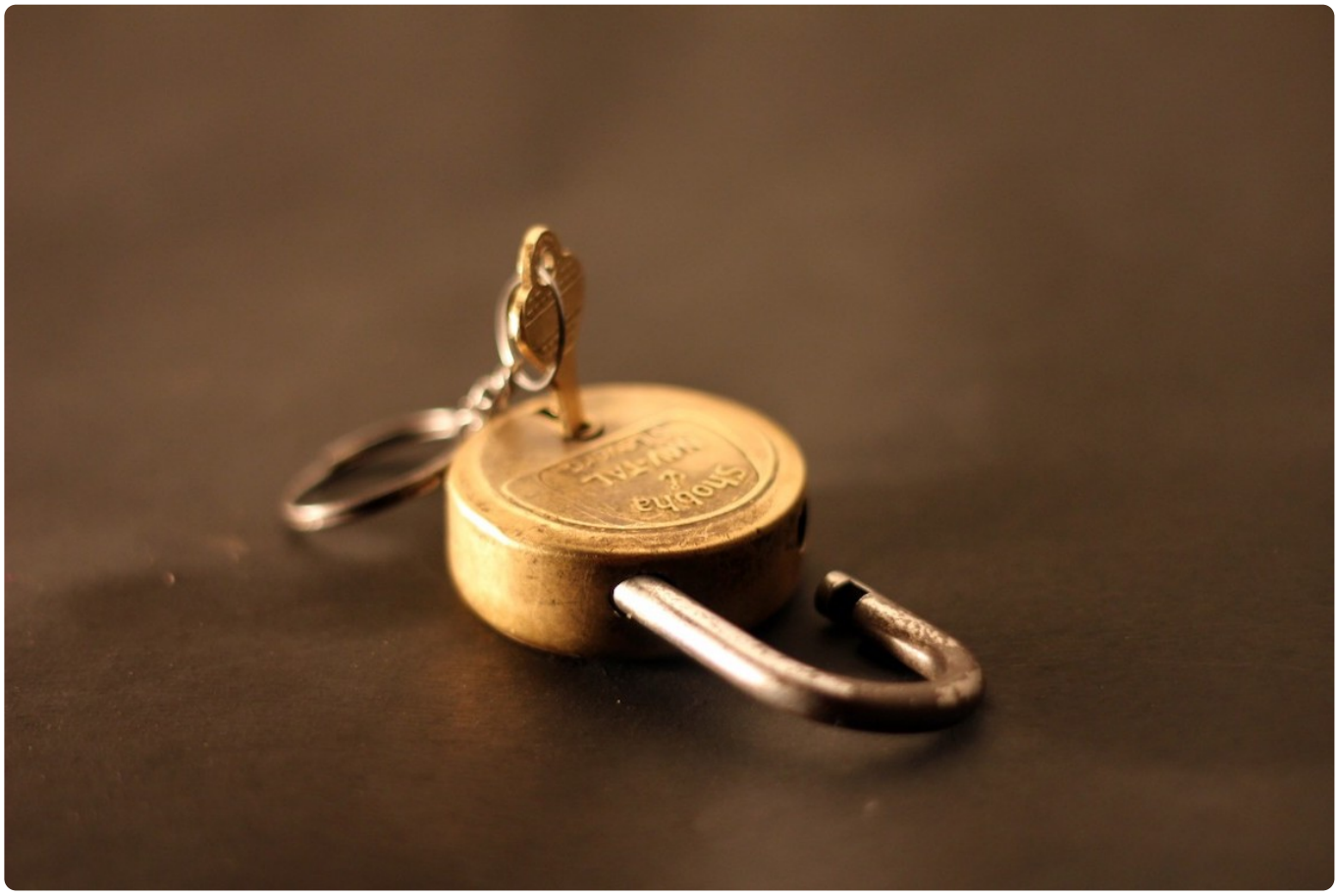
开篇词 | 人人都要会点密码学

2020-11-23 范学雷

实用密码学 进入课程 >



讲述：范学雷
时长 12:45 大小 11.69M

你好，我是范学雷。

2020 年，庚子年。如果你问我，2020 年有什么愿望，我想说，这一年，咱们能不能重启？如果一切真的可以重启，哪些事情是我们可以做得更好的？哪些问题是我们依然无法避免的？

如果可以重来，我想，Zoom 最想做的，一定是聘用密码学领域的专家，提高研发人员的密码学见识，让研发人员都学会和用好密码学。

Zoom 怎么了?

Zoom 怎么了？为什么 Zoom 要和密码学较劲?

熟悉在线会议系统的都应该知道，Zoom 是这个领域的市场领先产品。2020 年初，随着 COVID-19（新冠肺炎）在全球的蔓延，高质量的在线会议变成了一个居家办公、远程工作的必需品。

这时候的 Zoom，也做好了所有的准备，它很好地满足了人们远程工作的急切需求。直到 2020 年 3 月底，Zoom 都是主流市场的主要选择之一。

然而，到 3 月底，事情急转直下。2020 年 3 月 31 日，研究者公开了 Zoom 的重大安全漏洞，认为 Zoom 并不适用于办公会议。**最严重的问题，就是和密码算法与密码管理相关的问题。**

比如说，Zoom 使用了 ECB 加密模式，而这种加密模式并不是一种安全的加密模式。而且，这件事也不是秘密，ECB 加密模式的安全问题至少披露了二三十年了。

随后，有不少知名的公司、教育机构以及政府组织，出于信息安全的考虑，禁止使用 Zoom，转而寻找替代产品。本该大展身手、攻城略地的时候，Zoom 被闷头打了一棒，把大量的机会拱手让给了竞争对手。而这种市场机会，我认为前五十年未见，后五十年难寻。

不过，Zoom 马上聘用了安全领域的专家，全力以赴地解决掉了这些问题。幸运的是，对 Zoom 来说，这些问题发现得并不算晚，应对得也不算拖拉。不幸的是，由于**算法选择失当**这样的“小问题”，Zoom 给了竞争者充分的空间，自身的品牌和信誉也受到了很大的伤害。

Zoom 是个特例吗?

从安全漏洞的角度来看，单个问题本身并不可怕。重要的是我们该怎么快速反应，该怎么杜绝后患。杜绝后患的思路之一，**就是要求同样的安全问题，一定不要重复上演。**

我相信，Zoom 可以做到这一点。但是，其他的公司呢？其他的产品呢？很遗憾，我不相信 Zoom 会是最后一个用错了 ECB 加密模式的产品或者公司。现在和未来，依然会有人

用错 ECB 加密模式，以及其他的密码算法。

今天，用错密码算法的产品和公司，能够快速反应并及时修复它们的安全问题吗？明天的产品和服务，能够做到在合适的场景下，使用合适的密码算法吗？对于答案，我依然有些悲观。

我之所以悲观，是因为大部分产品的研发人员，甚至都不知道 ECB 加密模式有什么问题，当然在使用它的时候也就很无畏。

如今，能够做到在不同的场景，使用不同的密码算法的研发人员，数量还很少；懂得密码学的安全领域的专家，数量更少；能够跟得上密码学发展进程的研发人员，数量更是少得可怜可叹。

为什么要学密码学?

为什么会这样？其实，这里面既有历史原因，也有学科原因。

十多年以前，操作系统和通信协议这样的基础设施，通过内嵌的安全机制，就可以满足大部分的点对点的信息安全需求了。所以，那时候的信息安全直接需求并没有那么大。

再加上现代密码学门槛高、出道晚，它的这种特殊性让其一直都是少数人的游戏。即使是数字化时代，隐私保护和信息安全已经成为重要议题的时候，密码学也没有成为每个程序员的必修课。

但是，**十年以前，这或许不是问题。可是，从今以后，这会是一个越来越严重的技术债。**

因为，现代信息安全的需求，越来越多地跳出了基础设施的范畴，进入了应用程序层面。

操作系统、通信协议这样的基础设施，早就已经满足不了应用的多样化需求了。比如，像 Zoom 这样的在线会议产品的安全需求，底层的基础设施提供的安全保障能力，是远远不够的。

不过，好在机遇与挑战总是并存的。近年来我参加的每一次密码学会议，**都会有人提到密码学专业人才的短缺**。的确是这样的，市场的需求和供给之间有一个巨大缺口。

总的来说，现在密码学的市场情况主要有以下两个特点：

> 密码学领域难以招聘，即使平均报酬已经高出了一大截；不过这也使得与密码学相关的工作超级稳定，很少会看到一个信息安全工程师有 35 岁的忧愁，抑或 45 岁的哀伤。
>
> 密码学应用很尴尬，由于研发团队缺乏专业的密码学素养，算法场景错配或使用有安全漏洞的算法和协议的问题层出不穷。遗憾的是，这个缺口还没有停止扩张的迹象。

密码学虽是一个小门类，但是涉及内容庞杂。从踏进门到能够使用密码学技术去设计一个像样的、安全的系统，需要短则两三年、长则七八年的积累。所以，无论是领取报酬的工程师或者是支付薪酬的公司，有耐心的实在是少数。

当然，好的耐心是有回报的。不同于其他的软件工程师，密码学是一个需要深度积累的领域，年头越长，见识越多，越了解其中的坑坑洼洼，生产效率和产品质量也越高。可以这么说，**有经验的信息安全工程师，是每一个公司的关键人力资源。**

45 岁，好日子才刚刚开始。

如何学习密码学?

既然密码学这么难，如果我们想学习密码学的知识，该从哪里开始呢？有没有办法降低门槛?

学习的途径，不外乎两个：读书和培训。

密码学最好的书籍，当属Bruce Schneier 的《应用密码学：协议、算法与 C 源程序》。这应该没有太多争议。很多同学的密码学入门，就是从这本书开始的。二十多年前，我也是从这本书开始的。即使是现在，它也是我能在市场上找到的、最好的密码学入门书籍。

不过，和其他密码学书籍一样，这本书虽然叫做应用密码学，对于普通的软件工程师，它依然太难了。除此之外，这本书的内容，是 1996 年之前的密码学世界，和现在的密码学相差有点远。

其中提到的算法，很少还能够继续使用了；书中的源代码，无论是理论上还是实践上，都有很多的安全漏洞，也已经不能用在现在的产品中了。所以，如果你发现，一个产品还在使用这本书的算法和源代码，它的安全性是值得你担心的。

这就需要我们重新审视和评价现在的密码算法：哪些还能用？哪些要淘汰？不同的场景，应该使用什么样的算法？使用算法的时候，有哪些常见的陷阱？作为软件开发者，我们应该掌握哪些密码技术？掌握到什么程度？这些问题，都是我们要重新梳理，重新认识的。

一般来说，非密码学专业领域的研发人员，是**不需要了解密码算法的数学细节和实现细节的**。那么，我们应该了解哪些密码学知识呢？我认为主要有以下三点：

密码学可以解决什么样的问题？

也就是说，我们需要了解密码学的基本概念和体系，知道密码学能解决什么样的问题，不能解决什么样的问题。这就算是敲了敲密码学的大门了。

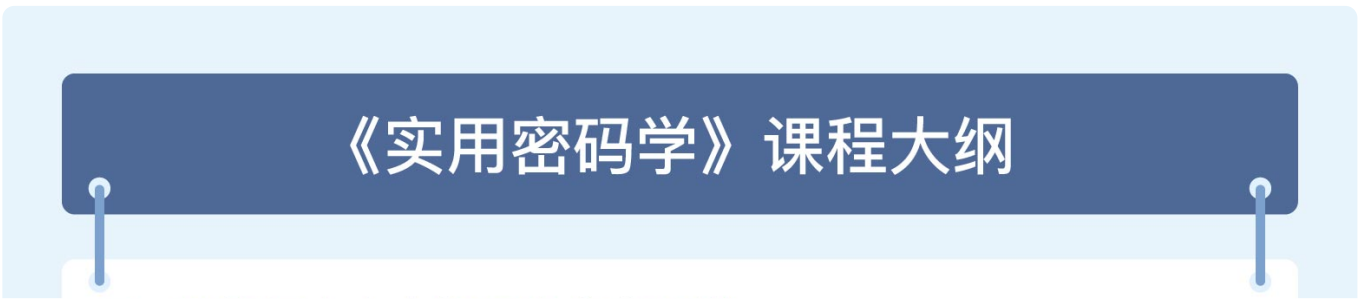
面对具体的问题，我们应该使用什么样的密码技术？

也就是说，如果遇到具体的问题，我们应该选择什么样的算法，当心什么样的问题。这需要我们了解每一个算法的适用场景，以及它的局限性。这算是跨进大门，打怪晋级，修炼十八般武艺。

面对真实的产品，应该怎样组合不同的密码技术？

一般来说，一个产品里需要组合多种密码技术，才能够实现信息安全。单独耐看的技术，搭配起来可能就是一团糟。这需要我们组合、搭配好不同的密码技术，甚至包括非密码的信息安全技术。也就是把密码技术用起来，解决真实的问题。

简单地说，就是要学会、用好密码学。



这个专栏教你什么?

我会带你厘清密码学及其算法背后的基本概念和基本逻辑。只有基本概念和基本逻辑弄清楚了，我们才会降低用错密码学技术的风险。这个专栏也是围绕基本概念和基本逻辑安排的。

不过，你不用担心基础知识枯燥难学。不同于一般的密码学课程和教材，我会把重点放在**各种密码技术的适用场景和局限性**上。因为，单纯地学习密码学的知识，其实没有特别大的用处，弄清楚基本概念和基本逻辑最好的办法，就是了解支持它们的实际问题和现实需求。

所以，这个专栏的每一篇文章，都是从问题开始的，也是以问题结束的。可以说，实际问题和现实需求是领着我们一步一步深入密码学内部的线索。

你也知道，用错密码学的后果很严重。所以，**教你用好密码学，就是这个专栏的目标。我想通过这个专栏帮助你把握住基本概念、弄明白适用场景、躲得开常见错误。**

不过，要学好这个专栏，还需要你做好两件事。

第一件事情是关注问题。当你阅读的时候，如果遇到提出问题的文字，停下来思考一小会儿，看看自己有没有什么想法，或者更多的问题。专栏里，我们会提出很多问题，每一个问题，都会引出更多的内容，甚至更多的问题。

你只有认真地思考了每一个问题，才能掌握这个问题，才能对后续的解决方法有更深入的了解。**在密码学的世界里，了解问题总是比掌握解决方法还要重要。**

第二件事情是提出问题。除了专栏里提出的问题之外，你会不会发现新问题，有没有新思路？密码学算法最神奇的地方之一，就是外行看觉得好完美，内行看觉得好无奈。

因为，**密码学的每一个基本概念，都有它的缺陷；每一个算法，都有要命的缺点**。专栏里，我试着向你去提出最关键的问题。但是毫无疑问，我不能覆盖所有的问题。

但我相信专栏里提问题的角度能给你一些启发，帮助你从不同的角度，掂过来倒过去地琢磨每一个基本概念和算法，看看你有没有新问题，有没有新思路。**你能够找到的无奈的地方越多，你对问题的了解就越深入，学到的东西也就越多。**

说实话，这个专栏有点硬，不是一个讲故事、听故事的专栏。我尽了自己最大的努力使它平实易懂，但是它依然是一个硬得硌人的专栏。这个硬度的主要来源，不是因为难懂，是因为我们要不断地思考各种各样的问题，而不是我塞给你一堆知识。

另外，本专栏会主讲密码学的基础知识和逻辑，对于密码学中较难的部分：非对称密码技术，我们课程暂时不会过多涉及。你可以先打好基础，再去拓展进阶的知识，这对于你来说，才是一条更好的学习路径。

我是谁?

最后介绍一下我自己吧。

我是范学雷，在密码学应用领域已经工作了二十多年了。目前，担任 Oracle 的首席软件工程师，是 Java 安全组的成员，OpenJDK 安全评审成员，也是 Java 安全的主要推动者和贡献者之一。

我的日常工作包括关注信息安全威胁与技术进展，参与信息安全领域国际合作，制定与实现 Java 安全规范，提升 Java SE 生态安全水准，促进 Java 技术的普及与运用等。

我曾在极客时间做过第一季专栏《代码精进之路》，在那个专栏里，我总结了自己 20 多年的编程心得和代码评审经验。而这一次，我希望可以带你走一小段密码学的旅程。

如果你还没有密码学的基础，那我们就可以从这里开始；如果你已经学习了《应用密码学》，或者有密码学应用的经验，那我们可以一起去看看密码学最新的进展，以及最新的密码学算法。

欢迎在留言区留言，记录、讨论你的想法，或者写下你的期待，让我们一起努力！

好，我们开始吧！

提建议

下一篇 01 | 学习密码学有什么用?

精选留言 (8)

写留言

Daiver
2020-11-23

期望能讲讲国密算法

展开

作者回复: 专栏正文部分没有计划，我看看是否可以做一个加餐。

7

rocedu
2020-11-23

有国密算法内容吗?

展开

作者回复: 国密算法暂时没有计划。据我所知，国密算法和世界通行的算法差别不大，或者就是通行算法的变形。了解了基本的算法，进阶国密算法应该没问题。

2 6

sugar
2020-11-23

赞👍，期待这个硬核专栏很久了。密码学的一些书籍，读起来晦涩得很，有这样一个专栏以更友好的方式提供给大家一个通向low level stuff的捷径。很棒!

展开

作者回复: 我们一起来看看，能不能有一个更好的方式普及密码学常识。

1

万丰路甲一号
2020-11-23

研究生唯一挂科的一门课

展开

作者回复: 这个专栏不会挂科，还一定比研究生课程有趣。

1

明
2020-12-02

我们公司前一阵子 公司安全检查的时候 服务器裤衩子都被扒出来了 😂😂😂

作者回复: 很正常，懂安全的人还很少。

TerryGoForIt

2020-11-25

范老师牛批！

展开

赵阳

2020-11-25

我是做区块链应用开发的工程师，一直想系统的学习密码学相关的知识，今天终于找到了

作者回复: 区块链持续的大热门啊！

咱是吓大的

2020-11-24

密码学向来是外行看热闹，内行看门道。从今天开始，我也来看看门道。

作者回复: ;-) 有门道的，看完之后就可以谈门论道了。