





一文看懂HTTPS、证书机构（CA）、证书、数字签名、私钥、公钥

 olaH 关注 IP属地: 浙江

 5 2019.07.27 11:39:07 字数 2,959 阅读 46,497

君问归期未有期

说到https，我们就不得不说tls/ssl，那说到tls/ssl，我们就不得不说证书机构（CA）、证书、数字签名、私钥、公钥、对称加密、非对称加密。这些到底有什么用呢，正所谓存在即合理，这篇文章我就带你们捋一捋这其中的关系。

对称加密

对称加密是指双方持有相同的密钥进行通信，加密速度快，但是有一个安全问题，双方怎样获得相同的密钥？你总不能总是拿着U盘把密钥拷贝给对方吧。
常见的对称加密算法有DES、3DES、AES等

非对称加密

非对称加密，又称为公开密钥加密，是为了解决对称加密中的安全问题而诞生，一个称为公开密钥(public key)，即公钥，另一个称为私钥(private key)，即私钥。但是它的加密速度相对于对称加密来说很慢。

- 公钥(public key)是对外开放的，私钥(private key)是自己拥有的。
- 公钥(public key)加密的数据，只能用私钥(private key)解密。
- 私钥(private key)加密的数据，只能用公钥(public key)解密。

信息安全问题

在信息安全性问题中，我们常常要做到三点才能保证信息的安全：

- 信息的保密性
- 信息的完整性
- 身份识别

信息的保密性（加密算法）

信息的保密性我们可以使用对称加密和非对称加密来完成，使用对称加密来完成，速度相对非对称加密很快，但是存在一个安全问题，密钥如何传递？由此通用的方法是使用非对称加密+对称加密来完成。客户端使用公钥对对称加密的密钥进行加密，然后传递给服务端，服务端使用私钥进行解密确认密钥，开始传输数据。

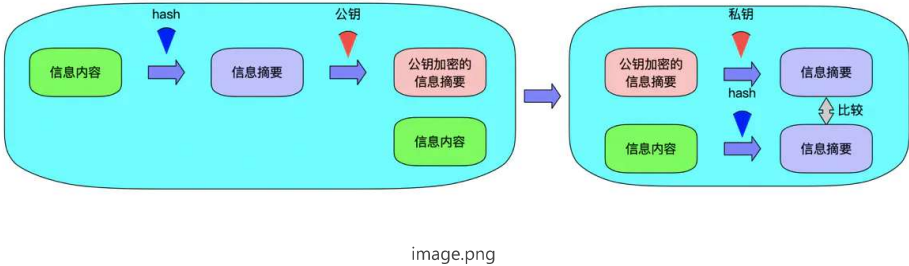
热门故事

- 母亲被迫净身出户，我却选择留下来，七年后当众让小姨母女一死一疯
- 我和网恋对象奔现，却发现他是我们学校赫赫有名的海王
- “今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”
- 完蛋了，我每天亲亲的网恋对象居然是校霸！
- 被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子
- 我首富之女的身份居然被人偷了
- 拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了
- 前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀
- 全校都在舔那个绿茶妹，没人知道我才隐藏大佬！
- 女儿满月那天，老公说他找到真爱了，让我放过他？！



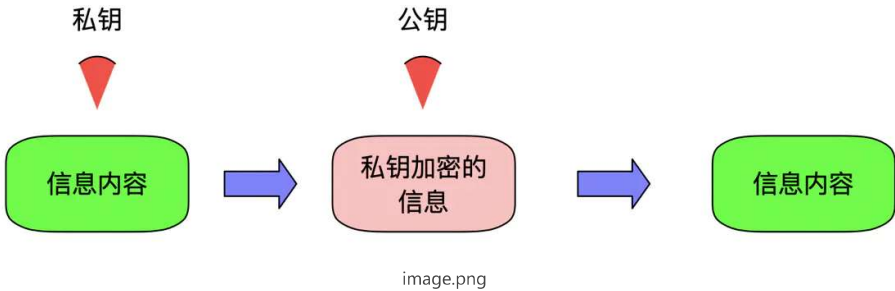
信息的完整性（数字签名）

信息传输的途中，我们的信息很有可能被第三方劫持篡改，所以我们需要保证信息的完整性，通用方法是使用散列算法如SHA1，MD5将传输内容hash一次获得hash值，即摘要。客户端使用服务端的公钥对摘要和信息内容进行加密，然后传输给服务端，服务端使用私钥进行解密获得原始内容和摘要值，这时服务端使用相同的hash算法对原始内容进行hash，然后与摘要值比对，如果一致，说明信息是完整的。



身份识别（数字证书）

在信息传输的过程中，我们通常需要验证信息的发送方的身份，这时我们转化一下思路就可以完成，把发送端的公钥发送给接收端，发送端通过把自己的内容使用私钥加密然后发送给接收端，接收端只能用发送端的公钥解密，自然就验证了发送端的身份。



数字证书

在传输的过程中，客户端如何获得服务器端的公钥呢？当时是服务器分发给客户端，如果一开始服务端发送的公钥到客户端的过程中有可能被第三方劫持，然后第三方自己伪造一对密钥，将公钥发送给客户端，当服务器发送数据给客户端的时候，中间人将信息进行劫持，用一开始劫持的公钥进行解密后，然后使用自己的私钥将数据加密发送给客户端，而客户端收到后使用公钥解密，反过来亦是如此，整个过程中间人是透明的，但信息泄露却不得而知。

热门故事

- 母亲被迫净身出户，我却选择留下来，七年后当众让小姨母女一死一疯
- 我和网恋对象奔现，却发现他是我们学校赫赫有名的海王
- “今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”
- 完蛋了，我每天亲亲的网恋对象居然是校霸！
- 被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子
- 我首富之女的身份居然被人偷了
- 拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了
- 前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀
- 全校都在舔那个绿茶妹，没人知道我才隐藏大佬！
- 女儿满月那天，老公说他找到真爱了，让我放过他？！

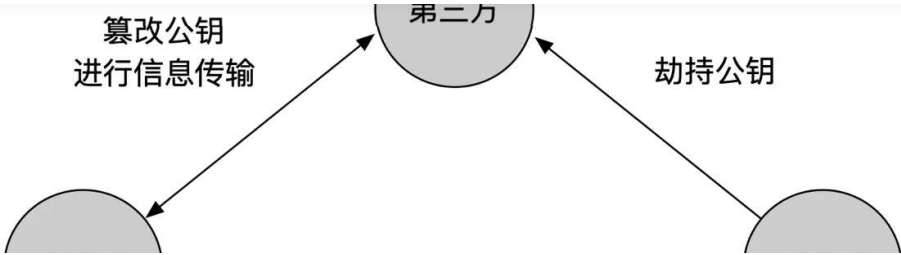


image.png

为了防止这种情况，数字证书就出现了，它其实就是基于上上面所说的私钥加密数据，公钥解密来验证其身份。

数字证书是由权威的CA（Certificate Authority）机构给服务端进行颁发，CA机构通过服务端提供的相关信息生成证书，证书内容包含了持有人的相关信息，服务器的公钥，签署者签名信息（数字签名）等，最重要的是公钥在数字证书中。

数字证书是如何保证公钥来自请求的服务器呢？数字证书上由持有人的相关信息，通过这点可以确定其不是一个中间人；但是证书也是可以伪造的，如何保证证书为真呢？

一个证书中含有三个部分：“证书内容，散列算法，加密密文”，证书内容会被散列算法hash计算出hash值，然后使用CA机构提供的私钥进行RSA加密。

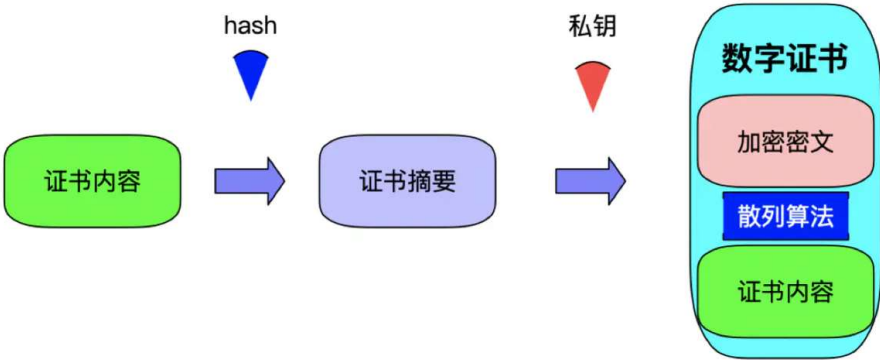


image.png

当客户端发起请求时，服务器将该数字证书发送给客户端，客户端通过CA机构提供的公钥对加密密文进行解密获得散列值（数字签名），同时将证书内容使用相同的散列算法进行Hash得到另一个散列值，比对两个散列值，如果两者相等则说明证书没问题。

热门故事

- 母亲被迫净身出户，我却选择留下来，七年后当众让小姨母女一死一疯
- 我和网恋对象奔现，却发现他是我们学校赫赫有名的海王
- “今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”
- 完蛋了，我每天亲亲的网恋对象居然是校霸！
- 被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子
- 我首富之女的身份居然被人偷了
- 拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了
- 前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀
- 全校都在舔那个绿茶妹，没人知道我才隐藏大佬！
- 女儿满月那天，老公说他找到真爱了，让我放过他？！



image.png

一些常见的证书文件类型如下：

- X.509#DER 二进制格式证书，常用后缀.cer .crt
- X.509#PEM 文本格式证书，常用后缀.pem
- 有的证书内容是只包含公钥（服务器的公钥），如.crt、.cer、.pem
- 有的证书既包含公钥又包含私钥（服务器的私钥），如.pfx、.p12

HTTPS，TLS/SSL

Hyper Text Transfer Protocol over Secure Socket Layer，安全的超文本传输协议，网景公式设计了SSL(Secure Sockets Layer)协议用于对Http协议传输的数据进行加密，保证会话过程中的安全性。

使用TCP端口默认为443

TLS：(Transport Layer Security，传输层安全协议)，用于两个应用程序之间提供保密性和数据完整性。

SSL：（Secure Socket Layer，安全套接字层），位于可靠的面向连接的网络层协议和应用层协议之间的一种协议层。SSL通过互相认证、使用数字签名确保完整性、使用加密确保私密性，以实现客户端和服务器之间的安全通讯。

SSL协议即用到了对称加密也用到了非对称加密(公钥加密)，在建立传输链路时，SSL首先对对称加密的密钥使用公钥进行非对称加密，链路建立好之后，SSL对传输内容使用对称加密。

对称加密

速度高，可加密内容较大，用来加密会话过程中的消息

公钥加密

加密速度较慢，但能提供更好的身份认证技术，用来加密对称加密的密钥

热门故事

母亲被迫净身出户，我却选择留下来，七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

“今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了

前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才是隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！

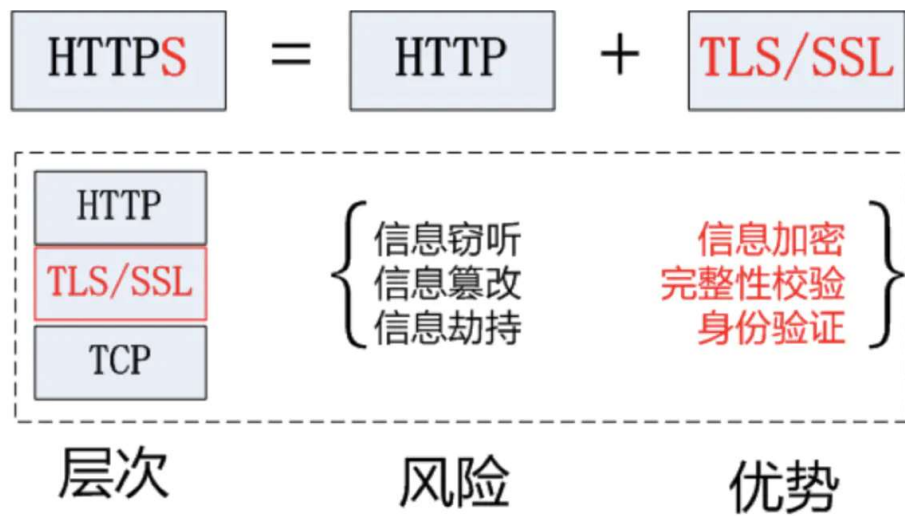


image.png

HTTPS 的构成

写下你的评论...

评论8

赞69

单向认证

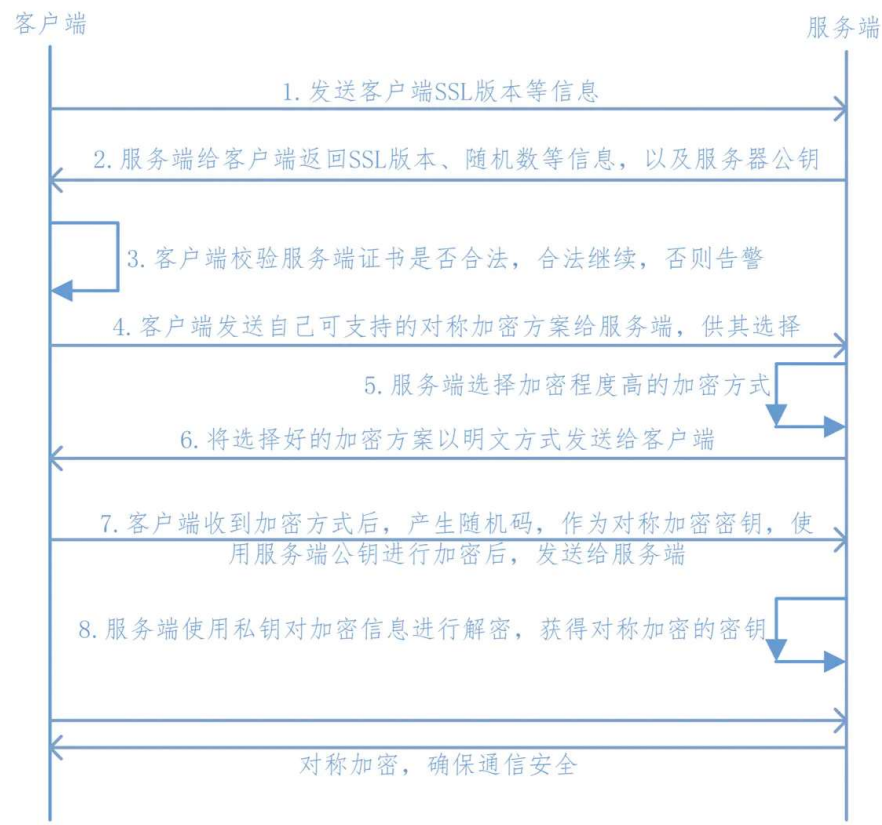


image.png

热门故事

母亲被迫净身出户，我却选择留下来，七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

“今日朕大婚，别让娘娘知道。”娘娘已经咽气了。”

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了

前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！

1. 客户端向服务端发送SSL协议版本号、加密算法种类、随机数等信息;
 2. 服务端给客户端返回SSL协议版本号、加密算法种类、随机数等信息，同时也返回服务器端的证书，即公钥证书;
 3. 客户端使用服务端返回的信息验证服务器的合法性，包括：
 - 证书是否过期;
 - 发行服务器证书的CA是否可靠;(通过查询浏览器或本机内的CA证书)
 - 返回的公钥是否能正确解开返回证书中的数字签名;(通过使用本机或浏览器内置的CA公钥进行解密)
 - 服务器证书上的域名是否和服务器的实际域名相匹配;
 - 验证通过后，将继续进行通信，否则，终止通信;
 4. 客户端向服务端发送自己所能支持的对称加密方案，供服务器端进行选择;
 5. 服务器端在客户端提供的加密方案中选择加密程度最高的加密方式;
 6. 服务器将选择好的加密方案通过明文方式返回给客户端;
 7. 客户端接收到服务端返回的加密方式后，使用该加密方式生成产生随机码，用作通过程中对称加密的密钥，使用服务端返回的公钥进行加密，将加密后的随机码发送至服务器;
 8. 服务器收到客户端返回的加密信息后，使用自己的私钥进行解密，获取对称加密密钥;
- 在接下来的会话中，服务器和客户端将会使用该密码进行对称加密，保证通信过程中信息的



双向认证和单向认证类似，它额外增加了服务端对客户端的认证：

双向认证

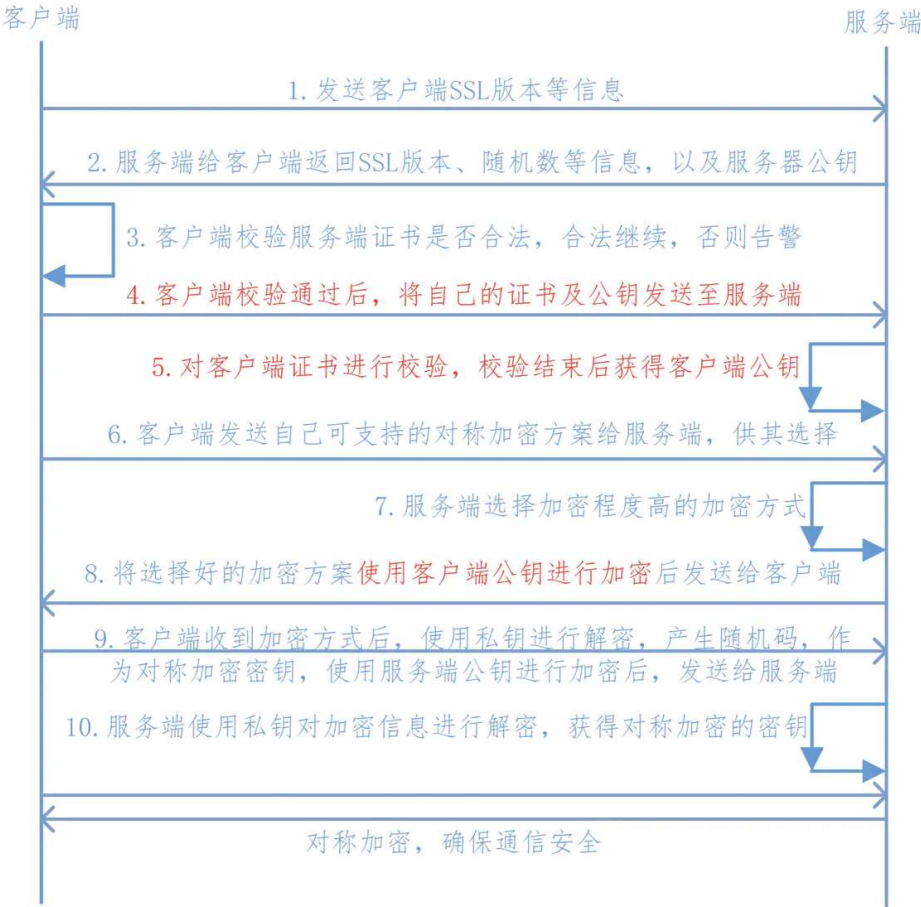


image.png

1. 客户端向服务端发送SSL协议版本号、加密算法种类、随机数等信息;
2. 服务端给客户端返回SSL协议版本号、加密算法种类、随机数等信息，同时也返回服务器端的证书，即公钥证书;
3. 客户端使用服务端返回的信息验证服务器的合法性，包括：
 - 证书是否过期;
 - 发行服务器证书的CA是否可靠;(通过查询浏览器或本机内的CA证书)
 - 返回的公钥是否能正确解开返回证书中的数字签名;(通过使用本机或浏览器内置的CA公钥进行解密)
 - 服务器证书上的域名是否和服务器的实际域名相匹配;
 - 验证通过后，将继续进行通信，否则，终止通信;
4. 服务端要求客户端发送客户端的证书即客户端证书公钥，客户端会将自己的证书发送至服务端;
5. 验证客户端的证书，通过验证后，会获得客户端的公钥;
6. 客户端向服务端发送自己所能支持的对称加密方案，供服务器端进行选择

热门故事

母亲被迫净身出户,我却选择留下来,七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

“今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了

前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！



9. 客户端收到服务端返回的加密方案密文后，使用自己的私钥进行解密，获取具体加密方式，而后，产生该加密方式的随机码，用作加密过程中的密钥，使用之前从服务端证书中获取到的公钥进行加密后，发送给服务端；
10. 服务端收到客户端发送的消息后，使用自己的私钥进行解密，获取对称加密的密钥，在接下来的会话中，服务器和客户端将会使用该密码进行对称加密，保证通过程中信息的安全；

69人点赞>

Computer Network

更多精彩内容，就在简书APP



"小礼物走一走，来简书关注我"

赞赏支持

共1人赞赏



olaH 很多人说的和做的不一样，我希望你不是
总资产8 共写了4.6W字 获得253个赞 共76个粉丝

关注

我和老婆认识20天闪婚，曾给我戴绿帽的前女友来砸场子

和清纯老婆闪婚的20天 我撞伤了一个老伯，不但没担责任，他还要把女儿嫁给我。没想到婚礼当天，曾被
我捉奸在床的前女...

茶点故事 阅读 15636 评论 2 赞 11

老同学找我借钱后, 把他的美艳妻子送上门来做"抵押"

放贷风波疫情爆发, 我和同学的妻子被封控在一起美艳人妻却不知, 我对她早已仰慕已久... 早几年的时候我
跟发小刘权开了个小...

沈念sama 阅读 1498 评论 0 赞 0

霸总老公为爱顶罪后我挖野菜求生

作者: 怀风

沈念sama 阅读 4350 评论 2 赞 4

泰国监狱里的中国女人

林欣蜷缩在监狱围墙里的一角，双眼无神地盯着另一边围墙上的铁丝网，几只小鸟正在上面盘旋着。她在里
面已经快呆了一个月...

以左a 阅读 726 评论 0 赞 7

演金丝雀太入戏，他还真以为我爱上他了

写下你的评论...

评论8

赞69

热门故事

母亲被迫净身出户, 我却选择留下来, 七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

"今日朕大婚，别让娘娘知道。""娘娘已经咽气了。"

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了


前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！


被骗去柬埔寨的人有多惨? 器官被明码标价, 男人的待遇像皇帝

我曾亲眼目睹近百具死婴尸体,都被挖了眼睛和内脏,悬挂在铁丝上风干,最后磨成粉.....我叫曹文静,今年25岁, ...

 沈念sama 阅读 918 评论 0 赞 2

连续离婚三次后，寡妇独自创办养驴厂，把驴当成丈夫一样细心伺候.....

寡妇与驴 我曾处理过一桩骇人听闻的案件，一个寡妇跟一头驴死在了她家的小院里。死前这一人一驴都服用过某种药物，而且...

 沈念sama 阅读 411 评论 0 赞 1


我在陵园发现了男友给我立的墓碑，还有闺蜜、同学，甚至他自己

我的男朋友很帅很帅，温柔体贴，但是他和闺蜜上了床。还在陵园给我立了一个碑。恐怖的是，我男朋友自己的墓碑就在我...

 茶点故事 阅读 2035 评论 0 赞 3

听到我随口哄骗的话，皇帝竟红了眼：你说你仰慕我，可是真的？

被退婚后，我嫁给了当朝新帝。本只想在后宫低调度日，却不料新帝是个恋爱脑。放着家世优越的皇后和貌美如花的贵妃不要...

 沈念sama 阅读 227 评论 0 赞 4

男子监狱发生内乱，唯一的女医生成了他们的斗争工具

1、美女医生进监狱 疫情刚开始的那年，我和护士小白，被紧急调到西城监狱支援防控。这里是男子监狱，那些囚犯很多都是...

 茶点故事 阅读 1956 评论 0 赞 1


因为我妈，一万块，我就能让人随便玩

我在学生会的时候，拉赞助，被合作方领导骚扰。这事还被人撞见，传了出去。而我妈听见了这些闲话，气势汹汹地杀来。 ...

 茶点故事 阅读 2388 评论 0 赞 1

喝避子汤被皇上当场抓包，“爱妃在喝什么？”“回皇上，十全大补汤。”

我吃了整整三年的避子药，因为怀过皇嗣的妃嫔都死了，无一例外。三年前帝后大婚，洞房花烛的第二天早上我就毅然决然饮下了...

 沈念sama 阅读 204 评论 0 赞 1


女儿满月那天，老公说他找到真爱了，让我放过他

我跟我前夫在商场里面给小孩买衣服，他现在的老婆不停地给他打电话。前夫没办法，只能撒谎说自己在公司开会。对方听清...

 茶点故事 阅读 3571 评论 0 赞 0

男性催乳师

我是一名男催乳师，新顾客竟是母亲的闺蜜。她竟邀请我与她丈夫三人同睡..... 1 我是一名男催乳师。一个备受争...

 Elverano 阅读 336 评论 0 赞 1

我和网恋对象提分手，正打架的校霸突然哭了

《网恋社死现场》一、面基当天，我把谈了三个月的网恋对象拉黑了。事情是这样的。那天我刚上完早课，叼了个冰棒走...

热门故事

母亲被迫净身出户,我却选择留下来,七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

“今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了

前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！



学生找上我，说愿...

茶点故事 阅读 1117 评论 0 赞 3

皇帝醉酒后认错人，竟对着白月光贵妃念出了我的名字

皇帝的白月光自尽了，我却瞧着他一点也不伤心。那日我去见贵妃最后一面，却惊觉她同我长得十分相似。回宫后我的头就开...

茶点故事 阅读 651 评论 0 赞 0

小姨抢走我爸爸，十年后，我盛装回归，抢走她女婿

谁能想到有朝一日，逼宫这种事会发生在我身边。被逼走的是我亲妈，始作俑者是我亲小姨。为了争得我的抚养权，母亲放弃...

茶点故事 阅读 835 评论 0 赞 2

春雨暮

我被心上人灌下晕药，送到了新科状元的床上。一年后的雨水，我被人毒死，扔进枯井之中。死前，我竟然听到了撕心裂肺的...

今天也要睡饱 阅读 18741 评论 10 赞 160

被以下专题收入，发现更多相似内容

- Java
- 云与网络
- 网络相关
- 转载部分
- 小程序
- iOS程序猿
- 微信小程序开发 展开更多

推荐阅读

更多精彩内容

数字证书原理,公钥私钥加密原理

原文地址：数字证书原理,公钥私钥加密原理 文中首先解释了加密解密的一些基础知识和概念，然后通过一个加密通信过程的例...

淇滨杜隆坦 阅读 3,963 评论 4 赞 46

网络通信分享（一）:数字签名，数字证书，https通信，数据加密

网络通信分享（一）:数字签名，数字证书，https通信，数据加密 加密算法：一：对称加密算法 在对称加密算法中，...

雷3雷 阅读 1,605 评论 0 赞 12

数字证书原理,公钥私钥加密原理

原文地址：不详 文中首先解释了加密解密的一些基础知识和概念，然后通过一个加密通信过程的例子说明了加密算法的作用，...

Caiaolun 阅读 1,218 评论 0 赞 3

数字证书原理，以及协作签名原理

前言 文中首先解释加密解密的一些基础知识和概念，然后通过一个加密通信过程的例子说明了加密算法的作用，以及数字证书的...

sunny冲哥 阅读 2,581 评论 0 赞 2

热门故事

母亲被迫净身出户,我却选择留下来,七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

“今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了

前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！



sunny冲哥 阅读 1,214 评论 0 赞 3

热门故事

母亲被迫净身出户,我却选择留下来,七年后当众让小姨母女一死一疯

我和网恋对象奔现，却发现他是我们学校赫赫有名的海王

“今日朕大婚，别让娘娘知道。”“娘娘已经咽气了。”

完蛋了，我每天亲亲的网恋对象居然是校霸！

被祖母下药不得已嫁进门，我娘冷笑着接回了一个私生子

我首富之女的身份居然被人偷了

拿校草当挡箭牌气心机闺蜜和前男友，没想到校草当真了

前世渣男把我迷晕还叫我别怕，转世彻底黑化的我复仇反杀

全校都在舔那个绿茶妹，没人知道我才隐藏大佬！

女儿满月那天，老公说他找到真爱了，让我放过他？！

