

42 | DHE/ECDHE算法的原理

2019-10-11 Chrono

《透视HTTP协议》

课程介绍 >



讲述：Chrono

时长 08:06 大小 6.50M



你好，我是 Chrono。

在🔗第 26 讲里，我介绍了 TLS 1.2 的握手过程，在 Client Hello 和 Server Hello 里用到了 ECDHE 算法做密钥交换，参数完全公开，但却能够防止黑客攻击，算出只有通信双方才能知道的秘密 Pre-Master。

这是 TLS 握手的关键步骤，也让很多同学不太理解，“为什么数据都是不保密的，但中间人却无法破解呢？”

解答这个问题必须要涉及密码学，我原本觉得有点太深了，不想展开细讲，但后来发现大家都对这个很关心，有点“打破砂锅问到底”的精神。所以，这次我就试着从底层来解释一下。不过你要有点心理准备，这不是那么好懂的。

领资料



先从 ECDHE 算法的名字说起。ECDHE 就是“短暂 – 椭圆曲线 – 迪菲 – 赫尔曼”算法 (ephemeral Elliptic Curve Diffie–Hellman)，里面的关键字是“短暂”“椭圆曲线”和“迪菲 – 赫尔曼”，我先来讲“迪菲 – 赫尔曼”，也就是 DH 算法。

离散对数

DH 算法是一种非对称加密算法，只能用于密钥交换，它的数学基础是“离散对数” (Discrete logarithm)。

那么，什么是离散对数呢？

上中学的时候我们都学过初等代数，知道指数和对数，指数就是幂运算，对数是指数的逆运算，是已知底数和真数（幂结果），反推出指数。

例如，如果以 10 作为底数，那么指数运算是 $y=10^x$ ，对数运算是 $y=\log x$ ，100 的对数是 2 ($10^2=100$ ， $\log 100=2$)，2 的对数是 0.301 ($\log 2 \approx 0.301$)。

对数运算的域是实数，取值是连续的，而“离散对数”顾名思义，取值是不连续的，数值都是整数，但运算具有与实数对数相似的性质。

离散对数里的一个核心操作是模运算，也就是取余数 (mod，在 C、Java、Lua 等语言里的操作符是“%”)。

假设有模数 17，底数 5，那么“5 的 3 次方再对 17 取余数得 6” ($5^3 \% 17 = 6$) 就是在离散整数域上的一次指数运算 ($5^3 \pmod{17} = 6$)。反过来，以 5 为底，17 为模数，6 的离散对数就是 3 ($\text{Ind}(5, 6) = 3 \pmod{17}$)。

这里的 (17, 5) 是离散对数的公共参数，6 是真数，3 是对数。知道了对数，就可以用幂运算很容易地得到真数，但反过来，知道真数却很难推断出对数，于是就形成了一个“单向函数”。

在这个例子里，选择的模数 17 很小，使用穷举法从 1 到 17 暴力破解也能够计算得到 6 的离散对数是 3。

领资料



但如果我们选择的是一个非常非常大的数，比如说是有 1024 位的超大素数，那么暴力破解的成本就非常高了，几乎没有什么有效的方法能够快速计算出离散对数，这就是 DH 算法的数学基础。

DH 算法

知道了离散对数，我们来看 DH 算法，假设 Alice 和 Bob 约定使用 DH 算法来交换密钥。

基于离散对数，Alice 和 Bob 需要首先确定模数和底数作为算法的参数，这两个参数是公开的，用 P 和 G 来代称，简单起见我们还是用 17 和 5 ($P=17$, $G=5$)。

然后 Alice 和 Bob 各自选择一个随机整数作为**私钥**（必须在 1 和 $P-2$ 之间），严格保密。比如 Alice 选择 $a=10$ ，Bob 选择 $b=5$ 。

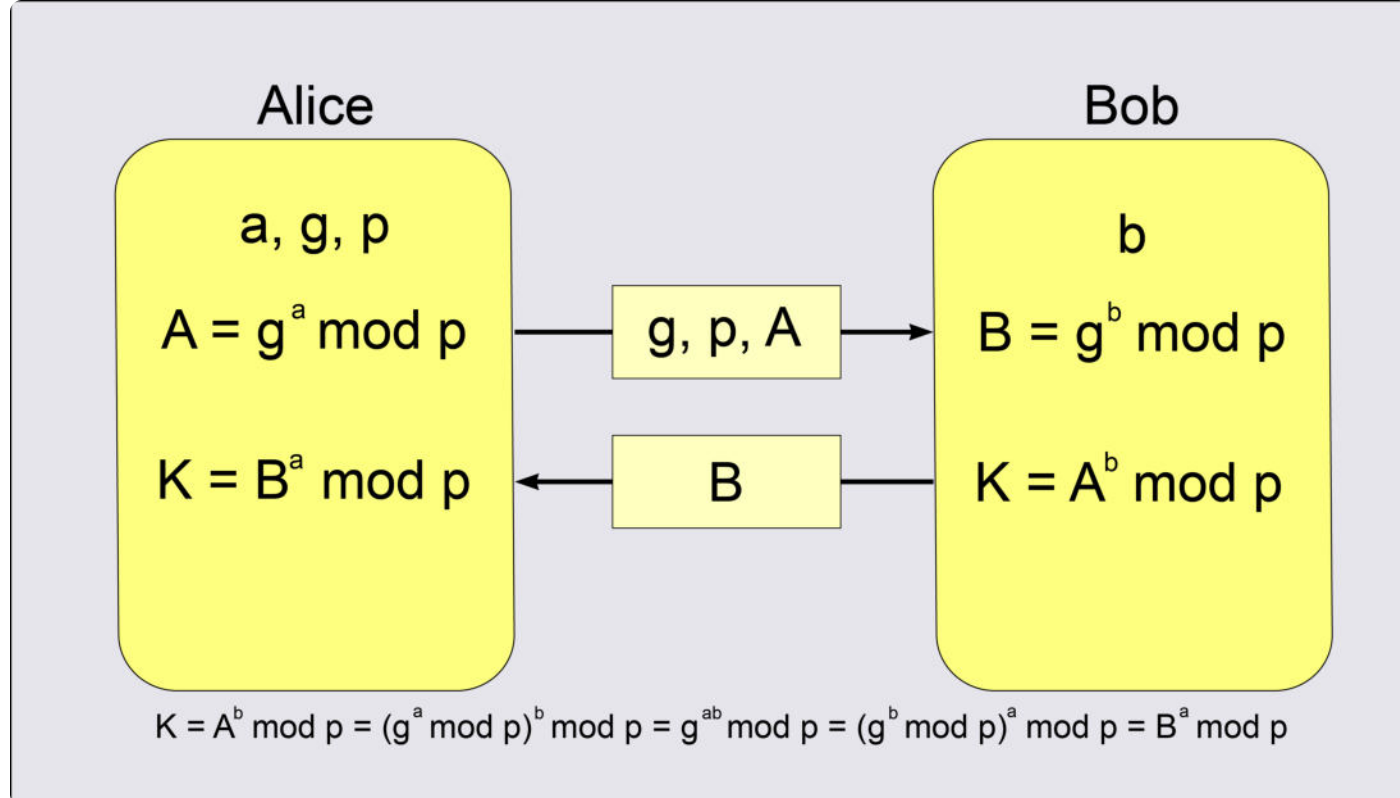
有了 DH 的私钥，Alice 和 Bob 再计算幂作为**公钥**，也就是 $A = (G^a \% P) = 9$ ， $B = (G^b \% P) = 14$ ，这里的 A 和 B 完全可以公开，因为根据离散对数的原理，从真数反向计算对数 a 和 b 是非常困难的。

交换 DH 公钥之后，Alice 手里有五个数： $P=17$ ， $G=5$ ， $a=10$ ， $A=9$ ， $B=14$ ，然后执行一个运算： $(B^a \% P) = 8$ 。

因为离散对数的幂运算有交换律， $B^a = (G^b)^a = (G^a)^b = A^b$ ，所以 Bob 计算 $A^b \% P$ 也会得到同样的结果 8，这个就是 Alice 和 Bob 之间的共享秘密，可以作为会话密钥使用，也就是 TLS 里的 Pre-Master。

领资料





那么黑客在这个密钥交换的通信过程中能否实现攻击呢？

整个通信过程中，Alice 和 Bob 公开了 4 个信息：P、G、A、B，其中 P、G 是算法的参数，A 和 B 是公钥，而 a 、 b 是各自秘密保管的私钥，无法获取，所以黑客只能从已知的 P、G、A、B 下手，计算 9 或 14 的离散对数。

由离散对数的性质就可以知道，如果 P 非常大，那么他很难在短时间里破解出私钥 a 、 b ，所以 Alice 和 Bob 的通信是安全的（但在本例中数字小，计算难度很低）。

实验环境的 URI“/42-1”演示了这个简单 DH 密钥交换过程，可以用浏览器直接访问，命令行下也可以用“resty www/lua/42-1.lua”直接运行。

DHE 算法

DH 算法有两种实现形式，一种是已经被废弃的 DH 算法，也叫 static DH 算法，另一种是现在常用的 DHE 算法（有时候也叫 EDH）。

static DH 算法里有一方的私钥是静态的，通常是服务器方固定，即 a 不变。而另一方（也就是客户端）随机选择私钥，即 b 采用随机数。

领资料



于是 DH 交换密钥时就只有客户端的公钥会变，而服务器公钥不变，在长期通信时就增加了被破解的风险，使得拥有海量计算资源的攻击者获得了足够的时间，最终能够暴力破解出服务器私钥，然后计算得到所有的共享秘密 Pre-Master，不具有“前向安全”。

而 DHE 算法的关键在于“E”表示的临时性上（ephemeral），每次交换密钥时双方的私钥都是随机选择、临时生成的，用完就扔掉，下次通信不会再使用，相当于“一次一密”。

所以，即使攻击者破解了某一次的私钥，其他通信过程的私钥仍然是安全的，不会被解密，实现了“前向安全”。

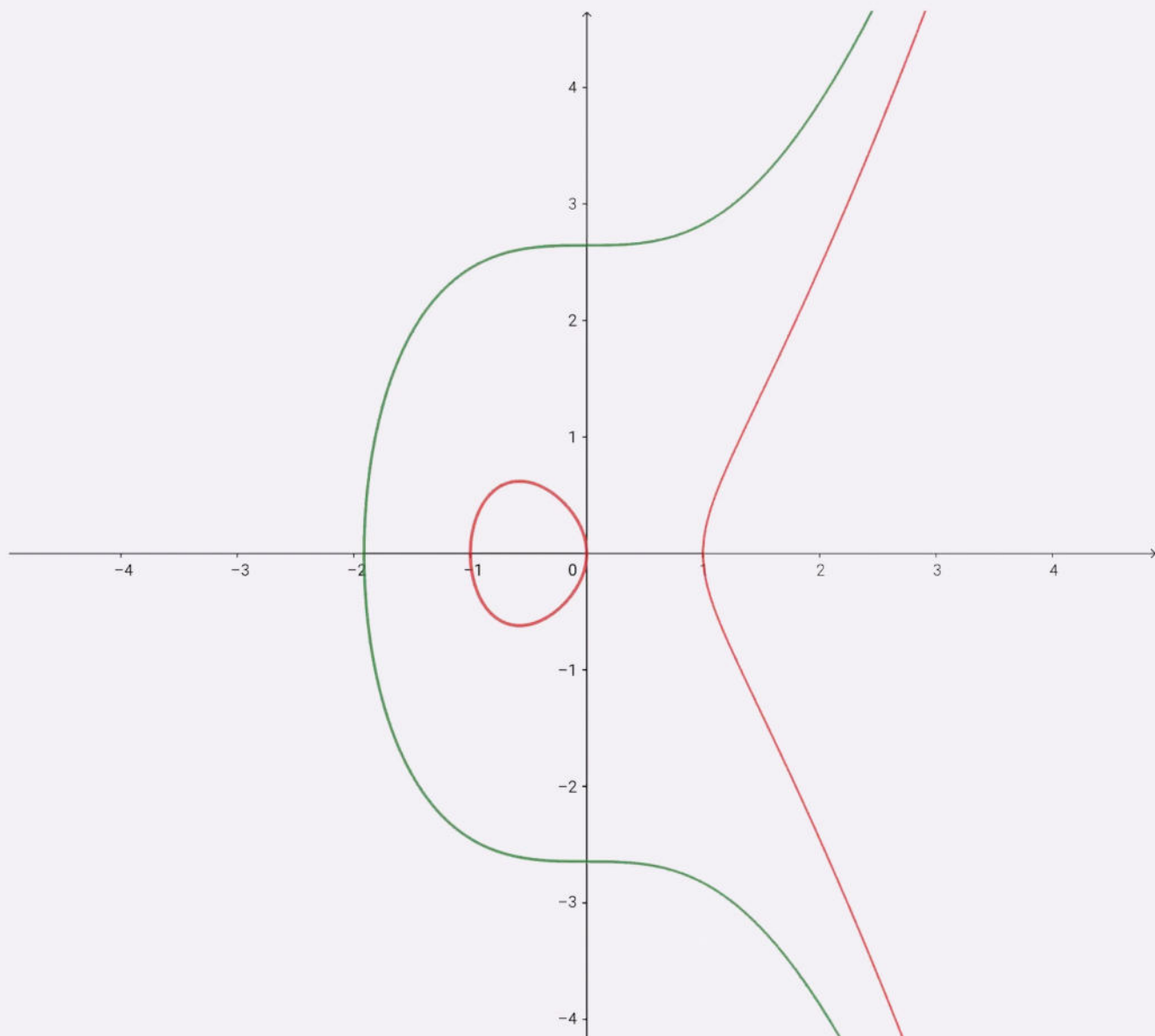
ECDHE 算法

现在如果你理解了 DHE，那么理解 ECDHE 也就不那么困难了。

ECDHE 算法，就是把 DHE 算法里整数域的离散对数，替换成了椭圆曲线上的离散对数。

领资料





原来 DHE 算法里的是任意整数，而 ECDHE 则是把连续的椭圆曲线给“离散化”成整数，用椭圆曲线上的“**倍运算**”替换了 DHE 里的幂运算。

在 ECDHE 里，算法的公开参数是椭圆曲线 C 、基点 G 和模数 P ，私钥是倍数 x ，公钥是倍点 xG ，已知倍点 xG 要想计算出离散对数 x 是非常困难的。

在通信时 Alice 和 Bob 各自随机选择两个数字 a 和 b 作为私钥，计算 $A=aG$ 、 $B=bG$ 作为公钥，然后互相交换，用与 DHE 相同的算法，计算得到 $aB=abG=Ab$ ，就是共享秘密 Pre-Master。

因为椭圆曲线离散对数的计算难度比普通的离散对数更大，所以 ECDHE 的安全性比 DHE 还要高，更能够抵御黑客的攻击。

领资料



最后留一个思考题吧：为什么 DH 算法只能用于密钥交换，不能用于数字签名，如果你理解了 DH 算法的原理应该不难回答出来。




课外小贴士

- 01 离散对数里对底数和模数有特殊要求，不是随便两个数就行的，底数必须是模数的“原根” (primitive root)，正文里没有过多介绍。
- 02 为了方便计算，DH 算法里的底数 G （术语叫生成元，generator）通常都很小，最常用的是 2，可以使用移位操作快速执行幂运算，可参考 RFC3526。
- 03 实验环境的脚本 42-1.lua 可以随意修改，变动 $P/G/a/b$ 来查看 DH 算法的效果， P/G 的取值可以是 (23, 7) (29, 3) (31, 11)。
- 04 使用传统计算机（冯诺依曼架构）很难计算离散对数，但量子计算机上已经出现了能够快速计算的算法（Shor's algorithm）。如果真能够

计算的算法（Shor's algorithm）。如果真能够开发出实用的量子计算机，那么 DHE/ECDHE 的安全性就会受到极大的挑战，现在正在研究可以替代 ECDH 的 SIDH（超奇异椭圆曲线同源密钥交换算法）。

分享给需要的人，Ta订阅超级会员，你将得 50 元

Ta单独购买本课程，你将得 20 元

 生成海报并分享

 赞 2  提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 41 | Linux/Mac实验环境搭建与URI查询参数

下一篇 43 | 如何进行Docker实验环境搭建？

领资料



JVM + NIO + Spring

各大厂面试题及知识点详解

限时免费



精选留言 (15)

写留言



djfhchdh

2020-03-25

DH算法只能用于密钥的交换，没有原文、摘要这些参数，无法生成数字签名。

作者回复: good。



5



许童童

2019-10-13

回答一下思考题：我觉得原因是,根据DH算法的原理，只能算出一个新的值出来用于交换密钥，而数字签名是需要解密数字证书得到数字签名，从而判断数字证书是否真实有效。DH是基于现有数据算出一个新值，公钥私钥算出的结果并不相同，RSA是对数据进行加解密。

作者回复: 有部分不太准确。

数字签名与证书没有直接关系。数字签名是对原文摘要的私钥加密，用对应的公钥解密后可以比对摘要，验证确实是私钥持有者做的加密，也就是签名。

证书是为了保证公钥不被伪造和有效性。

领资料



DH算法里没有原文、摘要这些参与者，所以无法生成签名。也就是说，给出一份文件或者摘要，dh算法无法对它进行任何操作。

共 2 条评论 >

👍 6



Geek_78044b

2020-09-23

老师你好，有个疑问。握手过程中的第三个参数，pre-master为何要用那么复杂的算法去避免破解呢？

我的理解是，第三个随机数是通过服务端的公钥加密后传输的，传递到服务端后，用服务端的私钥才能解密出来这个随机数。

黑客没有服务端的私钥，完全不可能破解pre-master的啊，为何要那么复杂的加密算法去生成这个pre-master？？？

作者回复: 如果用rsa算法，公钥加密pre-master，当然也是可以的，但这个不具有前向安全。国家级别的计算能力是有可能算出私钥的，这就会导致公钥加密的所有pre-master被解密，从而所有历史消息都被破解。可以参考安全篇对前向安全的解释。

而dhe和ecdhe不仅难以破解，而且密钥都是随机生成的，所以即使破解了也不影响其他消息的安全。



👍 1



猫头鹰波波

2020-02-08

老师，为什么ECDHE更难破解么，是因为离散的点选取更具备随机性吗

作者回复: 这是由椭圆曲线的特性决定的，具体的数学理论我也不是很了解，无法解释的更细。



👍 1



fxs007

2020-02-08

刚才看了下RSA验证签名的过程(<https://crypto.stackexchange.com/questions/12768/why-hash-the-message-before-signing-it-with-rsa>)，我觉得DH算法本身是可以用来验证数字签名。比如双方已经完成了DH密钥交换过程，
签名方发送 $\text{text} + \text{DH-enc}(\text{sha256}(\text{text}))$ ，其中 $\text{DH-enc}(\text{sha256}(\text{text}))$ 是对text进行hash算法然后DH加密

领资料



验证方 用DH-dec解密签名，然后和sha256(text)比较，相等就说明验证通过
只是DH一般用在双方确定身份以前，验证没有身份的签名并没有什么意义。

作者回复: 嗯，如果用变通的方法也是可以做到的，但意义不大，属于“曲线救国”。



1



Jasmine

2021-07-09

老师，等式 $B^a = (G^b)^a = (G^a)^b = A^b$ 左右两边就算忽略mod17值也不相等啊，为什么说经过运算都等于8呢？实际应用计算的底数超级大，给定了算法，数字运算的结果还是固定的呀，哪怕差0.00001那pre-master也不相同啊。困惑ing

作者回复: 这个是离散指数、对数在整数域的运算，不是普通的实数运算，可以照着正文里的例子再算一下。



张欣

2021-04-13

老师，不知道我理解的对不对：
根据文中以及之前tls文章的讲解，DH算法的主要目的就生成不可逆操作的公钥和私钥，然后再次执行算法生成两端相同的pre-master。这里面生成的公钥和私钥是可以拿来再次对文件摘要进行签名和验证，但是DH算法本身并没有这个作用。假设参数可以是文件摘要，就算算法能够算出，之后拿到证书的人也破解不开，根本没有意义。

作者回复: 理解有点偏差。

DH算法主要是用于密钥交换，生成的pre-master用来加密会话，一般不做签名验签。

签名算法常用的是RSA和ECDSA。

建议再回顾一下之前的课程，有不明白的或者我没说清楚的这问。

共 2 条评论 >



Ball

2021-01-06

原理完全没看懂，得花点时间消化一下了。

作者回复: 先把dh理解了，然后dhe和ecdhe就好懂了。

领资料





久念

2020-10-15

老师好，”国家级别的计算能力是有可能算出私钥的“ -- 如果私钥是可以被算出来的，那 Root CA 对应的私钥也有可能被破解，这样的话 黑客是不是就可以随意的颁发证书

作者回复: 是的，但这个的难度非常大。



djfhchdh

2020-03-24

因为DH算法，由公钥反向计算私钥是非常难的。

作者回复: 回答的不是太对，可参考其他同学的答案。



子杨

2020-02-23

对证书这块还是有点晕。证书应该只是用来证明站点的身份的吧？使用证书颁发机构的公钥对证书中的 hash 值进行解密，同时对 data 做 hash，如果相等就说明身份可信。

作者回复: 基本正确。

首先要理解公钥体系，理解签名。证书是为了安全可信地发布公钥。



Hills录

2020-02-20

DHE不能用于数字签名，是因为无法使用公钥验证私钥有效性

作者回复: 注意DHE和DH还是有区别的，DHE里的公私钥对都是临时产生的，显然无法签名，因为私钥用完就丢弃了，不会被任何人持有。

共 2 条评论 >



mark

领资料



2019-10-21

DH算法是选择一个数字作为私钥，hash好像不可逆，如果类似hash这样的算法，生成一个整数，是不是就可以用DH算法加密文本了。

作者回复: DH算法只能用于密钥交换，这种思路有点接近DSA算法。



饭团

2019-10-11

老师问题是不是是因为DH算法是动态的！即2个参数是相辅相成的，而数字签名中，公钥是不变的！

作者回复: 不是，可以再看一下dh算法的过程，它不能对一段文本的摘要做加密，无法生成签名，只能双方交换得到共享秘密。

共 3 条评论 >



饭团

2019-10-11

真棒老师，估计好多同学都不知道您更新了！谢谢您了！

作者回复: 是啊，好像缺少这个更新通知的功能。

共 2 条评论 >



领资料

