RSA的IS索引的变化，所有更多的人的东西。这都是例子，公钥。

One last night before we are just related to some impractical, are any of you have a quantum computing? Probably. Have you heard about quantum computing and security? Have you heard that people say if one of the computers happen, it will basically write encryption algorithms. Anyone heard that before? All? Right. So is that true? Or isn't that true? It is partly true. The thing was part of computing. She said, if they get it to work, there is an algorithm that is shown to be able to run quantum computing with school scores algorithm. As short algorithm is able to do factorization. And the street marker problem solving extremely efficiently. All right. The implications for is that it will probably break asymmetric encryption as we are in the because things like rsa and development relies on the street border and all of the characterization problem to be hard. If we suddenly have computing systems that solve that problem very easily, then you have a problem. That's it. If I make my quantum computing, solve, a is brute force research. It is still gonna be equally bad as my article future.  
前一晚我们只是涉及到一些不切实际的东西，你们中有谁拥有量子计算吗？大概。你听说过量子计算和安全吗？你有没有听说过人们说，如果其中一台计算机发生了，它基本上会编写加密算法。有人听说过吗？所有？对的。那是真的吗？这难道不是真的吗？这是部分正确的。这是计算机的一部分。她说，如果他们让它工作，有一种算法被证明能够运行量子计算与学校分数算法。因为Short算法能够进行因式分解。以及非常有效地解决街道标记问题。好吧。的含义是，它可能会打破非对称加密，因为像RSA这样的东西和开发依赖于街道边界，所有的表征问题都很难。如果我们突然有了计算系统，可以很容易地解决这个问题，那么你就有问题了。就这样了。如果我把我的量子计算，解决，一个是蛮力研究。它仍然会和我未来的文章一样糟糕。

All right. In other words, when people talk about this one to propose or adapting crypto, it would be resistant to quantum computing. It must be realized the case of a different finding new methods for isolated photography that would be able to lost, even if people wrote partial of computers. The entry group ship was over, you must be fine. And so that everything else is going to be in this competition, going on the proposed. There are a lot of different candidates, because for asymmetric encryption, encryption asked me everything we do in the curve. But for isometric, is responsible for exchange, is responsible for encryption, as all responsible for the digital signature, as we'll see. The meeting today, there's a number of different candidates that are considering some for providing digital energy services, an example, providing the exchange encryption services.  
好吧。换句话说，当人们谈论这个来提出或适应加密时，它会抵制量子计算。必须认识到，在不同的情况下，为孤立的摄影寻找新的方法，即使人们编写了部分计算机，也会丢失。入境小组船结束了，你一定很好。所以其他的一切都将在这场比赛中进行，继续进行。有很多不同的候选者，因为对于非对称加密，加密要求我们在曲线中做的所有事情。但是对于Isometric，它负责交换，负责加密，负责数字签名，正如我们将看到的。在今天的会议上，有许多不同的候选人正在考虑提供数字能源服务，例如，提供交换加密服务。

And those are, once again, vote on ap hard problems, like characterization, discrete algorithm problems. While on that is supposed to propose all those, they are not vulnerable to be easily solved by other people or foundation order. So basically is changing the heart problems. That is the best part. So that is the interesting thing. Okay? Right? So that is the in population. As every I will put the notes for these issues on campus. After the tutorial was included, before the solutions there, right now, we can solve, and we can then, at the long right, you can look on your provisions. And as I say, would you say in this room, if you want to say for the authority, you can say when I leave, and these are means of it. And you believe the problem and you want to immediate or any holiday survive, you are the same way in the world and you can say and everybody that wants to do the work that I can stay here, and we'll just do one procession. Okay, thank you.  
再一次，这些是对AP困难问题的投票，比如特征描述，离散算法问题。虽然在这一点上应该提出所有这些，但它们不容易被其他人或基金会的命令轻易解决。所以基本上是改变心脏问题。这是最好的部分。这就是有趣的事情。好的？对的？这就是人口。每个人我都会把这些问题的笔记放在校园里。在教程被包括之后，在那里的解决方案之前，现在，我们可以解决，然后我们可以，在右边，你可以看看你的规定。正如我所说的，你能在这个房间里说，如果你想为当局说话，你可以在我离开的时候说，这些都是它的手段。你相信这个问题，你想立即或任何假期生存，你在世界上是一样的，你可以说，每个人都想做这项工作，我可以留在这里，我们只做一个游行。好的，谢谢。