网络攻防实战

第1周

陈健

chenj@nju.edu.cn

课程简介

- 课程名称-《网络攻防实战》
- 教学目标
  - **培养学生对网络安全领域的兴趣**
  - 通过实验进一步巩固和加深对计算机网络安全、信息安全基本概念的理解与掌握
  - 掌握网络渗透攻击实战所需要的基本能力
  - 掌握安全漏洞的独立分析、挖掘与验证所需要的基本能力

助教团队（trinity战队）

- 梁瀚中
- 王润川
- 李骁

战绩

- defcon china qual第一
- SEC-T ctf全球第五
- 全国高校网安联赛第六
- 护网杯决赛
- 。。。。。。

刑法中关于计算机犯罪相关条款

- 第285条－(非法侵入计算机信息系统罪)
  - 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。
- 第286条－(破坏计算机信息系统罪)
  - (1) 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。
  - (2) 违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。
  - (3) 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。
- 第287条－(利用计算机实施的各类犯罪)
  - 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

刑法修正案-285条

- 2009年2月刑法修正案(七)，十号主席令
- 285条增加两款
  - 侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。
  - 提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚
  - 拓展法律保护的范围，加强了惩罚力度

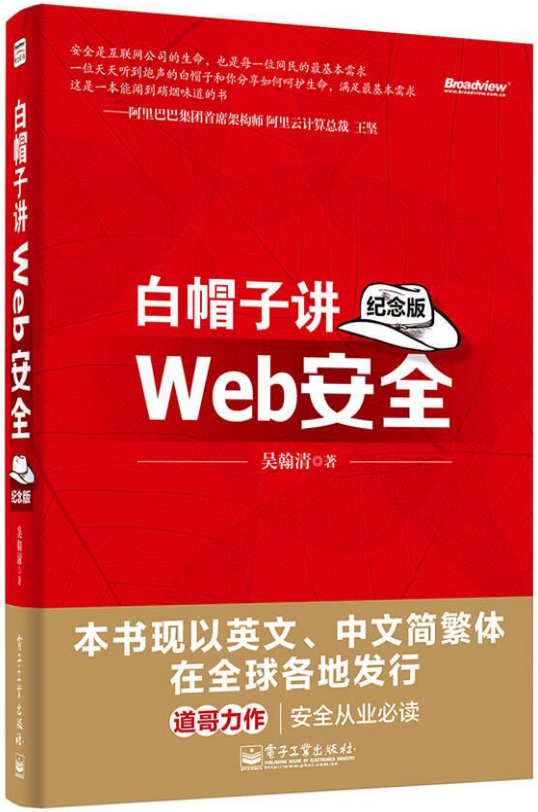
网络安全法

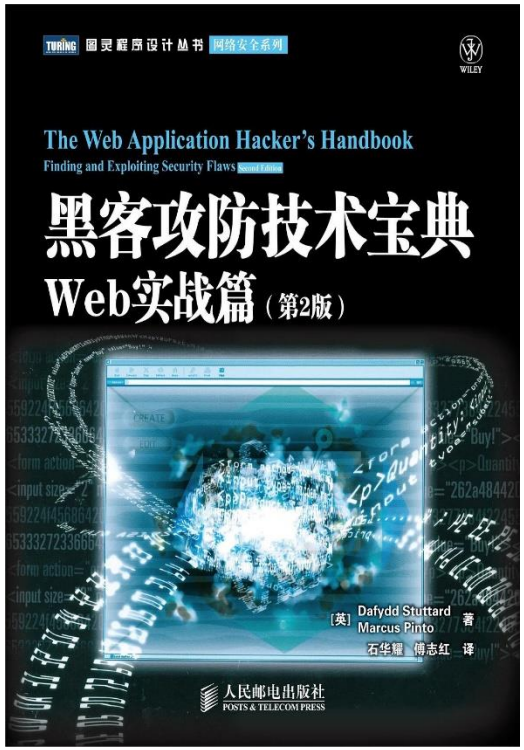
- 我国第一部全面规范网络空间安全管理方面问题的基础性法律
- 2017年6月1日起正式施行

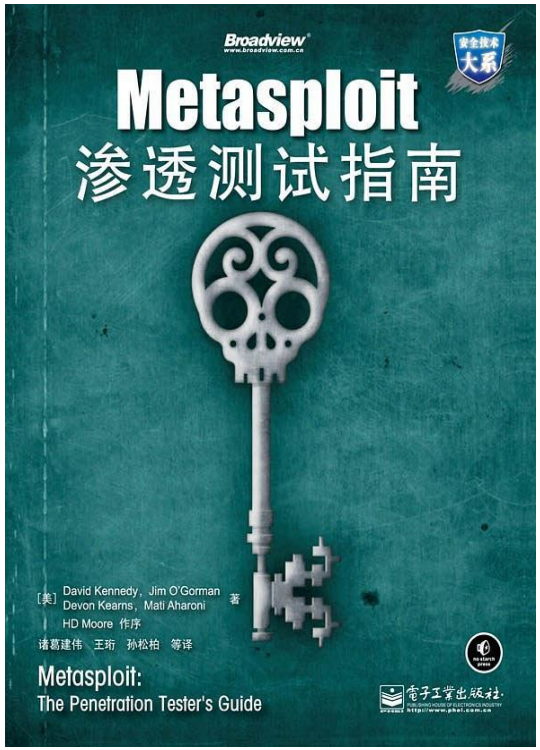
怎么学习网络安全

对于安全入门来说，宽度比深度更重要！

安全入门书籍


安全是互联网公司的生命，也是每一位网民的最基本需求
一位天天听到泡声的白帽子和你分享如何呵护生命，满足最基本需求
这是一本能闻到硝烟味道的书
——阿里巴巴集团首席架构师 阿里云计算总裁 王坚
Broadview
白帽子讲Web安全
白帽子讲 Web安全
纪念版
吴翰清 著
本书现以英文、中文简繁体
在全球各地发行
道哥力作 | 安全从业必读
電子工業出版社


TURING 图灵程序设计丛书 网络安全系列
WILEY
The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws Second Edition
黑客攻防技术宝典
Web实战篇（第2版）
[英] Dafydd Stuttard
Marcus Pinto 著
石华耀 傅志红 译
人民邮电出版社
POSTS & TELECOM PRESS


Broadview
安全技术大系
Metasploit
渗透测试指南
[美] David Kennedy, Jim O'Gorman
Devon Kearns, Mati Aharoni 著
HD Moore 作序
诸葛建伟 王珩 孙松柏 等译
Metasploit:
The Penetration Tester's Guide
電子工業出版社

进阶练习

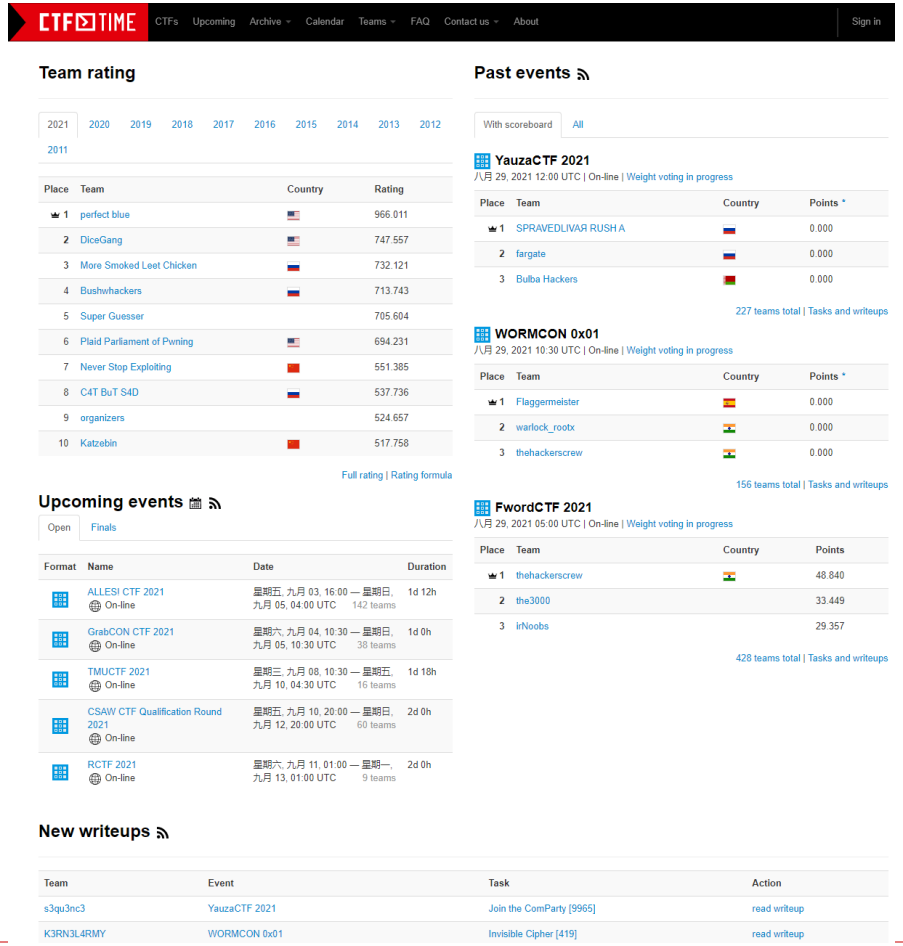
- WebGoat
  - https://owasp.org/www-project-webgoat/
- pwnable.kr
- CTF比赛
  - https://www.xctf.org.cn/
  - ctftime.org

CTF夺旗赛简介

- CTF（Capture The Flag）夺旗赛是网络安全领域中网络安全技术人员之间进行技术竞技的一种比赛形式
  - 起源于1996年DEFCON全球黑客大会
- 竞赛模式
  - 解题模式（Jeopardy）
    - 题目主要包含六个类别：RE逆向工程、Pwn漏洞挖掘与利用、Web渗透、Crypto密码学、Mobile移动安全和Misc安全杂项
  - 攻防模式（Attack-Defense）
  - 混合模式（Mix）

网络安全竞赛简介

- ctftime.org



网络安全竞赛简介

- DEFCON CTF
  - 起源于1996年DEFCON全球黑客大会
  - 全球最有影响力的黑客竞赛 –“黑客世界杯”
  - 1996年开始，已成功举办25届
  - 2015：blue-lotus、Oops、HITCON：4-6
  - 2016：bl0Op：2 PPP：1
  - 2017：HITCON：2 A*0*E：3 PPP：1
  - 2018：DEFKOR00t：1 PPP：2 HITCON：3
  - 2019: PPP：1 HITCON：2 A*0*E：4
  - 2020：A*0*E: 1 PPP: 2 HITCON: 3
  - 2021：Katzebin：1 Plaid：2 Tea Deliverers：3

DEFCON CTF 拉斯维加斯决赛现场

网络安全竞赛简介

- Pwn2Own
  - 黑客界的奥林匹克
- CGC
  - 旨在推进自动化网络攻防技术的发展
- XCTF联赛
- 全国大学生信息安全竞赛
- 强网杯全国网络安全挑战赛
- HITCON CTF
- 0CTF/TCTF

网络安全会议简介

- RSA
  - 网络安全行业的风向标
- DEFCON
  - 由Jeff Moss于1993年在拉斯维加斯发起
- Black Hat
  - 由Jeff Moss于1997年创办
- 中国互联网安全大会ISC
  - 亚太地区规格最高、规模最大、最有影响力的安全会议之一

网络安全学术会议简介

- CCS
  - ACM Conference on Computer and Communication Security
- NDSS
  - Network and Distributed System Security Symposium
- Oakland S&P
  - IEEE Symposium on Security & Privacy
- USENIX
  - USENIX Security Symposium

安全证书

证书	特点	难度	安全方向
CISP	国内安全证书之首	中	公司防御
CISSP	国际上含金量最高的安全证书之一，安全管理者会考	高	公司防御
OSCP	攻击渗透方向上非常实用的证书	高	攻击渗透

安全资讯

- FreeBuf
  - https://www.freebuf.com/
- 安全客
  - https://www.anquanke.com/
- 安全牛
  - https://www.aqniu.com/

网络安全是什么

- 任何应用最本质的东西就是数据
- 网络安全的本质就是保护数据被合法地使用
  - 如何保证数据被合法地使用
    - CIA三元组

CIA三元组


Integrity
完整性
Information Security
CIA三元组
Confidentiality
机密性
Availability
可用性

CIA：机密性

- 确保数据只被授权的主体访问，不被任何未授权的主体访问，即**不可见**
- 明确授权规则
- 数据的存储、传输和处理过程需要保护
  - 加密、隔离、混淆、隐藏等
- 针对机密性的攻击方式
  - 针对保护技术进行破解
  - 人为原因导致的疏忽
- 当前机密性保护的要点是引导人去做正确的事情，避免看似低级、实则普遍的漏洞发生
  - 权限滥用
  - 弱密钥
  - 。 。 。

CIA：完整性

- 确保数据只被授权的主体进行授权的修改，即**不可改**
  - 所谓“授权的修改”，就是对主体可进行的操作进行进一步的限制
  - 强调对修改行为的日志记录，并有合适的监督机制进行审计
- 完整性和机密性是紧密相连的。因此，大部分的机制和技术都同时对完整性和机密性提供保护

CIA：可用性

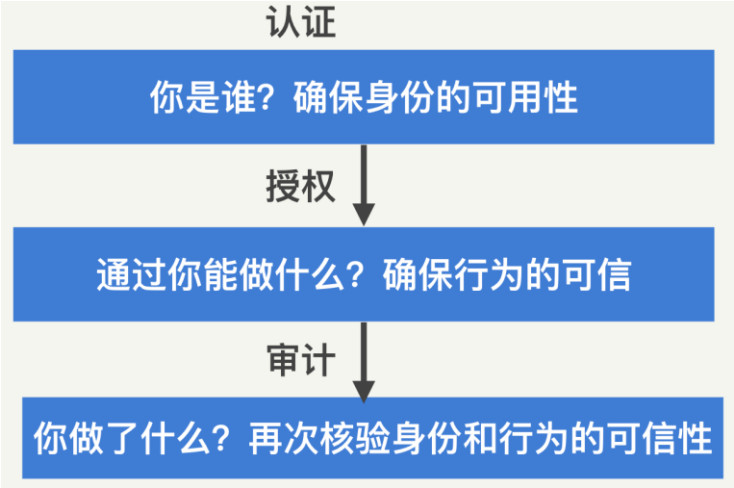
- 确保数据能够被授权的主体访问到，即**可读**
- 确保授权机制能够正确运行，使得拥有访问数据权限的主体能够及时地被授权，这是可用性的基本
  - 运维层面：机房建设、多地冗余、服务备份、资源冗余等
  - 研发层面：降低响应延迟、处理海量数据等
  - 攻击角度：DoS攻击

CIA三元组的取舍

- 根据不同的发展阶段，列好CIA的优先级，是建设安全体系首先要做的事情
- 互联网企业发展初期
  - 可用性的优先级较高
    - 涉及金钱相关的业务，完整性的优先级更高
    - 涉及个人隐私相关的业务，机密性的优先级更高
- 互联网企业发展后期
  - 可用性投入降低，而完整性和机密性投入会越来越大

黄金法则

- 黄金法则主要包含三部分：认证（Authentication）、授权（Authorization）、审计（Audit）
  - 加上问责（Accounting），组成“4A 法则”
  - 加上身份识别（Identification），组成“IAAAA 法则”



黄金法则：身份识别和认证

- 身份识别和认证通常是同时出现的一个过程
  - 身份识别强调的是主体如何声明自己的身份
  - 身份认证强调的是主体如何证明自己所声明的身份是合法的
- 认证形式（由弱到强）
  - 你知道什么（密码、密保问题等）
  - 你拥有什么（门禁卡、安全令牌等）
  - 你是什么（生物特征，指纹、人脸、虹膜等）
- 可信的身份认证是建立安全保障体系的第一步

黄金法则：授权

- 你能做什么、你能做多少
- 自动化的授权机制
  - 自主访问控制
  - 强制访问控制

黄金法则：审计和问责

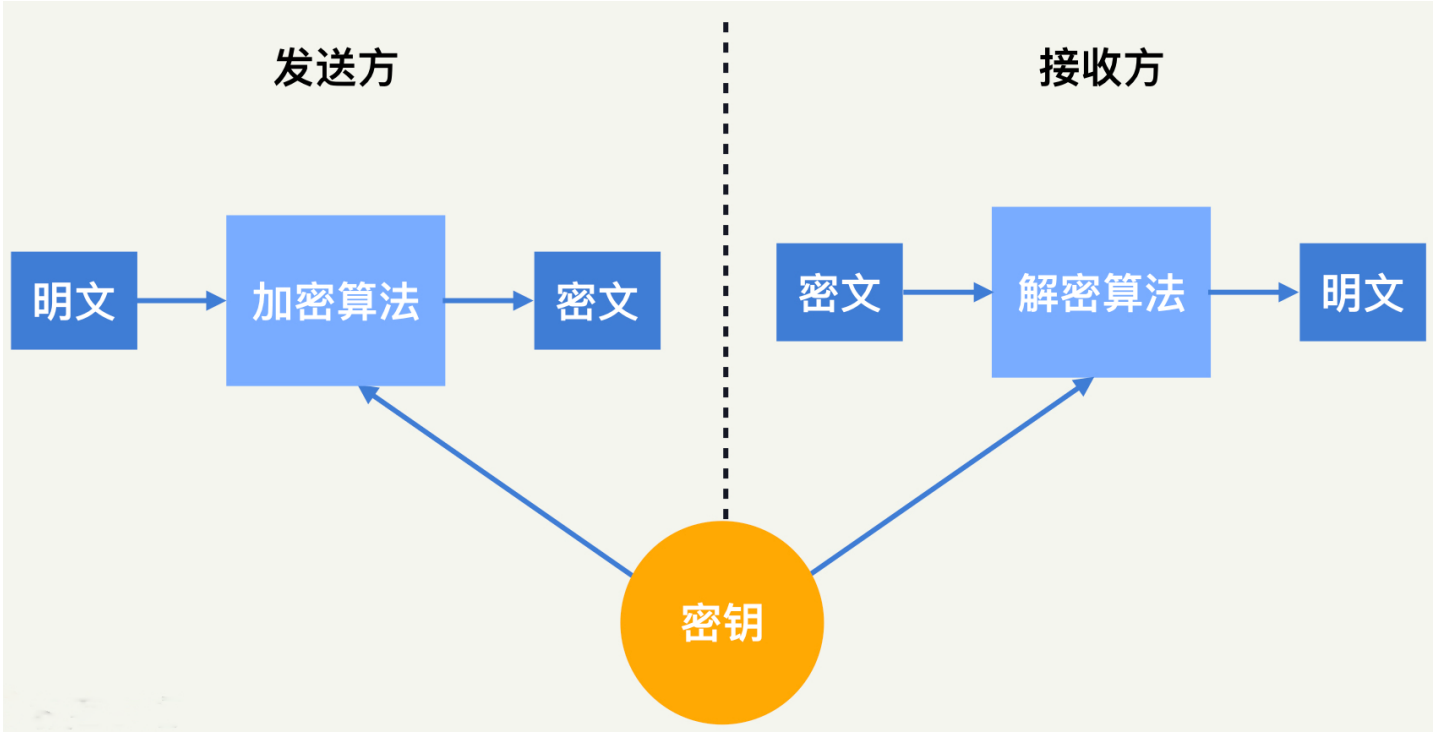
- 当你在授权下完成操作后，安全需要检查“你做了什么”，这个检查的过程就是**审计**。当发现你做了某些异常操作时，安全还会提供你做了这些操作的“证据”，这个过程就是**问责**
- 审计和问责通常是共同出现的一个过程，因为它们都需要共同的基础：**日志**
  - 审计通过日志还原出用户的操作历史
  - 问责通过日志的完整性，确保日志还原出来的操作是可信的
- 事前防御属于认证，事中防御属于授权，事后防御属于审计

黄金法则总结

- 所有的安全保护措施或者工具，都是在黄金法则的一个或者多个模块中进行工作
- 安全应严格遵从“木桶原理”，只专注于某一个方向必然无法产出最优的结果
- 安全没有“银弹”，不要过分追求完美

密码学基础：对称加密算法

- 加密和解密使用的是同一个密钥



密码学基础：经典对称加密算法

- DES
  - 数据加密标准，Data Encryption Standard
  - 最早的现代密码学算法之一。它由美国政府提出，密钥长度为56位
  - 已过时，目前不推荐使用
  - S盒的秘密
- IDEA
  - 国际数据加密算法，International Data Encryption Algorithm
  - 由瑞士研究人员设计，密钥长度为128位。IDEA的优势在于没有专利的限制

密码学基础：经典对称加密算法

- AES
  - 高级加密标准，Advanced Encryption Standard
  - 美国政府推出，提供了128位、192位和256位三种密钥长度
  - 国际上最认可的密码学算法。在算力没有突破性进展的前提下，AES在可预期的未来都是安全的
- 国密SM1和SM4
  - SM1算法不公开，属于国家机密，只能通过相关安全产品进行使用
  - SM4属于国家标准，算法公开，可自行实现使用

密码学基础：经典对称加密算法对比

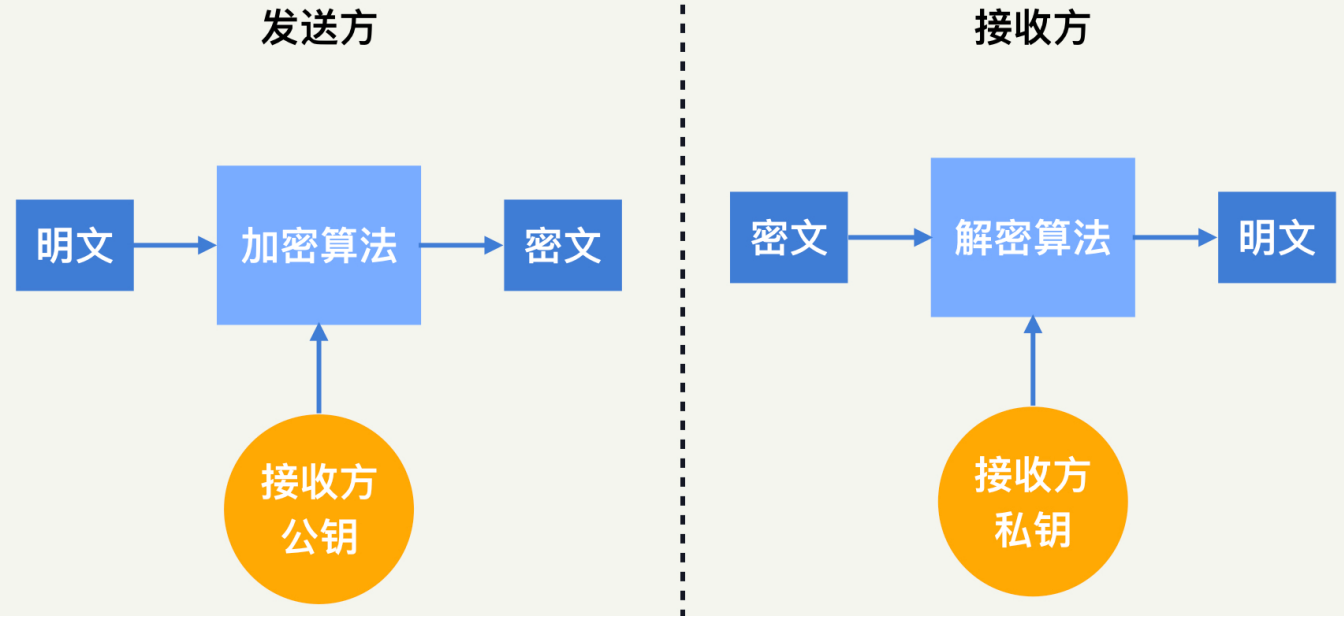
	密钥长度	加密强度	性能	版权
DES	56	弱	快	美国
3DES	168	中	慢	美国
IDEA	128	强	中	瑞士
AES	128、192、256	强	快	美国
SM1	128	强	未测试	中国（算法保密）
SM4	128	强	未测试	中国（算法公开）

对称加密算法的应用

- 在加密通信中（如HTTPS、VPN、SSH 等），通信双方会协商出一个加密算法和密钥，对传输的数据进行加密
- 存储加密技术中，通信双方将存储空间中的数据进行加密
- 公司通常选取AES128进行加解密运算
- 有合规需求，则需应用国密算法
- 加密算法的分组计算模式
  - 选取CBC和CTR这两种模式可以满足大部分需求

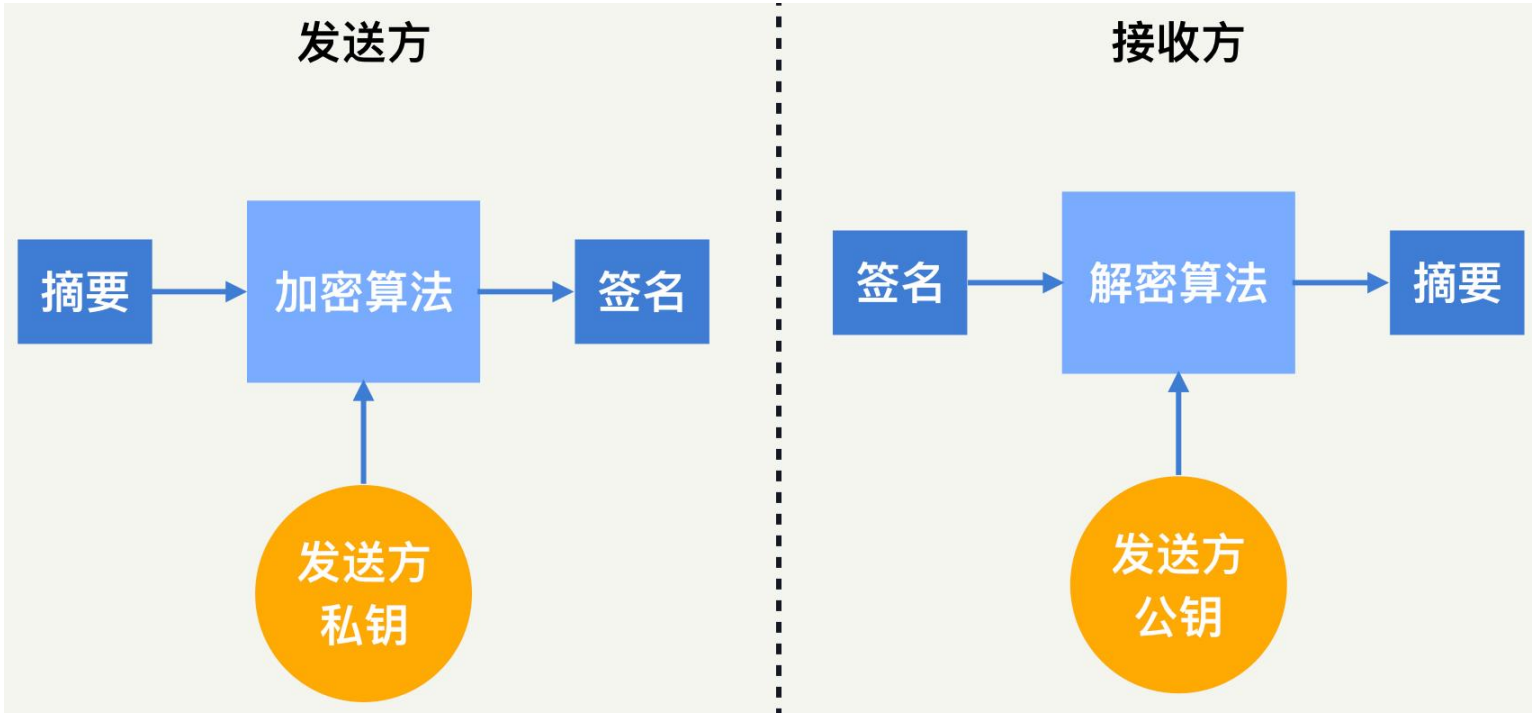
密码学基础：非对称加密算法

- 加密和解密使用不同的密钥
  - 发送方使用公钥对信息进行加密，接收方收到密文后，使用私钥进行解密



密码学基础：非对称加密算法

- 大部分的非对称算法提供签名功能
  - 使用私钥加密，公钥解密



密码学基础：经典非对称加密算法

- 所有的非对称加密算法，都是基于各种数学难题来设计的
  - 这些数学难题的特点是：正向计算很容易，反向推导则无解

密码学基础：经典非对称加密算法

- RSA
  - RSA加密算法，RSA Algorithm
  - RSA的数学难题是：两个大质数p、q相乘的结果n 很容易计算，但是根据n去做质因数分解得到p、q，则需要很大的计算量
  - 性能比较快，想获得较高的加密强度，需要使用很长的密钥
- ECC
  - 椭圆加密算法，Elliptic Curve Cryptography
  - 基于椭圆曲线的一个数学难题设计
  - 目前国际上加密强度最高的非对称加密算法
- 国密SM2
  - 基于椭圆曲线的一个数学难题设计
  - 加密强度和国际标准ECC相当

密码学基础：经典非对称加密算法对比

对比前提：同等密钥长度、加密强度

	加密强度	密钥生成性能	加解密性能	版权/专利
RSA	弱	慢	快	RSA公司
ECC	强	快	慢	争议中
SM2	强	快	慢	中国

非对称加密算法的应用

- 大部分的认证和签名场景
  - SSH登录
  - Git上传
  - 。。。

密码学基础：散列算法

- 对任意长度的输入，计算出一个定长的id
  - 不可逆性
  - 鲁棒性
    - 同样的消息生成同样的摘要
  - 唯一性
    - 不存在两个不同的消息，能生成同样的摘要

密码学基础：经典散列算法

- MD5
  - 消息摘要算法，Message-Digest Algorithm 5
  - 目前应用比较普遍的散列算法，生成一个128位的消息摘要
  - 唯一性已被破解，但并不会构成大的安全问题
- SHA
  - 安全散列算法，Secure Hash Algorithm
  - 美国开发的政府标准散列算法，分为SHA-1和SHA-2两个版本
  - 唯一性已被破解，但并不会构成大的安全问题。目前，SHA-256 遍被认为是相对安全的散列算法
- 国密SM3
  - 国家标准，算法公开，加密强度和国际标准的SHA-256相当

密码学基础：散列算法对比

	长度	冲突概率	安全性	性能
MD5	128	中	中	中
SHA	160、256	低	高	慢
SM3	256	低	高	未测试

密码学基础：散列算法之盐

在使用散列算法的时候，一定要注意加“盐”。所谓“盐”，就是一串随机的字符，是可以公开的。将用户的密码和“盐”进行拼接后，再进行散列计算，这样，即使两个用户设置了相同的密码，也会拥有不同的散列值。同时可以提升黑客利用彩虹表暴力破解散列值的难度。

密码学基础：总结

- 对称加密具备较高的安全性和性能，应优先考虑
- 存在密钥分发难题时，使用非对称加密
  - 多人登录服务器
- 不需要可逆计算时，使用散列算法
  - 存储密码
- 对称加密用AES-CTR、非对称加密用ECC、散列算法用SHA256加盐
  - 能够满足大部分的使用场景