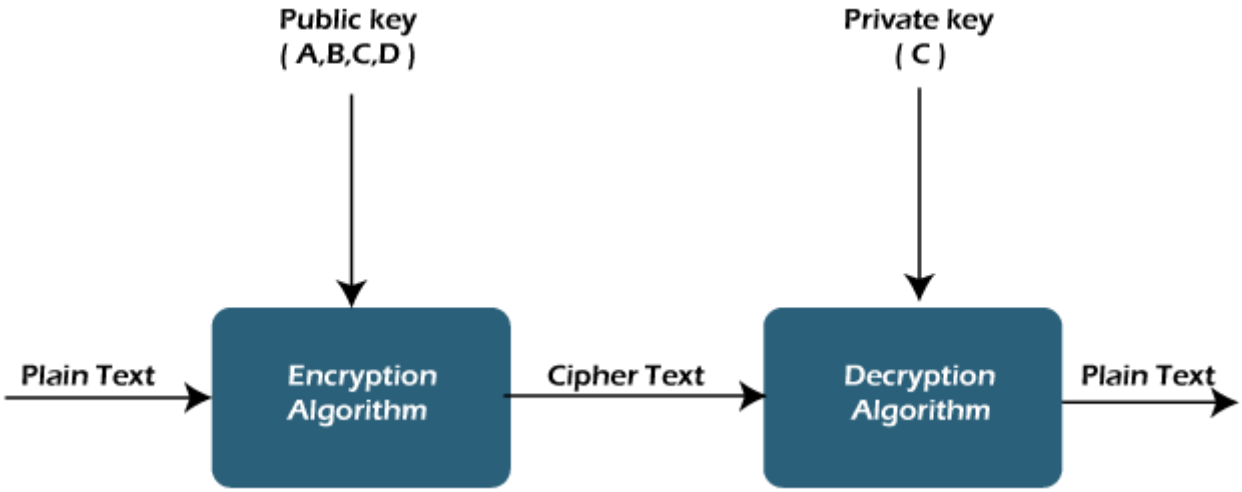
公钥和私钥的区别

在本文中，我们将讨论公钥、私钥以及它们的区别。 私钥和公钥这两个术语通常用于加密和解密。因此，了解这两个键以及它们的区别非常重要。

公钥

它是一种使用一对密钥(公钥和私钥)进行安全数据通信的加密技术。 在这对密钥中，公钥用于对明文进行加密以将其转换为密文，而私钥用于对密文进行解密以读取消息。
将私钥提供给接收者，而将公钥提供给公众。 公钥密码术也称为非对称密码术。
可以共享公钥而不损害私钥的安全性。 所有非对称密钥对都是唯一的，因此使用公钥加密的消息只能由拥有相应私钥的人阅读。 该对中的密钥比对称密码学中使用的密钥长得多。 因此，很难从其公共对应物中破译私钥。 我们中的许多人都听说过 RSA，这是当今使用的最常见的非对称加密算法。



公钥加密比密钥加密慢。 在密钥加密中，使用单个共享密钥来加密和解密消息，而在公钥加密中，使用不同的两个密钥，它们通过复杂的数学过程相互关联。 因此，我们可以说加密和解密在公钥加密中花费了更多的时间。

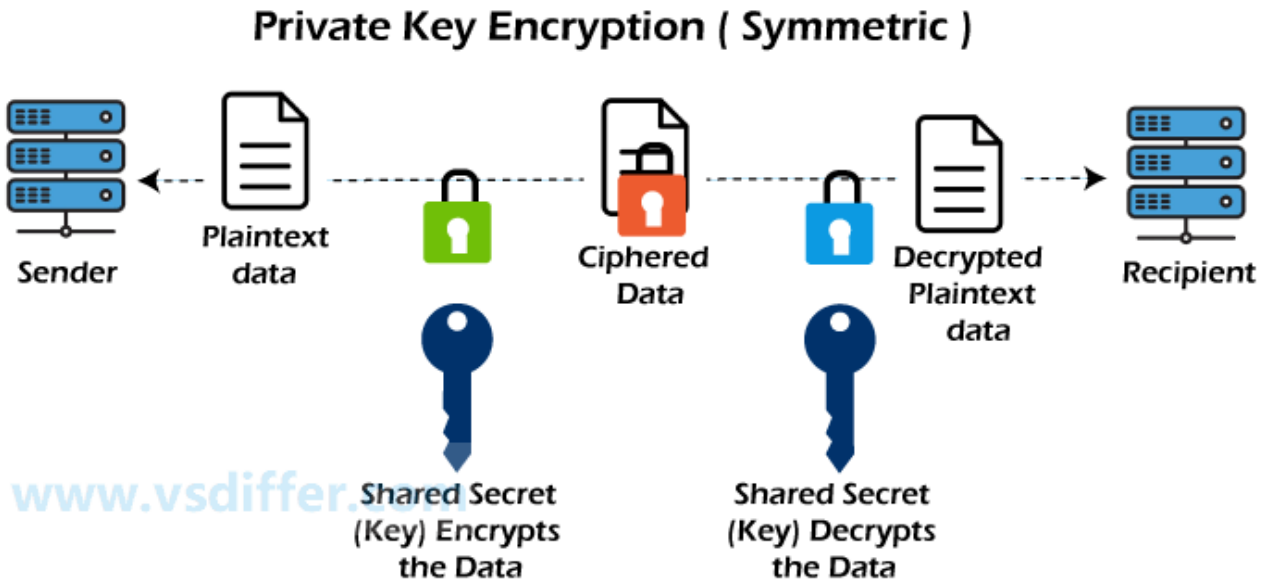
公钥的应用
公钥的应用是 -

- 公钥加密可用于加密电子邮件以保持其内容的机密性。
- 非对称加密或公钥加密也用于安全套接字层 (SSL) 协议，以建立与网站的安全连接。
- 公钥也用于区块链和密码技术。 例如，生成一对密钥，同时设置一个新的加密货币钱包。

- 它可用于在 Ubuntu、Red Hat Linux 软件包分发等操作系统软件中创建数字签名。

私钥

在私钥中，双方（即发送方和接收方）使用相同的密钥（或秘密密钥）进行加密/解密技术。
发送方使用密钥和加密算法进行加密，而对于解密，接收方使用此密钥和解密算法。 在密钥加密/解密技术中，用于加密的算法与用于解密的算法相反。 这意味着如果加密算法中使用了加法和乘法的组合，那么解密算法将使用减法和除法的组合。



密钥加密算法也称为对称加密算法，因为双向通信使用相同的密钥。 私钥机制比公钥密码机制更快。 这样做的原因是密钥的大小很小。

公钥与私钥

这是关于公钥和私钥的描述。让我们看看这两个键之间的比较图表 -

比较项目	公钥	私钥
定义	它被定义为使用两个不同的密钥进行加密和解密的技术。它被定义为使用单个共享密钥（秘密密钥）来加密和解密消息的技术。也称为非对称密钥加密。	它也被称为对称密钥加密。这是因为双向通信中使用了相同的密钥。
效率	由于这种技术仅用于短消息，因此效率低下。	它很有效，因为建议将这种技术用于大量文本。
速度	因为它使用两个不同的键，所以速度较慢；这两个键通过复杂的数学过程相互关联。	它更快，因为它使用单个密钥进行加密和解密 VSdIfFer。

比较项目	公钥	私钥
秘密	它是免费使用的。	除了发送者和接收者之外，私钥是保密的，不向任何人公开。
目的	公钥算法的主要目的是安全地共享密钥。	密钥算法的主要目的是传输大量数据。
密钥丢失	密钥丢失的可能性较小，因为密钥是公开持有的。	有可能丢失使系统无效的密钥。

相关主题

- AVG Android安全性和NetQin Android安全性 (https://www.vsdiffer.com/avg-android-security-vs-netqin-android-security.html)
- McAfee全面保护和Internet安全 (https://www.vsdiffer.com/mcafee-total-protection-vs-internet-security.html)
- McAfee防病毒和互联网络安全 (https://www.vsdiffer.com/mcafee-antivirus-vs-internet-security.html)
- 加密和散列 (https://www.vsdiffer.com/encryption-vs-hashing.html)
- 加密和未加密 (https://www.vsdiffer.com/encrypted-vs-unencrypted.html)
- 卡巴斯基反病毒软件和Internet安全 (https://www.vsdiffer.com/kaspersky-antivirus-vs-internet-security.html)
- 卡巴斯基安全软件和卡巴斯基反病毒软件 (https://www.vsdiffer.com/kaspersky-internet-security-vs-kaspersky-antivirus.html)
- 安全与隐私的区别 (https://www.vsdiffer.com/security-vs-privacy.html)
- 对称加密和非对称加密的区别 (https://www.vsdiffer.com/symmetric-encryption-vs-asymmetric-encryption.html)
- 联网安全和网络安全 (https://www.vsdiffer.com/cyber-security-vs-network-security.html)
- iOS和Android的区别 (https://www.vsdiffer.com/ios-vs-android.html)

随机

- 尼康D3100和D5100 (https://www.vsdiffer.com/nikon-d3100-vs-d5100.html)
- COUNT和COUNTA (https://www.vsdiffer.com/count-vs-counta.html)
- 狼和豺狼的区别 (https://www.vsdiffer.com/wolf-vs-jackal.html)
- HashMap和Hashtable (https://www.vsdiffer.com/hashmap-vs-hashtable.html)
- .Net Core和.Net Framework的区别 (https://www.vsdiffer.com/dot-net-core-vs-dot-net-framework.html)
- Canon HF10和Canon HF100 (https://www.vsdiffer.com/canon-hf10-vs-canon-hf100.html)
- Quicktime和Windows Media Player (https://www.vsdiffer.com/quicktime-vs-windows-media-player.html)
- 主动运输和被动运输 (https://www.vsdiffer.com/active-vs-passive.html)
- JSON和XML的区别 (https://www.vsdiffer.com/json-vs-xml.html)
- Python yield和Python return (https://www.vsdiffer.com/python-yield-vs-python-return.html)
- Redis和MongoDB的区别 (https://www.vsdiffer.com/redis-vs-mongodb.html)
- EOS 450D和尼康D80 (https://www.vsdiffer.com/eos-450d-vs-nikon-d80.html)

最新更新
公共部门与私营部门的区别 (https://www.vsdiffer.com/public-sector-vs-private-sector.html)
蛋白质和脂肪的区别 (https://www.vsdiffer.com/protein-vs-fat.html)
兔子和野兔的区别 (https://www.vsdiffer.com/rabbit-vs-hare.html)
种族与民族 (https://www.vsdiffer.com/race-vs-ethnicity.html)
RAM和ROM的区别 (https://www.vsdiffer.com/ram-vs-rom.html)
生奶和巴氏杀菌奶的区别 (https://www.vsdiffer.com/raw-milk-vs-pasteurized-milk.html)
大鼠和小鼠的区别 (https://www.vsdiffer.com/rat-vs-mice.html)
RDBMS和HBase的区别 (https://www.vsdiffer.com/rdbms-vs-hbase.html)
递归和迭代的区别 (https://www.vsdiffer.com/recursion-vs-iteration.html)
Aerospike和Redis的区别 (https://www.vsdiffer.com/aerospike-vs-redis.html)
Redis和Elasticsearch的区别 (https://www.vsdiffer.com/redis-vs-elasticsearch.html)

Redis和Memcached的区别 (https://www.vsdiffer.com/redis-vs-memcached.html)

Redis和MongoDB的区别 (https://www.vsdiffer.com/redis-vs-mongodb.html)

Redis和RDBMS的区别 (https://www.vsdiffer.com/redis-vs-rdbms.html)

Redis与其他键值对存储的区别 (https://www.vsdiffer.com/redis-vs-other-key-value-stores.html)

关系数据库与NoSQL数据库 (https://www.vsdiffer.com/relational-vs-nosql-database.html)

可再生资源和不可再生资源的区别 (https://www.vsdiffer.com/renewable-vs-non-renewable-

核糖体和溶酶体的区别 (https://www.vsdiffer.com/ribosomes-vs-lysosomes.html)

RISC和CISC的区别 (https://www.vsdiffer.com/risc-vs-cisc.html)

河流和湖泊的区别 (https://www.vsdiffer.com/river-vs-lake.html)

岩石与矿物的区别 (https://www.vsdiffer.com/rocks-vs-minerals.html)

根和茎之间的区别 (https://www.vsdiffer.com/roe-vs-caviar.html)

自转与公转的区别 (https://www.vsdiffer.com/rotation-vs-revolution.html)

路由器和网关的区别 (https://www.vsdiffer.com/router-vs-gateway.html)

行与列的区别 (https://www.vsdiffer.com/row-vs-column.html)

Ruby和Python的区别 (https://www.vsdiffer.com/ruby-vs-python.html)

RPC和Document Web服务的区别 (https://www.vsdiffer.com/difference-between-rpc-vs-

销售与营销的区别 (https://www.vsdiffer.com/sales-vs-marketing.html)

沙子和土壤的区别 (https://www.vsdiffer.com/sand-vs-soil.html)

Sass和SCSS的区别 (https://www.vsdiffer.com/sass-vs-scss.html)

蝾螈和蜥蜴的区别 (https://www.vsdiffer.com/salamander-vs-lizard.html)

苏格兰威士忌和威士忌的区别 (https://www.vsdiffer.com/scotch-vs-whiskey.html)

优点和缺点

充气饮料的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-aerated-

腺样体切除的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-removing-

马来西亚留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

澳大利亚的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

荷兰留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

美国留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

日本留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

加拿大留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

印度留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-cons-studying-in-india.html)

瑞士留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

新加坡留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

阿根廷留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-studying-in-

英国留学的优点和缺点 (https://www.vsdiffer.com/proscons/pros-cons-studying-in-uk.html)

橡子的优点和缺点 (https://www.vsdiffer.com/proscons/acorns-advantages-and-

狗鹿角磨牙棒的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-antlers-for-

强生疫苗的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-johnson-and-

增强现实的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-augmented-

吸脂的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-liposuction.html)

网络中立的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-net-

守望者(Watchman)设备的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-

绝缘车库的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-insulating-

Linx手术的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-linx-surgery.html)

可穿戴技术的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-wearable-

电子图书馆的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-e-libraries.html)

早起的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-waking-up-early.html)

买房的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-buying-house.html)

针灸的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-acupuncture.html)

小睡的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-power-naps.html)

私人健身教练的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-hiring-a-

深呼吸练习的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-deep-

跑步机的优点和缺点 (https://www.vsdiffer.com/proscons/pros-and-cons-of-treadmill.html)

保健品的好处和坏处 (https://www.vsdiffer.com/proscons/pros-and-cons-of-health-

关于Hasdiffer

有区别（Hasdiffer）致力于为用户提供事物的比较区别，优点和缺点，好处和坏处，以及对比选择哪个好等等。我们将不断更新文章，以提高质量和正确性。

最新文章

Bootstrap 4 和 Bootstrap 5 框架的区别
React和Svelte的区别 (/article/39879)
物理文件系统和逻辑文件系统的区别
操作系统中共享内存和消息传递的区别
德尔塔和Mu变体的区别 (/article/39800)
命名空间和类的区别 (/article/39753)
基于进程和基于线程的多任务处理的区别
SQL中简单视图和复杂视图的区别

最新项目

马来西亚留学的优点和缺点 (/proscons/pros-
澳大利亚的优点和缺点 (/proscons/pros-and-
荷兰留学的优点和缺点 (/proscons/pros-and-
美国留学的优点和缺点 (/proscons/pros-and-
日本留学的优点和缺点 (/proscons/pros-and-
加拿大留学的优点和缺点 (/proscons/pros-and-
印度留学的优点和缺点 (/proscons/pros-cons-
新加坡留学的优点和缺点 (/proscons/pros-and-

最新下载

Marketing
Visual Assistant

关于网站

关于我们
Find Developers

System Analysis

Advertise

团队

Advertise

API