### Security\_week5\_lec1数论基础-20240929

说话人1 00:00  
Just before we start with casualties and financial welcome announcement, canvas, it is remind you problems that one is available on campus. It's been on there for some time. Please remember to take a look at that. And the define is the repeat of over at 2 o'clock. The other thing I want to try today, so i'm only gonna try today, and then i'll the questionnaire and is how we can do it going forward. But we were supposed to have two tutorial classes about the four classes of the poor. The other one starts at five. But it seems like this one is very popular in many people got to that one. Then the second one is not so popular and very few people come to that one. So thats okay. I'm happy doing both. It's fine. Maybe a few people that come to the second one really also come to the first one. So for today, because it's sunday, and maybe you can decide I only want to have one class.  
就在我们开始伤亡和财务欢迎公告之前，画布，它是提醒你的问题，一个是在校园里。它已经在那里有一段时间了。请记得看一下那个。定义是在2点钟方向上的重复。我今天想尝试的另一件事，所以我今天只想试一试，然后我会做问卷，然后我们如何继续做下去。但我们本来要上两节关于穷人四个班的辅导课。另一个在五点开始。但似乎这个很受欢迎，很多人都喜欢那个。然后第二个就不那么受欢迎了，很少有人来。所以没关系。我很高兴两件事都做。它很好。也许有几个来第二个的人真的也来了第一个。所以今天，因为是星期天，也许你可以决定我只想上一节课。

So I think this classroom is as if you if we just have the tutorial in this classroom, after the lecture is and anyone that wants to do tutorial today, whether you are registered for a class or registered for 5 o'clock class, you can just read tutorial at 4 o'clock.  
所以我认为这个教室就像我们在这个教室里上辅导课一样，在讲座结束后，今天任何想上辅导课的人，不管你是注册了一节课还是注册了5点钟的课，你都可以在4点钟的时候读辅导课。

And afterwards on campus, i'll ask some opinion about this. If this is a more popular way going forward, and it's quite a few students, you don't want to wait an hour before I the second one or the first group of students that are having a for the exercise student.  
然后在校园里，我会问一些关于这方面的意见。如果这是一种更受欢迎的方式，并且有相当多的学生，你不想在第二组或第一组学生之前等待一个小时，他们正在为学生做练习。

And I can ask the university, we can just have one for your class. I'm very bored, but i'll discuss them with you later all the time today. And I would like opinion, hold on campus and you can tell me what you see about this going forwards. Okay? Right. Last week we finish the major incursion. I put some extra readings or some extra things that you could look at on there, give you a little bit of indication about how you might use chp encryption in the real world.  
我可以问大学，我们可以只为你的班级准备一个。我很无聊，但我今天会一直和你讨论这些问题。我想在校园里发表意见，你可以告诉我你对未来的看法。好的？对的。上周我们完成了主要的入侵行动。我把一些额外的读数或一些额外的东西放在那里，你可以看看，给你一些关于如何在现实世界中使用CHP加密的指示。

I said that if you want, you can look at the emp codes dissertation. So the emb cosification is quite famous, because it's basically a consortium or a group of six nurse. Mastercard is a basically union, a american express in the summer. And what they do is they maintain payment card standard for anyone pays with any of these cards, whether it is with an actual card, whether it is with your mobile, whether it is online. Basically, they determine how things are going to work in terms of paying with that card. Specifically, the standards that we want to look at is for paying with you actual credit card. Right? So in terms of actual physical part conception, right? Basically works worldwide and basically does more than 90 % of the worldwide transactions for credit card payments. All right. Everyone is up to 99 % in most parts of the world, except for asia and for the us all right.  
我说，如果你愿意，你可以看看电磁脉冲代码论文。所以EMB联盟是非常有名的，因为它基本上是一个联盟或一个由六名护士组成的小组。万事达卡基本上是一个联盟，是夏天的美国运通。他们所做的是维护支付卡标准，任何人都可以使用这些卡进行支付，无论是使用实际的卡，还是使用手机，还是在线支付。基本上，他们决定如何使用该卡进行支付。具体来说，我们要看的标准是用你的实际信用卡支付。对的？所以在实际的物理部分概念方面，对吧？基本上在全球范围内工作，基本上完成了全球90%以上的信用卡支付交易。好吧。在世界大部分地区，每个人都达到了99%，除了亚洲和美国。

So I think in asia, the explanation for that is that some places have so use the magnetic stripe on the card, right? But also other types of agencies quite popular. Many people like you are all sorts of other things. The motivation to really not change the way they use credit cards is maybe a bit slower than other places. There are some other alternatives that may be also good. The united states, it was referred to activate the slide, because they're always historically preferred online transaction. Online transaction means when I pay, the merchant is online, you can once I phone my bank, immediately, the payment terminal can find off the bank and say this is I have money. And then the bank would approve the transaction. But very slowly, they're also very fast at adopting regard with the actual pro and the chip on it. Because the strength of that is that you can actually approve offline transactions.  
所以我认为在亚洲，对此的解释是一些地方使用卡上的磁条，对吗？但其他类型的代理也很受欢迎。很多像你这样的人都是各种各样的人。真正不改变他们使用信用卡的方式的动机可能比其他地方慢一点。还有一些其他的选择，可能也不错。在美国，它是指激活幻灯片，因为他们总是在历史上首选的在线交易。在线交易意味着当我付款时，商家是在线的，你可以一旦我打电话给我的银行，马上，支付终端就可以找到银行，并说这是我有钱。然后银行会批准这笔交易。但非常缓慢，他们也非常迅速地接受了实际的专业人士和它的芯片。因为它的优势在于您可以实际批准离线交易。

You have to say maybe many years ago, somebody comes in with these credit card. Most people are paying cash. You have the time for your system to dial up on the bank, make a transaction, approve it as a head. He says, you have like lots of people coming. You want also sales volume. You don't want to create every single time because it costs it's a safer car. And the machine can just themselves aside offline, whether the payment should receive it up. That is pretty good. Ok that's what enp does. Env does for env as if you could look, if you want the env version, or if you go through, so who specifies the crypto for car payment?  
你不得不说，也许很多年前，有人带着这些信用卡进来。大多数人都付现金。你有时间让你的系统拨号到银行，进行交易，作为负责人批准它。他说，你有很多人来。你还想要销量。你不想每一次都创造，因为它是一辆更安全的车。而机器则可以只把自己放在一边下线，是否该收钱就收起来。这是相当不错的。好的，这就是ENP所做的。如果你想要ENV版本，或者如果你通过，那么谁来指定汽车支付的密码？

All right. And if you actually look at the book is very long, a couple of 100 pages. So just remind yourself of of everyone, when you talk about standards and women are, sorry, industry standards. You can remember that I said in some cases, some of these specifications are very complicated, right? At the same time, they give you a lot of options.  
好吧。如果你仔细看，这本书很长，有100页。所以，当你谈论标准时，请提醒你自己，女性是行业标准。你记得我说过在某些情况下，这些规范中的一些是非常复杂的，对吗？同时，他们也给了你很多选择。

So if you look for it and you look for symmetry prefer, you will see that you have an option of using 2 types of photography. You can either use this in the two key triple a series of people to our last week. Or you can use a is about twenty eight nine two or two fifty six thirty, right? Or adding, you had everything with zero so that you may see it will be a multiple of the block size of the cyber.  
因此，如果你寻找它，你寻找对称偏好，你会看到你可以选择使用2种类型的摄影。你可以用这两个关键的三A系列的人来我们的最后一周。或者你可以用大约2892或25630，对吗？或者加上，你所有的东西都是零，所以你可以看到它将是网络的块大小的倍数。

I think you can use ecd or cbc mode. Remember, when we talked about los angeles, is it important? Every loss address? How much is it small size? How many bits are gonna be created online? And what is this e source? Right? So I say is the one create a good book. What i'm going to add 190 to fifty six fifteen. And for days, we had a fifty six thirty. If you see all the law. So if you are given the choice between ds and as I hope that you would use aes because it's in either one and it's a bigger one. Right? If you had a choice between ecb and cbc mode, I hope that you could recognize that you used to use cbc mode. I remember that picture. We have alice, and then the encrypted error with ecb and the encrypted error with cbc and then we had a picture of alice with ecb mode.  
我认为你可以使用ECD或CBC模式。记住，当我们谈到洛杉矶时，这很重要吗？每个丢失地址？小号的多少钱？有多少比特是在线创建的？这个E源是什么？对的？所以我说是创造一本好书的人。我要把190加到5615。几天来，我们都是5630。如果你看到所有的法律。所以如果你在DS和AS之间选择，我希望你会使用AES，因为它在任何一个中，而且它是一个更大的。对的？如果您可以在ECB和CBC模式之间进行选择，我希望您能够认识到您曾经使用过CBC模式。我记得那张照片。我们有爱丽丝，然后是ECB的加密错误和CBC的加密错误，然后我们有一张爱丽丝在ECB模式下的照片。

And so see, most of us, the cbc was he was completely hit.  
所以，我们大多数人，加拿大广播公司是他完全被击中了。

If you remember that picture, you should know that cbc mode is better than ec because the strength of cbc is that the current subjects that you've made it depends on the current plane takes, the whole other plane takes that upon before that as well. Right? So that is a little bit of extra reading if you want to do that. So did I were actually doing two lectures? We split it up into two, but it's two very short pictures. Actually. Three is not the theory or a little bit of background on the theory.  
如果你还记得那张照片，你应该知道CBC模式比EC模式更好，因为CBC模式的优势在于，你所做的当前主题取决于当前飞机的拍摄，整个其他飞机也在此之前拍摄。对的？所以如果你想这样做的话，这是一些额外的阅读。所以我实际上是在做两个讲座吗？我们把它一分为二，但这是两张很短的照片。其实。三是没有理论或有点背景的理论。

Then before you think about on the theory too much, and you think this is an ass force, immediately go to a symmetric refer for which we will use another theory, right?  
然后在你考虑太多的理论之前，你认为这是一个驴力，立即去一个对称的参考，我们将使用另一个理论，对吗？

It's on earth. I would say that the dominant theory lecture is not supposed to. We are in this study on the theory, and also a simple problem set one. When i'm asking me some numbers is another equation to encourage you to study how it works. I will not give you another theory questions in the exam or in the woods. What I will give you is i'll give you is the matrix encryption questions. I'll say, can you do rsa and give you alcohol? Can you do it at the moment? For to do that? You need to apply some number here. Right? But you really need to solve any difficult number theory. Questions of the number theory proofs, or anything like that. So I will summarize it again. What the core knowledge is. What do we need to know about number theory before we go to the asymmetric impression? The previous article, we talked about symmetric encryption. We started with really old, i'm suffers most of the time people use substitutions suffers substitution. Doctors have the limitation of the underlying disease of the plaintiffs.  
它在地球上。我想说的是，主导理论讲座不应该。我们在这个研究上的理论，也是一个简单的问题集一。当我问我一些数字时，是另一个鼓励你学习它是如何工作的等式。我不会在考试中或在树林里再给你一道理论题。我要给你们的是矩阵加密问题。我会说，你能做RSA并给你酒精吗？你现在能做吗？为了做那件事？你需要在这里申请一些数字。对的？但你真的需要解决任何困难的数论。数论证明之类的问题。所以我再总结一下。核心知识是什么。在我们进入不对称印象之前，我们需要知道关于数论的什么？在上一篇文章中，我们讨论了对称加密。我们开始的时候真的很老，我很痛苦，大多数时候人们都在使用替代品。医生有原告基础疾病的限制。

Also came through into the cyber text, and people wrote it with frequency analysis. And he was sort of taking five differently about security. They developed the subset. One time had people signing one time back from various theoretical aspects. From communication theory, information theory, they realized it was pretty good, but they also realized that it wasn't really practical. Therefore, if they started rolling speed cyphers, it was a practical version of the one time pad. It didn't have the perfectly secure property, but it was actually practical. And then later, modern day, symmetric encryption moving philosophers. We look at this with the variations of this. Variations of is as if I cover for the fact that is the size as usual, then we move on to as which is the symmetric infrastructure that we use that.  
也进入了网络文本，人们用频率分析来写它。他在安全方面采取了五种不同的做法。他们开发了子集。有一次，人们从不同的理论方面签了一次。从通信理论，信息理论，他们意识到这很好，但他们也意识到这并不实用。因此，如果他们开始滚动速度密码，这是一个实用版本的一次性垫。它没有完全安全的属性，但它实际上是实用的。后来，在现代，对称加密感动了哲学家们。我们用这个的变体来看这个。IS的变化就像我涵盖了通常的大小，然后我们继续讨论AS，这是我们使用的对称基础设施。

Finally, we ended with modes of operation, which is how we use more service to encourage messages that are more than one more, and we really discuss area population. In other words, what happens if some of the message is corrupted? Some of the message is lost? And how much of the main text message is it affected by the error? The extra we gonna do, we gonna talk about the background of the mathematics we need to do, probably the cryptography, and then also taking some looks at some number of theory essays, this nature, other side of five properties, the design of security mechanisms in terms of the underlying design of public equipment.  
最后，我们以操作模式结束，这是我们如何使用更多的服务来鼓励更多的信息，我们真正讨论了区域人口。换句话说，如果某些消息被损坏，会发生什么情况？有些信息丢失了。有多少主要文本消息受到错误的影响？我们要做的额外工作，我们会讨论我们需要做的数学背景，可能是密码学，然后也会看一些理论论文，这个性质，五个属性的另一面，在公共设备的底层设计方面的安全机制的设计。

So why is the number here? All right. Without getting too much into what on the theory is, it sure it's a roster mathematics that knows if you are working with ets now the theory was only the integers are number 123467, and the negatives. All right? So it is obvious. We can discuss about adviser. We have two integers, a and b and b divided into a exactly. Then we can say that b is a divisor of a it also means that there is some other integer and that you can multiply by b it was because the result especially be divided to a in class and innovation for that is a single life.  
那为什么数字在这里？好吧。在没有太多理论的情况下，它肯定是一个花名册数学，如果你现在和ETS一起工作，理论只是整数123467和负数。好吧？所以很明显。我们可以讨论一下顾问的事。我们有两个整数，a和B，并且B被a整除。然后我们可以说B是A的除数，这也意味着还有其他整数，你可以乘以B，因为结果特别是在类和创新中被除以A，因为这是一个单一的生命。

B is advisor, ok so if we have the number 20 3123468, 12, 24, all the wives, 80, 24, right? Some basic properties of devices. If b is a divisor of one, then he must be + - 1. If b is a divisor of a but a is also a divisor of b and b must be plus minus a anything can be divisor zero. He said zero because you cannot divide by zero. Then finally, if he can divide into g and he can divide into h if you can also divide into any linear combination of g and h we can multiply g by any integer. We can multiply ah by any, in terms we added together. We will divide into that answer.  
B是顾问，好的，如果我们有数字203123468，12，24，所有的妻子，80，24，对吗？器件的一些基本特性。如果B是1的除数，那么他一定是+-1。如果B是A的除数，但A也是B的除数，并且B必须是正负A，则任何东西都可以是除数零。他说零是因为你不能被零除尽。最后，如果他能分成G和H，如果你也能分成G和H的任何线性组合，我们可以将G乘以任何整数。我们可以把AH乘以Any，把它们加在一起。我们将分成几个答案。

The next concept is on groups. Essentially, a is congruent to b a is not going to be much again. If n is advisor of a minus b congress is innovation that we use in modular reduction, because we have these equal, because we're already say a mod n is equal to p mod n because a is not really equal to p but some are very good.  
下一个概念是关于组的。本质上，A和B是全等的，A不会再多了。如果N是A的顾问减去B，Congress是我们在模约简中使用的创新，因为我们有这些相等的，因为我们已经说过A mod N等于P mod N因为A并不真正等于P，但有些是非常好的。

He said they are on. Good. That's it. If you're doing some of the theory question, and you should really be using the conference sign that you get confused, use the equal sign. For this course, at all matter, I make that same mistake sometimes.  
他说他们开始了。好。就这样了。如果你在做一些理论题，你应该使用会议符号，你会感到困惑，使用等号。当然，无论如何，我有时也会犯同样错误。

All right. The early discussion about it is daily know what the concept of goods is. 23, modular five is congruent to a modular five, because five is a divisor of the e bd minus a - 11, modular eight hundred and five hundred eight, because 8 and divided to 5, 16. And 81 has been given to 0 or 35 with 87 supervisor of 81. If a is compared to b it also implies that he is concluded a and if a is concluded b and c is compared to be the a and c are also operate. All right. We saw the modular. What does the modular mean? So the modular, that's one of the reduction. So usually we're looking for something in the format of a or in is equal to a remainder or a residue, right? Basically, we can also write it as a is equal to qn plus r a is something is equal to some portion integer. I multiplied by n plus the remainder. The right there must be larger or equal to zero, and it must be smaller than a right?  
好吧。关于它的早期讨论是每天都知道商品的概念是什么。23，模5与模5全等，因为5是E BD减去A的除数-11，模800和500 8，因为8被除为5，16。81已被赋予0或35，其中81的监督者为87。如果将A与B进行比较，这也意味着他被断定为A，并且如果A被断定为B，则将C与A进行比较，A和C也被操作。好吧。我们看到了模块化。模块化是什么意思？所以模块化，这是减少的一部分。所以通常我们要找的是A或In等于余数或余数的格式，对吧？基本上，我们也可以把它写成A等于Qn加上R，A等于某个部分整数。I乘以n再加上余数。这里的右必须大于或等于零，并且它必须小于右。

And I think your question is the largest integer below a divided by n If we look at eighteen one two nine seven, what is the remainder? Or so quite easy, what is the question? Two, 18 is 2 × 7 + 4. Your question is two, and you remain. There is four. The second one is quite easy. My period of this political party equation, if you were right, there would be one. It's an odd number and degree modularity. Right? In terms of the relation between modular reduction and congress, I think it has the same remainder as the same modulus in the same reminder that there will be concrete. - 12 is hundred, - 5 is a grade, two is a grade. Is it for a negative number, if we have - 2 more to receive, it is equal to two.  
我认为你的问题是A下面的最大整数除以n，如果我们看181297，余数是多少？或者很简单，问题是什么？二，18是2×7+4。你的问题是两个，你留下。有四个。第二个很容易。在我的政党方程式时期，如果你是对的，就会有一个。这是一个奇数和程度模块化。对的？就模数减少和国会之间的关系而言，我认为它有相同的余数，因为相同的模数在相同的提醒下，会有混凝土。-12是100，-5是一个等级，2是一个等级。是不是对于一个负数，如果我们有-2多收，就等于二。

There is two. What is the quotient, in this case? Minus two. Basically, minus r is equal to qn plus r which is equal to minus two times seven plus two ok the interesting thing we can think about our delivery of the day is that sometimes when we have a large number or many operations, we can use the modular reduction at any .. Right? I understand this is a bit. It's nice to come here. So you have a plus b as supposed to be a bracket. If you have a bus being watched again, you can either add ab together and get a larger number, and you can watch the reduction. Or you can first do the marginal reduction, a the margin of the reduction, only of the added two reductions together.  
有两个。在这种情况下，商是什么？减二。基本上，负R等于Qn加R，等于负2乘以7加2。好的，我们可以考虑一件有趣的事情，关于我们当天的交付，有时当我们有一个很大的数字或很多操作时，我们可以在任何地方使用模约简。对的？我知道这有点。很高兴来到这里。所以A加B应该是一个括号。如果你有一辆公共汽车再次被监视，你可以把AB加在一起，得到一个更大的数字，你可以监视减少。或者你可以先做边际减少，减少的边际，只是两个减少加在一起。

Then finally, you want to the end of that song. If you have 97 + 20 3107, you can add 97 to 23 to give you 120, and then do the water reduction. Alternatively, you can do the modular reduction of 97 first, which is six. You can do the larger reduction of anything, which is two. I give you 6 + 2, and then you do the modular reduction, seven. And that gives you one. So it's simplified for you the way you can do exactly the same thing with negative number or. And suppression, they can say, 11, 183, forty one eighty six, b minus 6108 is minus minus d 108, which is equal to five, right? That is useful, but this is actually not going to be multiple, because multiply will give you much larger numbers.  
最后，你想听完那首歌。如果你有97+20 3107，你可以把97加到23上，给你120，然后做减水。或者，您可以先对97进行模数缩减，也就是6。你可以做任何事情的更大的减少，也就是两个。我给你6+2，然后你做模约简，7。这就给了你一个。所以这对你来说很简单，你可以用负数或来做同样的事情。抑制，他们可以说，11，183，4186，B减去6108等于-D 108，等于5，对吗？这是有用的，但这实际上不会是倍数，因为乘法会给你更大的数字。

Absolutely. You can do the same thing with occupation. You can like 11 and multiply by 14 and then write it with your reduction where you can also just do the reduction of 12st, which is to be, you can take the reduction of 14, modular eight, which is six. You have 3 × 6, which is 18, 508, which is also equal. You can simplify things quite easily by reading the modular reduction at different people, considering the problem, a larger problem, it is smaller parts. Okay? In other theory, we often talk about two parts of numbers. There are prime numbers and opposite numbers. A prime number is a number that is divided by one and itself. Right? And nothing else. We look at 3357. And in fact, any of these numbers here, you will see that they divide by the number except one and themselves. If the number is not the prime number, it is a opposite number. Right? In terms of opposite numbers, every single opposite number and factorize into a sequence or a product of prime numbers. Any opposite number can be basically a prime number to an experiment on the prime number, to an exponent on the prime number of these I remaining prime numbers unique.  
绝对地。你可以对职业做同样的事情。你可以用11乘以14，然后写出你的约简，你也可以只做12的约简，这是，你可以取14的约简，模8，也就是6。你有3×6，也就是18，508，也是相等的。你可以很容易地通过阅读不同人的模块简化来简化事情，考虑到这个问题，一个更大的问题，它是更小的部分。好的？在其他理论中，我们经常谈论两部分数字。有质数和相反数。质数是被1和它本身整除的数。对的？别的什么都没有。我们看3357。事实上，这些数字中的任何一个，你都会看到它们被除以1和它们自己。如果这个数不是质数，它就是相反数。对的？就相反数而言，每一个相反数和因式分解为一个素数序列或素数乘积。任何相反数基本上都可以是素数，可以是素数上的实验，可以是这I个剩余素数的素数上唯一的指数。

For example, if we look at 12,000, 250 as opposite number, and that could be represented by sevens with as far as the r three as two.  
例如，如果我们看12，000，250作为相反数，这可以用7来表示，直到R 3等于2。

So 257 are all five numbers. We want to have a very basic way to do it on a piece of paper. Usually we take the composite number and divided by the smallest prime, and we see how many times that time can provide exactly into that number. Right?  
所以257都是五个数字。我们希望在一张纸上有一个非常基本的方法。通常我们取合数，然后除以最小的素数，然后我们看看这个时间可以精确地提供多少次。对的？

So actually, in 4013 50, it could revive anyone's. And then we take the result, and we try divided by the next number three. We should actually have another five y and then you take the next one, which is five, and you realize that you can we can divide by 53 times. You're not yet at one. So we can say five to the three behind divide by five, the 4th time. So we go to the 7th. We see that by now we have hundred and twenty one ÷ 7 to give us. You have, sorry, we can drive by 17 or 7 and we can drive by 1745 again. So that means we have cities with us 5 to 53 × 2. That's quite a natural way of doing it. It looks like all the small numbers are not very well for large numbers. Right? And that gives us the next ., doing this characterization for very high numbers or smaller numbers is very easy, right? Quite easy to talk that. I heard the larger the number becomes, the larger it is more difficult departments.  
所以实际上，在401350年，它可以让任何人复活。然后我们把结果除以下一个数字3。我们实际上应该有另外5个y，然后你取下一个，也就是5，你意识到你可以我们可以除以53。你还不到一岁。所以我们可以说五除以后面的三，第四次。所以我们去7号。我们看到，到现在为止，我们有一百二十一点七给我们。你有，对不起，我们可以开到17或7，我们可以再开到1745。所以这意味着我们有5到53×2的城市。这是一种很自然的做法。看起来所有的小数字都不适合大数字。对的？这给了我们下一个。，对非常大的数字或更小的数字进行这种表征是非常容易的，对吧？说起来很容易。我听说数字越大，部门就越困难。

In fact, for us, this is quite important. We will come back to this, either would be talking about, probably prefer, but it's probably preferred, is based on typical mathematical problems. We'll see later than one of these problems is prime factorization. One of the things that we want to do for a symmetric, is it calculate something for the modular inverse?  
事实上，对我们来说，这是相当重要的。我们将回到这个问题，或者讨论，可能更喜欢，但它可能更喜欢，是基于典型的数学问题。我们稍后会看到，其中一个问题是素因子分解。我们要做的其中一件事，就是计算一个对称矩阵的模逆？

We need a way to do that. We'll talk about the modular in the short is talking. But the first part of our connecting the ones that are in this is basically to calculate the greatest model advisor between few numbers. The greatest common divisor is the largest integer. It can be an advisor of the two divided numbers. For example, for 60 and 24, the largest number that divides into bars is twelve o k if the largest number that divides into the two given numbers is one, they are relatively prime. Relatively prime is different prime.  
我们需要一种方法来做到这一点。我们将在简短的谈话中讨论模块化。但我们连接这些的第一部分基本上是计算几个数字之间的最大模型顾问。最大公约数是最大的整数。它可以是两个除数的顾问。例如，对于60和24，划分为条的最大数是12Ok。如果划分为两个给定数的最大数是1，则它们互质。相对质数是不同的质数。

We look at the example here, 8 and 15. The largest number that divides into both of it is one. But they themselves are not prime. Numbers is a divide by 1248. Five is ÷ 135, and 13, right? Either if you have two prime numbers, they will always be relatively part. Because the biggest thing that will divide both of them would be one and themselves and then divided to each other. So they will always be relatively fine. Right? How can we calculate the greatest common divisor? The first way that we can do it is we can do that for method, moving this around the numbers. And you can find factorize each of the composite numbers. For example, we can say 540 is q squared times three, q times five. And 144 is q to the r four times three squared. And then we can look for common factors. They don't. One has a five, but the other one has another five. So that's not a common factor. This one has e to the power two, this one also has e to the power two, this one has two to the power two. This one also contains e to the power two into the power 2 times into the power three is the greatest common divisor, which is 36.  
我们看看这里的例子，8和15。能分成两部分的最大数是1。但它们本身不是质数。数字是除以1248。5是÷135，13，对吗？如果你有两个质数，它们总是相对的。因为分裂他们两个的最大的东西将是一个人和他们自己，然后再分裂给对方。所以它们总是相对较好的。对的？如何计算最大公约数？我们可以做的第一个方法是我们可以为方法做这个，在数字周围移动它。你可以找到每个合数的因式分解。例如，我们可以说540是Q的平方乘以3，Q乘以5。144是Q与R的四次方。然后我们可以寻找共同的因素。他们没有。一个有一个5，但另一个有另一个5。所以这不是一个共同的因素。这个有E的2次方，这个也有E的2次方，这个有2的2次方。这个也包含e的2次幂乘以2的3次幂是最大公约数，也就是36。

As we said, this works fine. If the values are small, this works very badly if the numbers are large. So why does it better way of doing it? The numbers are large. So the easier and more efficient people are. The greatest common divisor is for the utility algorithm. And the rising idea that you create an algorithm is the notion that the greatest dominant divisor of a and b is also equal to the greatest common divisor of a and a modulus.  
正如我们所说，这工作得很好。如果值很小，如果数字很大，则效果很差。那么，为什么这是更好的做法呢？数字很大。所以人们越容易，效率越高。最大公约数用于效用算法。你创造一个算法的想法是，A和B的最大优势因子也等于A和A的最大公约数。

A sorry, b modulus a there is a common divisor of a and the modular reduction of b modulus a is basically also we write this on the divisor of a and b now, if we have larger numbers, we can reduce these numbers on very quickly.  
A，对不起，B的模数A，A有一个公约数，B的模数A的模约简基本上也是我们现在把它写在A和B的除数上，如果我们有更大的数字，我们可以很快地减少这些数字。

The greatest common divisor of 911 and 999. It's very common divisor of 911 and 999 marginal, 911, which is 88. The greatest on the divisor of, which is then equal to the rights on the divisor of ak and 31. It is a very common divisor, 31 and 26, which is, anyway, from the divisor of 5 and 26. This is the greatest common divisor of five. What right now? We can say that's easy to see a lot of things that divided the divide. One is one. Actually, these numbers are also relatively right, is the largest in the device, because this one, we can also write it in a different format. This one that comes from the way we write down the 30 after the almost in code form. We can say we have a variable a which is equal to one number a we have a variable b which is equal to the second number. While variable b is larger than zero, we will do remainder is equal to a module b and a will become equal to b b will become equal to r and as long as b is larger than zero, we will continue with the zoo.  
911和999的最大公约数。它是911和999的公约数，911是88。的除数上的最大值，它等于AK和31的除数上的权利。它是一个非常常见的除数，31和26，无论如何，它来自除数5和26。这是五的最大公约数。什么现在？我们可以说，很容易就能看到很多分裂的东西。一个是一个。实际上，这些数字也是相对正确的，是设备中最大的，因为这一个，我们也可以写成不同的格式。这一点来自于我们在代码形式中写下“几乎”后面的30。我们可以说，我们有一个变量a，它等于一个数a，我们有一个变量B，它等于第二个数。当变量B大于零时，我们将做余数等于模B，并且a将变得等于B，B将变得等于R，并且只要B大于零，我们将继续动物园。

And finally, if b is equal to zero, we will basically return a if we write down this algorithm, you can write the modulus are the explosion remainder form. We can say a is equal to the version times b plus r 999 is equal to 1 × 911 + 88. Then this 911 will move over to the side, because it will have to become the new a the or will become the ub in 511 is equal to 10 × 88 + 31. The ob will come to the ua the. Or will come to the ubak is 2 times 31 plus 56. There you are because the ua is 36 of gdp then the y is equal to 136 plus 5. 36 becomes the ua five becomes the ub 36 is equal to 5 and 5 + 1. Five becomes the ua one becomes the ub and basically, five is equal to 5 . 1 + 0, one of the ua zero of the ub rb is no longer bigger than zero.  
最后，如果B等于0，我们基本上会返回A，如果我们写下这个算法，你可以写出模是爆炸余数的形式。我们可以说A等于版本乘以B加上R999等于1×911+88。然后这个911将移动到一边，因为它将成为新的A，或者将成为511中的UB，等于10×88+31。OB会来到UA。或将来到乌巴克是2乘以31加56。这是因为UA是GDP的36%，那么Y等于136加5。36变成UA 5变成UB 36等于5和5+1。5变成了UA，1变成了UB，基本上，5等于5。1+0，UB RB的UA零之一不再大于零。

We have an a which is basically one, right? You can write it in this form. You can write it in this form, or we can constitute it in this form. Why do you do this? Because the first half of getting us the modular in this. So where is the module of english? A is the modular increase of b module in if a times b modular n is equal to y a is denoted as e minus one point n but he would also be a - 1 . 8.  
我们有一个A，基本上是1，对吗？你可以用这种形式来写。你可以把它写成这种形式，或者我们可以把它构成这种形式。你为什么要这么做？因为让我们在这方面模块化的前半部分。那么英语的模块在哪里呢？A是B模的模增量，如果A乘以B模N等于Y，A记为E减一点N，但他也是A-1。8.

These are very monitoring versus of each other. Right? The most important thing to remember here, as many people have this mistake, really. If there is a and b are so integers, you can just say a is equal to a fraction, which is one over b and one over b times b is equal to one modular in is one. They probably need to be a teacher, right? This is where the difficulty in finding the monitoring this comes in. Otherwise it would be very easy. You multiply something with itself inverted, and then basically we get a lot.  
这些都是相互监督的。对的？最重要的是要记住这里，因为很多人都有这个错误，真的。如果a和B都是整数，你可以说a等于一个分数，也就是1/B，1/B乘以B等于1的模。他们可能需要成为一名教师，对吗？这就是找到监控的困难所在。否则就很容易了。你把一个东西和它的倒数相乘，然后基本上我们得到了很多。

The thing is to find another integer. We can multiply e and the result review as a residue of a lot, right? As an example, he is the popular inverse of 507. The 3 × 5 is 15. Why do I say this? 17 is the marker inverse of 712, 16, 77 is 49, more than acc in the axis. For the answer, the reminder is one, right? The only thing that we need to remember, if we try to find a modular inverse of the mother in it will only work. It be more and n are relatively quiet. If you and am are relatively quiet, you will not be able to find a modular, even so the greatest on the divisor between p and n must be equal to one. We still have our numbers 911 and 199. So where is the modular english? All right? The modular inverse?  
关键是要找到另一个整数。我们可以把E和结果Review相乘，作为一个很大的残差，对吗？举个例子，他是流行的507的反面。3×5是15。我为什么这么说？17是712的标记倒数，16，77是49，比轴上的ACC多。对于答案，提醒是一个，对吗？我们唯一需要记住的是，如果我们试图找到母亲的模逆，它只会起作用。它更多和N是相对安静的。如果你和Am相对安静，你将无法找到一个模，即使这样，p和n之间的除数的最大值也必须等于1。我们还有电话号码911和199。那么模块化英语在哪里？好吧？模逆？

The next second part, I think the modular inverse is that we want to basically get the two numbers into the following format. We are given two numbers, a and b there is something called the extended utility and algorithm. It can basically solve for x and y a times x plus b times y is equal to the greatest common divisor of a and b in an example, you first do the billion of them, which we already did in the previous in two slides ago. So we know that the greatest on the rise of these two numbers are one. We know that they haven't wanted to reverse, and we have already written it down in the following order. What they said you can encounter like us is it takes this format from the video album, and it's gonna trace it back.  
接下来的第二部分，我认为模逆是我们想要把这两个数字变成下面的格式。我们有两个数字，A和B，有一种叫做扩展效用和算法的东西。它基本上可以解决X和y的问题，A乘以X加上B乘以y等于A和B的最大公约数。在一个例子中，你首先计算其中的十亿个，我们在前两张幻灯片中已经计算过了。所以我们知道这两个数字上升的最大值是1。我们知道他们没有想要逆转，我们已经按照以下顺序写下来了。他们说，你可以像我们一样遇到的是，它从视频相册中获取这种格式，并将其追溯。

In previous, we're going to take this last equation, 56 equals ~ 5 . 5 + 1. We are going to reorder it, and we're going to say, if anything is equal to 5 . 5 + 1, that means one is equal to 26 - 5 . 5. Then we're going to see this five term up here. You're going to reorder this order of this equation to say five is equal to 31, five, or one out of 86. You can substitute that in five. You can multiply out. And then you're gonna grow up, and you see this term between six. And you can reorder it. And you can say 26 is equal to 88 - 2 × 31. We substitute this equal 26. We multiply, and then we go to the 31, and we say 31 is equal to 111 minus ak we start to do this input anyone, and we multiply everything hard to hit, and we did terms with 508 and 8.  
在前面，我们将采用最后一个等式，56等于~5。5 + 1. 我们要重新排序它，我们要说，如果有任何东西等于5。5+1，这意味着1等于26-5。5. 然后我们会在这里看到这五个术语。你要把这个方程的顺序重新排序，比如5等于31，5，或者86中的1。你可以用五个来代替。你可以乘出来。然后你会长大，你会看到这个学期在六岁之间。你可以重新订购。你可以说26等于88-2×31。我们代入这个等于26。我们相乘，然后我们去31，我们说31等于111减去AK，我们开始做这个输入任何人，我们乘以所有难以击中的东西，我们做了508和8的项。

And then you can serve in the last one is 88. 88 is equal to 999 - 1 times 911, and we multiply it out.  
然后你可以在最后一个88发球。88等于999-1乘以911，我们把它乘出来。

And now we have the following format. Now we have read this common divisor of a and b which is one, is equal to 176 × 999 - 193 times 911. And I see we basically have something in this format. Where is on the divisor is one. A is 911, x is - 193. B is 999, and y is 176. All right? Next step is to do the last. If you want to do this, what we are going to do is going to take this equation, which is one is equal to 1 76,099 - 100, 93 × 911. We're going to do the modular reduction of 900 and 99.  
现在我们有了以下格式。现在我们已经读到了A和B的公约数，它是1，等于176×999-193乘以911。我看到我们基本上有这种格式的东西。除数上的是1。A是911，X是-193。B是999，Y是176。好吧？下一步是做最后一件事。如果你想这样做，我们要做的是用这个方程，它等于176，099-100，93×911。我们将对900和99进行模数缩减。

So now we get one. Why should I 999 is equal to decide one hundred nine hundred ninety nine. And if we have something, why should I 999? What's gonna happen to this term? We are something occupied by the modulus, and we tried to do modular reduction. What would be the remainder? Zero, because the larger is divided exactly to this term. This term is disappears, because they remain. There is zero. The area is one is - 100, 93 plus one hundred and one hundred and ninety nine. Right? And we can take this number. We can send it to the smallest positive number that is ungrouped, because you don't want to monitor in this. That is negative, right? That means it's 808.  
所以现在我们得到了一个。为什么我九百九十九等于决定一千九百九十九。如果我们有什么，我为什么要999？这个学期会发生什么？我们是被模数占据的东西，我们试着做模数归约。剩下的是什么？零，因为较大的正好除以这一项。这个术语消失了，因为它们仍然存在。有零。面积是一是-100，93加上一百一百九十九。对的？我们可以用这个号码。我们可以将其发送到未分组的最小正数，因为您不希望在此进行监视。这是消极的，对吗？也就是说是808。

Now, what happens is we have one is equal to 106 times 511, modular 990 990 solved for the moderators, because the question is, why can we multiply by 911? So that if the result is introduced by 999, the answer would be one. Okay? The right mind is it is quite complicated, but actually I promise you it is not sometimes it requires you to be part of a population. So this a lot of 6 year in terms of multiplying out, we have to be five people. But luckily, after you do every step, you can always check back by this. Having this include calculator to answer is the one. And if you've done the population, I really recommend i'll give you quite a few examples. If you try to do some of these results, you get a little bit use to doing the method in terms of finding it and seeing if you could find the right values, and you can follow my examples of you.  
现在，发生的是我们有一个等于106乘以511，模990，990为主持人解决了，因为问题是，为什么我们可以乘以911？因此，如果结果是由999引入的，则答案将是1。好的？正确的想法是它是相当复杂的，但实际上我向你保证它不是有时它需要你成为一个群体的一部分。所以这是6年的时间，我们必须有5个人。但幸运的是，在你完成每一步之后，你可以随时通过这个进行检查。有这个包括计算器回答是一个。如果你做过人口统计，我建议你给你举几个例子。如果你试着做一些这样的结果，你会有点习惯于用这种方法来找到它，看看你是否能找到正确的值，你可以按照我的例子来做。

The next concept we discuss is something called the word is notion for the waiters I function.  
我们要讨论的下一个概念是一个词，它是我所扮演的侍者的概念。

Basically, the oil supply function, the notes, the size of the second number, we say, five or n the five function is the total number of values between one and n that are relatively prime to it. Right? The other ways, if we sort of say, what is the 52, the total set of numbers between one and two that is relatively from the two is what? There is one number on the set. The answer is one. Then we have 53, then we have two numbers, one, and two. That are relatively 5 ° of the size of the cities, too. If we have four, one is ready to be prime, two is moderate to be private. Three is to be possible, is true and said, for 55 is the prime, number is 123, and four over the prime. And for six, one, and 550 prime for the size of the seat, they are all the same is two. You see that it's the size. It's it's the size of the state of the numbers between one. And in that is relatively propane, the size of the state of all the numbers between one and five, they are relatively 5 to 5, right?  
基本上，石油供应函数，音符，第二个数字的大小，我们说，5或n，5函数是1和n之间的值的总数，这些值与它互质。对的？另一种方法，如果我们说，52是什么，1和2之间的数字的总集合是什么？电视机上只有一个号码。答案是一个。然后我们有53，然后我们有两个数字，1和2。这也是城市规模的5°。如果我们有四个，一个是准备好的质数，两个是中等的私有。三是可能的，是真的，说，55是质数，数是123，四是质数。对于6，1和550，对于座位的大小，它们都是相同的。你看它的大小。它是1之间的数字状态的大小。这是相对的丙烷，所有数字的状态的大小在1到5之间，它们是相对的5到5，对吗？

These four different numbers, these few things that happened with the five function, we have a two if the greatest common divisor of a in a one. So we're in the end of relative reply. If we try to do five of him times in, it, just becomes five in as five in. All right? And for a prime number, we can calculate the five, the prime number as follows. If we have five of prime number to an exponent, then the phi function is p to the exponent minus 1 times p minus one. What these effects mean is that we can calculate the phi function of any opposite number by this prime factor being the prime factorization of that opposite number. It would be this opposite number is e to re times e two times e two times e three times e three, for example, that e to the ee two to the e two and e three to the e three, those are all really to be fine, because they're all prime numbers.  
这四个不同的数字，这几个发生在五函数中的事情，我们有一个二，如果A的最大公约数是一。所以我们在相对回复的最后。如果我们试着做五次，它就变成了五次。好吧？对于一个质数，我们可以计算出5，这个质数如下。如果我们有5个质数的指数，那么φ函数是p的指数减去1乘以p减1。这些效应的意思是，我们可以计算任何相反数的φ函数，通过这个素因子是那个相反数的素因子分解。这个相反数是e到re乘以e 2乘以e 2乘以e 3乘以E3，例如，e到ee 2到E2和E3到E3，这些都很好，因为它们都是质数。

Basically, we can just calculate the fire of the first time is representation, the five, the second crime, the five, the third crime and multiply them all together. So basically, for opposite number, that as prime factorization, we just basically calculate the five of each of the individual items separately and multiply them together. So five, 37, 37 is a prime number. So this is 537 to the power one. Using the equation, here, we just e to the e minus one times e minus one. This means we have 37 to the power of 1 - 1, which is the power of zero, which is 1 × 37 - 1, which is 36. For 5, 21. 21 is the composite number in privatization is 7 × 3. We have three to the power one. I'm sitting to the power one. That means there's three to the power 0 × 2 × 7 to the power 0 × 6. So that just becomes 2 . 6, which is equal to two. I I think it is equal the last little here.  
基本上，我们可以计算第一次的火灾是代表，第五次，第二次犯罪，第五次，第三次犯罪，并将它们相乘。所以基本上，对于相反数，作为质因式分解，我们只是分别计算每一项的5，然后把它们相乘。所以5，37，37是一个质数。所以这是537的乘方。使用这个等式，这里，我们只需要e到e-1乘以e-1。这意味着我们有37的1-1次幂，也就是零的幂，也就是1×37-1，也就就是36。为了5，21。21是私有化的合数，是7×3。我们有三到一的力量。我坐在动力一号。这意味着有三个0×2×7的0×6次幂。所以就变成了2。6，等于2。我认为它相当于这里的最后一点。

Philosopher here says that if a is not divisible, ip a to the p one is on grade one of the p the more useful version of this is the boiler generalization, which basically says that a is relatively five to n a to the five game is on going to one of the a it is to look at an example. If a is bn is n five, n is four, b to the bar four is 81, which is 108, where a is two, and n is 11. 5, 11 is. And due to the power gain is compared to 1,084 is under the 1 . 11. He did. There are a lot of theorem we can use in several ways, the way the generalization is, basically what makes far as a group. But I was saying that in the tutorial and the next loss of that world, but the other way we can use it is we can also use it. If we have a relatively small modulus and a very large exponent, and that we want their intention, and then we can reduce it a little bit, because then we can say 11 and 30 are relatively high.  
这里的哲学家说，如果A不是整除的，那么IP A到P 1是在P的第一级上，更有用的版本是锅炉泛化，它基本上是说A是相对于N的，A到5的博弈是在去A的一个上，这是一个例子。如果A是BN是N 5，N是4，B到条形4是81，也就是108，其中A是2，N是11。5，11是。由于功率增益与1，084相比低于1。11. 他做到了。有很多定理我们可以用几种方式来使用，推广的方式是，基本上是作为一个群体。但我在教程中说的是那个世界的下一个损失，但我们可以使用它的另一种方式是我们也可以使用它。如果我们有一个相对较小的模数和一个非常大的指数，并且我们想要它们的意图，然后我们可以把它降低一点，因为我们可以说11和30是相对较高的。

5, 13 is equal to 12, which means 11 to the power 12, much less 30 is on group one.  
5，13等于12，这意味着11的12次幂，更少的30在第一组上。

If you basically see this very large exponent as the multiple components of crowd, you consider 11 to the 12 concepts of any of the files. All these terms would reduce, divided, organizing any day with an event to the part of the or to the could be in a very specific eyes, made that we could use to make the explosion smaller. Maybe one of the communication. The reason for this is and why we are interested in modular explanation is that a lot of probability for code requires us to pay the integer, raise it, to explain it, and then they want to the reduction.  
如果您基本上将这个非常大的指数视为Crowd的多个组件，则可以考虑任何文件的11到12个概念。所有这些术语都会减少，划分，组织任何一天的事件，或者在一个非常具体的眼睛里，我们可以用来使爆炸变小。也许是其中一种交流。我们对模块化解释感兴趣的原因是，代码的很多概率要求我们支付整数，提高它，解释它，然后他们想要减少。

So another way for this is one of the exponentiation.  
另一种方法是求幂。

Basically, we're trying to operate a to the re modulo a if we use 70, if we say, 11 to the power of ea modular, 13, we do that. What do their reduction? It will be studied different terms and use the marginal reduction for all the individual terms. We can say this is either multiplied by itself 50 times. We're back in 18 months, 11 or 30, which is for I got four of them, and a lot of five are the accident.  
基本上，我们试图将A运算到RE模A，如果我们使用70，如果我们说，11到EA模的幂，13，我们这样做。他们的减少是什么？它将研究不同的术语，并对所有单独的术语使用边际减少。我们可以说这要么是乘以自身的50倍。我们在18个月后回来，11个月或30个月，这是因为我有四个，而很多五个都是意外。

And then that will be five. And then we'll take the 5 and 15, 11, and we'll get the next time. And we'll go through it and through it. And we finally find the value of the slide. It works. But it's not very efficient. So basically, the complexity is relative to the size of the exponent, because the size of the exponent is 50. And we needed 40 modular multiplication. The experiment becomes very large. We need to talk about this modular exponentiation of the very large exponent. Our calculation will become very slow. We need a better way of doing this. One of the most common ways to do modular explanation is something called the square and multiply algorithm. How does the square multiply under the word? We have 11 to the 15 module as it's the same as years before. But the first thing that we're going to do is we're going to take this 15 and write it as hours of 2, hours of 2 or 124, 8, 16, 32, sixty four hundred and twenty eight and 6. And it, all right. 15 is 4 + 8 + 2 + 1.  
然后就是五个。然后我们坐5路和15路，11路，我们下次再坐。我们将经历它，经历它。我们最终找到了幻灯片的值。这很管用。但效率不高。所以基本上，复杂性与指数的大小有关，因为指数的大小是50。我们需要40个模乘。实验变得很大。我们需要讨论这个非常大的指数的模幂运算。我们的计算会变得很慢。我们需要一个更好的方法。进行模块化解释的最常见方法之一是所谓的平方和乘法算法。这个词下面的正方形是怎么相乘的？我们有11到15个模块，因为它和几年前一样。但我们要做的第一件事是我们要把这个15写成小时2，小时2或者124，8，16，32，6428和6。还有它，好吧。15是4+8+2+1。

18 to the 15, sorry, 11 to 15 is equal to 11 to the ra plus four plus 2 plus 7, basically. 11 to the ra times 11 to the 4 times 11 squared times 11. What are you doing now? Is the square 11. It is hundred thirty one. We do the modular reduction, which is for then we're gonna take 11 to the power of four. We treated as interpreter as 11 square, all square, but we've already talked about it. The answer for 11 square, which is four. We get this substitute in here. Then you simply say four squared, which is 16 or 13, which is three. And then we get to 11 to the car, right? It is equal to 11 to the power, four, all squared. But we already calculated the answer already. And for I was three, so we just up feeling three. We do one square. That is not.  
18到15，对不起，11到15等于11到RA加4加2加7，基本上。11到RA乘以11到4乘以11的平方乘以11。你在做什么？是正方形11。它是一百三十一。我们做模约简，然后我们要取11的4次幂。我们把翻译当作11个正方形，所有的正方形，但我们已经讨论过了。11平方的答案是4。我们把这个替代品放在这里。然后你简单地说4的平方，也就是16或13，也就是3。然后我们到11点上车，对吗？它等于11的次幂，4，全部平方。但我们已经计算出答案了。我当时只有三岁，所以我们感觉只有三岁。我们做一个正方形。那不是。

Now we learn the positive reduction for it into eight, which is 9, 11 to the 4, which is 3 and 11 squared, which is four. We substitute it back in here. We substitute nine for it. Today. You substitute 3 or 11 to the 4. You substitute 4 or 11 squared and 11. I will just do three more multiplication. I have 3 × 4 × 7 on july 30 is equal to four. The advantage of this is rather complexity being related to the size of e the complexity now becomes the log of v right? That is significantly more efficient for everybody.  
现在我们学习它的正归约为8，也就是9，11到4，也就是3和11的平方，也就等于4。我们把它放回这里。我们用九来代替它。今天。你用3或11代替4。你用4或11的平方和11来代替。我再做三次乘法。我7月30日的3×4×7等于4。这样做的好处是复杂度与E的大小有关，复杂度现在变成了V的对数，对吗？这对每个人来说都更有效率。

In the lecture, I said the number theory is quite useful. You understand asymmetric equation? And that is true. But as we said, in the first lecture, is also useful to have a broad knowledge of information, security, even if you are not interested in specific parts a lot, because it helps you in other areas. All right? So even if you're saying might not necessarily, they will propose or not necessary, if you are going to develop or implement secure systems, it's so useful for you to understand the good of all these words. Why we can look at one example. Here is the code that we used to implement squared multiply algorithm, or at least probably we can use to implement this very multiplier. We make the exponent, and we saw the body representation of the exposure. Basically, it certainly becomes a binary value. Right? Most valuable, very significant bit on the air is significant bit on the right.  
在演讲中，我说数论很有用。你懂不对称方程吗？这是真的。但正如我们在第一堂课中所说的，对信息、安全有广泛的了解也是有用的，即使你对特定的部分不感兴趣，因为它在其他领域对你有帮助。好吧？所以即使你说可能不一定，他们会建议或没有必要，如果你要开发或实施安全系统，理解所有这些词的好处对你来说是非常有用的。为什么？我们可以看一个例子。这是我们用来实现平方乘法算法的代码，或者至少我们可以用来实现这个乘法器。我们做了指数，我们看到了曝光的身体表现。基本上，它肯定会变成一个二进制值。对的？广播中最有价值的、非常重要的部分是右边的重要部分。

There are key bits in the binary representation of there is equal to one, and they have a four loop For I equal to t minus one, down to zero, due to the following. There is equal to zero square model in, right? If the current is started, that is one, then you z equal to z times a modular in. If the current expanded is zero, this goes straight back to the volume. The z is equal to z square on the end. What do you think is interesting about this piece of photo? What happens if our exponent it is common in asymmetric incursion? Usually a secret value of private value, or the value that we try to take? Is this. So, right? If somebody is looking for the exponent, but somebody can somehow get access to our computing platform. And I can see how long it takes one loop of this world is Complete? Why are they able to do? What happens in this view? If e is one, we have a square and multiply. If e is zero, we only have a square.  
在的二进制表示中有等于1的密钥位，并且由于以下原因，它们有一个四循环，I等于t减1，下降到0。中有一个等于零的平方模型，对吗？如果电流是开始的，那就是一，那么你的Z等于Z乘以一个模。如果扩展的电流为零，则直接返回到卷。Z等于末端的Z平方。你觉得这张照片有什么有趣的地方？如果我们的指数在不对称入侵中很常见，会发生什么？通常是私人价值的秘密价值，或者是我们试图获取的价值。是这个吗。所以，对吧？如果有人在寻找指数，但有人可以以某种方式访问我们的计算平台。我可以看到这个世界的一个循环需要多长时间才能完成。他们为什么能做到？在这个视图中发生了什么？如果e是1，我们有一个平方和乘法。如果e是零，我们只有一个平方。

The loop will run faster away when he is good one or e is the zero. It will run faster with a bit of zero, because they can only do a swear. Whereas if the village is one, we do have a square. We do a lot of fun. So in one case, we have two modulus. The other one, we have one where the square module in. If e is zero, we have a square module in. And then as it comes a modular in, if e is equal to one, it is definitely a loop is short. When it is zero, group is long. We did this one. And why is this important that in the large segment of security, in terms of other happy, it is referring to as 500 analysis.  
当他是好的1或者E是0的时候，循环会跑得更快。它会运行得更快一点零，因为他们只能做一个发誓。然而，如果村庄是一个，我们确实有一个广场。我们玩得很开心。所以在一种情况下，我们有两个模数。另一个，我们有一个正方形模块。如果e是零，我们有一个平方模。然后当它进入模的时候，如果e等于1，它肯定是一个短循环。当它为零时，组为长。我们做了这个。为什么这很重要，在安全的大部分中，就其他快乐而言，它被称为500分析。

When we run code on a processor that the processor is made up of billions of transistors. So there is an easy way to switch, right? Which is either on marble. As I'm writing my code, millions of 7, billions of switches off as the switches turn on and off, the power consumption of your processor changes. Right? If the attacker comes along and measures the power consumption of your processor, they can somehow sometimes find patterns that indicates that what the code is actually doing. So many of you have any comics that switch on the board really fast. So the electronics are acting as radio emitter, right? They give us electromagnetic signals. If you look at apc board, sometimes it happens on PC board. Like if you have faces, it just be a different subsidiary in the high frequency communication. That trace wire becomes an antenna, and it comes at all.  
当我们在处理器上运行代码时，处理器是由数十亿个晶体管组成的。所以有一个简单的方法来切换，对吗？要么是在大理石上。当我写代码的时候，数百万，数十亿的开关随着开关的开启和关闭，处理器的功耗也会发生变化。对的？如果攻击者出现并测量您的处理器的功耗，他们有时可以以某种方式找到表明代码实际在做什么的模式。你们中的很多人都有在黑板上快速切换的漫画。所以电子设备就像无线电发射器一样，对吗？它们给我们电磁信号。如果你看看APC板，有时它发生在PC板上。就像如果你有脸，它只是高频通信中的一个不同的附属部分。那根追踪线变成了天线，它来了。

All right? And you can basically listen to the communication if you have the right, and then you have to receive it, but it is completely unimaginable. The side channel is all about getting Information from platform behavior. There is an additional sometimes you also heard you may be like Google channel. Google channel is different. Every channel is, I have access to the platform. I am actually trying to be better without anyone finding out. Five channel is a platform is doing the same, but unintentionally meeting Information. What we have here. This is actually a chip is a smart card running rsa and doing more to the explanation. It's raising the size of x to the private key is the experiment. And the sockets is the value that you are raising and you're doing modulus with the public modulus a and if you look very closely at these, the relations between the spies, the little spice you see in the car price is actually every single part of the four loop of these all results.  
好吧？而且你有权的话基本上可以听一下，然后你要接收一下，但是完全不可想象。侧通道是指从平台行为中获取信息。有一个额外的，有时你也听说你可能喜欢谷歌频道。谷歌频道则不同。每一个渠道都是，我都有进入的平台。我其实是想在别人不知道的情况下做得更好。五频道是一个平台，也在做同样的事情，但无意中遇到了信息。我们这里有什么。这实际上是一个芯片，是一个运行RSA的智能卡，并做了更多的解释。实验是将X的大小提高到私钥。插座是你提高的值，你用公共模数A做模数，如果你仔细观察这些，间谍之间的关系，你在汽车价格中看到的小香料实际上是所有这些结果的四个循环的每一个部分。

You see, that is a short gap and a short gap. And a short gap is something. There's a long gap. Then there's a short gap and a short gap and a longer one, and a short, and long and a short, long, short. And how can you see this price? You not just read up the priority, because you can get 00001001001, 00010005050. I probably would be extremely bad. Our analysis can be very powerful. They correctly analysis the same. This is unit is exactly the same. The reason for this happening is that with a short gap going in despair, along the gap year of the square and multiply. And there's lots of people who work on. This is a very, other, very complicated things that people could do.  
你看，那是一个短暂的缺口和一个短暂的缺口。短暂的差距是很重要的。有很长的间隙。然后有一个短的缺口，一个短的缺口，一个长的，一个短的，长的，短的。你怎么能看到这个价格？你不只是读了优先权，因为你可以得到00001001001，00010005050。我可能会非常糟糕。我们的分析可以非常强大。他们正确地分析了同样的问题。这个单位是完全一样的。发生这种情况的原因是，随着短暂的间隔走在绝望中，沿着间隔年的平方和相乘。有很多人在研究。这是人们可以做的另一件非常复杂的事情。

So actually, this this one on the right, actually an acoustic measure. So they just look at this on PC like a really high quality microphone. And they were listening to the sounds coming over the PC while they were doing it on a procratic algorithms. I have some way of giving it some chosen matrix doing curve. It would make something happen to the encryption algorithm that sometimes they found unique.  
所以实际上，右边的这个，实际上是一个声学测量。所以他们只是在PC上看这个，就像一个真正高质量的麦克风。当他们在ProCratic算法上做这件事的时候，他们正在听电脑上传来的声音。我有一些方法给它一些选择的矩阵做曲线。它会使加密算法发生一些变化，有时他们会发现这是独一无二的。

What do you frequencies in specific patterns that would indicate? Then what the secret material of the soccer was? The idea was actually sometimes decipher or makes the process work really hard for a very big amount of time. It's always actually come from the power supply. The design needs to adapt to basically deliver much more power and only that. But it is a very interesting science study insecurity. It was very profitable. In the 1990s. Some students are in Stanford on came up with an idea for a new attack of all the rates of our analysis. They were very smart, because on today everybody does is they publish their attack. It's a conference. You get a very nice conference, but they didn't do this. Instead, they got a complication of good, and then they acted the competition. I asked that the confirmation they come out and say, hey, by the way, we got this wonderful attack is going to break it with you. All right.  
你在特定模式中的频率表明了什么？那足球的秘密材料是什么？这个想法实际上有时会被破译，或者让这个过程在很长一段时间内非常困难。它实际上总是来自电源。设计需要适应，基本上提供更多的权力，仅此而已。但研究不安全感是一门非常有趣的科学。它非常有利可图。上世纪90年代。斯坦福大学的一些学生提出了一个新的想法，对我们所有的攻击速率进行分析。他们非常聪明，因为今天每个人都在发表他们的攻击。这是个会议。你得到了一个非常好的会议，但他们没有这样做。相反，他们得到了好的并发症，然后他们在比赛中表演。我要求确认他们出来说，嘿，顺便说一句，我们得到了这个美妙的攻击将与你打破它。好吧。

And then basically, all the companies review proper processors had to license. It happens. I think in some sense, it was rumors that for every single parent part of the world, they need to be paid a couple of things if you get all right. And there's only a couple of things for a credit card. You have to think that is like a clear card. That is a very good amount of money. But it's a very powerful attack.  
然后基本上，所有公司审查适当的处理器都必须获得许可。它发生了。我认为在某种意义上，有传言说，对于世界上的每一个单亲家长来说，如果你一切顺利，他们需要得到一些东西。信用卡只有几样东西。你必须认为这就像一张明牌。这是一笔很大的数目。但这是一种非常强大的攻击。

It's something that always needs to be considered if you write in code, because usually the kind of class code guess about it, because he doesn't worry about the hardware. Right? At the same time, the security guy doesn't really worry about how the code gets into a lot of the something interesting that he wanted to consider. We're able to decide analysis. If you have to interpret the processors, they will not have mitigation booking. So they have random are places to be interviewed. So they are high power consumption, rather be people code this, but I think he would rather delay. Right? And there will be some other masking going on to find high this behavior, a very strong attack. It's something that was considered very for interest. So it's available. Now. We can take a 10 minute break, and then we can have these on around 8 +. And.  
如果你写代码，这是需要考虑的事情，因为通常类代码会猜测它，因为他不担心硬件。对的？同时，安全人员并不真正担心代码如何进入他想要考虑的许多有趣的东西。我们能够决定分析。如果你必须解释处理器，他们将不会有缓解预订。所以他们有随机的地方接受采访。所以他们的功耗很高，宁愿被人编码，但我认为他宁愿延迟。对的？还会有一些其他的掩蔽继续进行，以发现这种行为，一种非常强烈的攻击。这是一件非常有趣的事情。所以它是可用的。现在。我们可以休息10分钟，然后我们可以在8+左右使用这些。和。