这是第二行阿斯顿这是一个简单的输入测试这是一个简单的输入测试这是第二行阿斯顿这是一个简单的输入测试这是一个简单的输入asdfdfvbgsdfgkjnDIAKJoifjskshenmeDLFHAGSDSJBljsdfbasjdb11dc01293847358735692347069457638516049738534698265934570234674这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试这是一个简单的输入测试

agjygvasdaksudfgaoseufsvkjlcbvkjxcbvkjvbsmdncb<mcvbhsdiufygweoifuysgufyddvksozIZjoIZjajsnkJGAVXHGcVWUEDYGiuaSHLIuhlIUBJHvnghfedmscjg difuhsidudhkvjfldsuhfsd sdv sdvhsdusdhf sdfsdfhlieufh sdlfsiuerbfjhwnbnr ybny rtjhrybjrhtvrgk liufvhldfiuvdgf vidflviegwefpqodq sidugaiugdequehfvssdvhiygkuygkugVHGCJGFcuyg usdcusydckgdvhdgfvhjjjjjjjjjjjjjjjvvvvvvvvvvvvv dskeiugvkjhvgixcuvyoziuvherjhfbrjthfvbkauyvgdfyvadfvidfuvh

公开密钥密码学（英语：Public-key cryptography）也称非对称式密码学（英语：Asymmetric cryptography）是密码学的一种算法，它需要两个密钥，一个是公开密钥，另一个是私有密钥；公钥用作加密，私钥则用作解密。使用公钥把明文加密后所得的密文，只能用相对应的私钥才能解密并得到原本的明文，最初用来加密的公钥不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。公钥可以公开，可任意向外发布；私钥不可以公开，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给被信任的要通信的另一方。

基于公开密钥加密的特性，它还能提供数字签名的功能，使电子文件可以得到如同在纸本文件上亲笔签署的效果。

公开密钥基础建设透过信任数字证书认证机构的根证书、及其使用公开密钥加密作数字签名核发的公开密钥认证，形成信任链架构，已在TLS实现并在万维网的HTTP以HTTPS、在电子邮件的SMTP以SMTPS或STARTTLS引入。

另一方面，信任网络则采用去中心化的概念，取代了依赖数字证书认证机构的公钥基础设施，因为每一张电子证书在信任链中最终只由一个根证书授权信任，信任网络的公钥则可以累积多个用户的信任。PGP就是其中一个例子。

概述

加密

非对称加密往往需要密码学安全伪随机数生成器的协助来产生一对密钥，其中一个可以随便公开，称为公钥；另一个不公开，称为私钥，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供。

如果任何人使用公钥加密明文，得到的密文可以透过不安全的途径（如网络）发送，只有对应的私钥持有者才可以解密得到明文；其他人即使从网络上窃取到密文及加密公钥，也无法（在数以年计的合理时间内）解密得出明文。典型例子是在网络银行或购物网站上，因为客户需要输入敏感消息，浏览器连接时使用网站服务器提供的公钥加密并上传数据，可保证只有信任的网站服务器才能解密得知消息，不必担心敏感个人信息因为在网络上传送而被窃取。

在现实世界上可作比拟的例子是，一个传统保管箱，开门和关门都是使用同一条钥匙，这是对称加密；而一个公开的邮箱，投递口是任何人都可以寄信进去的，这可视为公钥；而只有信箱主人拥有钥匙可以打开信箱，这就视为私钥。

加密过程

在非对称加密中，爱丽丝使用鲍伯的公钥加密明文，得到密文，而只有鲍伯因为持有私钥才可以解密，得到明文。

在数学上，

�

(

�

(

�

)

)

=

�

{\displaystyle d(c(x))=x}，使用典型的爱丽丝与鲍伯假设来解释：

爱丽丝与鲍伯事先互不认识，也没有可靠安全的沟通渠道，但爱丽丝现在却要透过不安全的互联网向鲍伯发送信息

爱丽丝撰写好原文，原文在未加密的状态下称之为明文

�

x

鲍伯使用密码学安全伪随机数生成器产生一对密钥，其中一个作为公钥为

�

c，另一个作为私钥

�

d

鲍伯可以用任何方法发送公钥

�

c 给爱丽丝，即使伊夫（窃听者）在中间窃听到

�

c 也没问题

爱丽丝用公钥

�

c 把明文

�

x 进行加密，得到密文

�

(

�

)

{\displaystyle c(x)}

爱丽丝可以用任何方法传输密文

�

(

�

)

{\displaystyle c(x)} 给鲍伯，即使伊夫在中间窃听到密文

�

(

�

)

{\displaystyle c(x)} 也没问题

鲍伯收到密文，用私钥d 对密文进行解密 (()){\displaystyle d(c(x))}，得到爱丽丝撰写的明文

x

由于伊夫没有得到鲍伯的私钥

d，所以无法得知明文

如果爱丽丝丢失了她自己撰写的原文

x，在没有得到鲍伯的私钥

d 的情况下，她的处境将等同伊夫，即无法透过鲍伯的公钥

c 和密文 (){\displaystyle c(x)}重新得到原文

x

数字签名

相反，如果某一用户使用他的私钥加密明文，任何人都可以用该用户的公钥解密密文；由于私钥只由该用户自己持有，故可以肯定该文件必定出自于该用户；公众可以验证该用户发布的数据或文件是否完整、中途有否曾被篡改，接收者可信赖这些数据、文件确实来自于该用户，这被称作数字签名，大部分国家已经立法承认数字签名拥有等同传统亲笔签名的法律效力。公钥可以透过数字证书认证机构签授的电子证书形式公布，接收者透过信任链形成一套完整的公开密钥基础建设。例如，从网上下载的安装程序，大部分都带有程序制作者的数字签名，可以证明该程序的确是该作者（公司）发布的而不是第三方伪造的且未被篡改过（身份认证/验证）。而现时的网上银行或购物网站都会使用HTTPS，避免沟通过程中的信息泄露。

《史记》最初没有固定书名，或称《太史公书》，或称《太史公记》，也省称《太史公》。“史记”本来是古代史书的通称，从三国开始，“史记”由通称逐渐成为“太史公书”的专名。《史记》是一部贯穿古今的通史，从传说中的黄帝开始，一直写到汉武帝元狩元年，叙述了中国三千年左右的历史。全书有本纪十二篇，表十篇，书八篇，世家三十篇，列传七十篇，共一百三十篇。班固在《汉书·司马迁传》中提到《史记》缺少十篇。三国魏张晏指出这十篇是《景帝本纪》、《武帝本纪》、《礼书》、《乐书》、《律书》、《汉兴以来将相年表》、《日者列传》、《三王世家》、《龟策列传》、《傅靳列传》。后人大多数不同意张晏的说法，但《史记》残缺是确凿无疑的。今本《史记》也是一百三十篇，有少数篇章显然不是司马迁的手笔，汉元帝、成帝时的博士褚少孙补写过《史记》，今本《史记》中“褚先生曰“就是他的补作。《史记》取材相当广泛。当时社会上流传的《世本》、《国语》、《国策》、《秦记》、《楚汉春秋》、诸子百家等著作和国家的文书档案，以及实地调查获取的材料，都是司马迁写作《史记》的重要材料来源。特别可贵的是，司马迁对搜集的材料做了认真地分析和选择，淘汰了一些无稽之谈。对一些不能弄清楚的问题，或者采用阙疑的态度，或者记载各种不同的说法。由于取材广泛，修史态度严肃认真，所以，《史记》记事翔实，内容丰富。

《千字文》原名為《次韻王羲之書千字》，南朝梁（502年─549年）周興嗣所作的一首長韻文。它是一篇由一千個不重複的漢字組成的文章。據說是梁武帝取了王羲之寫的一千個字體，令其親人練習書法，而後覺得雜亂無章，於是又命周興嗣（470年─521年）編為一tes 篇文章。[1]

《千字文》全篇主題清晰，章句文理一脈相承，層層推進，語言優美，詞藻華麗，幾乎是句句引經，字字用典。出典包括《易經》、《淮南子》、《詩經》、《尚書》、《禮記》、《春秋》、《論語》、《孝經》、《孟子》、《史記》、《神農本草經》、《管子》、《韓非子》、《莊子》、《漢書》。[2]《千字文》以儒家思想為主體，兼納自然、歷史、社會常識，寓意深刻、結構清晰、語言簡明優美，可以說是一首四言長詩。是用來教授兒童基本漢字之重要啓蒙讀物，和《三字經》、《百家姓》、《千家诗》合稱“三百千千”[3][4]。《千字文》是其他幾篇也公認為不錯的訓蒙讀物不能比的。所以歷代書法家都競相書寫，如智永、懷素、歐陽詢、趙佶、趙孟頫、文徵明等都有留傳至今的帖本。同時在漢字文化圈各國也受到重視。

創造背景

中國很早就出現專門用於啟蒙的識字課本，秦代出現的有倉頡篇爰歷篇漢代則有司馬相如的凡將篇賈魴的滂喜篇蔡邕的勸學篇史游的急就章三國時代有埤蒼廣蒼始學篇等這些作品中只有急就章影響後世，其餘影響不大急就章雖是倉頡篇之後較為突出的小學之書，但流傳中出現種種問題，其權威性到南北朝時已大不如前，這一時期出現的啟蒙讀物如庭誥詁幼之類，可讀性有限千字文就是在這樣的背景下問世。

三國時期的書法家鍾繇曾寫過一篇《千字文》，但毀於西晉的動亂之中。王羲之又重新編綴過一篇，但文理音韻皆不佳。李倬《尚書故實》记载梁武帝為教育子侄，命大臣殷鐵石模次王羲之書碣碑石的字跡，又要求拓出互不重複的一千個字，以賜八王。殷铁石拓出後，此千餘字互不聯屬，梁武帝又命令周兴嗣将这一千字编成有意义的句子，“卿有才思，為我韻之。”周興嗣竟一夜编成。[5]