开发人员
应该了解的密码学常识

Yuan Zhang

什么是密码学？

密码学是主要研究**密码编码**和**解码**的一种学科，

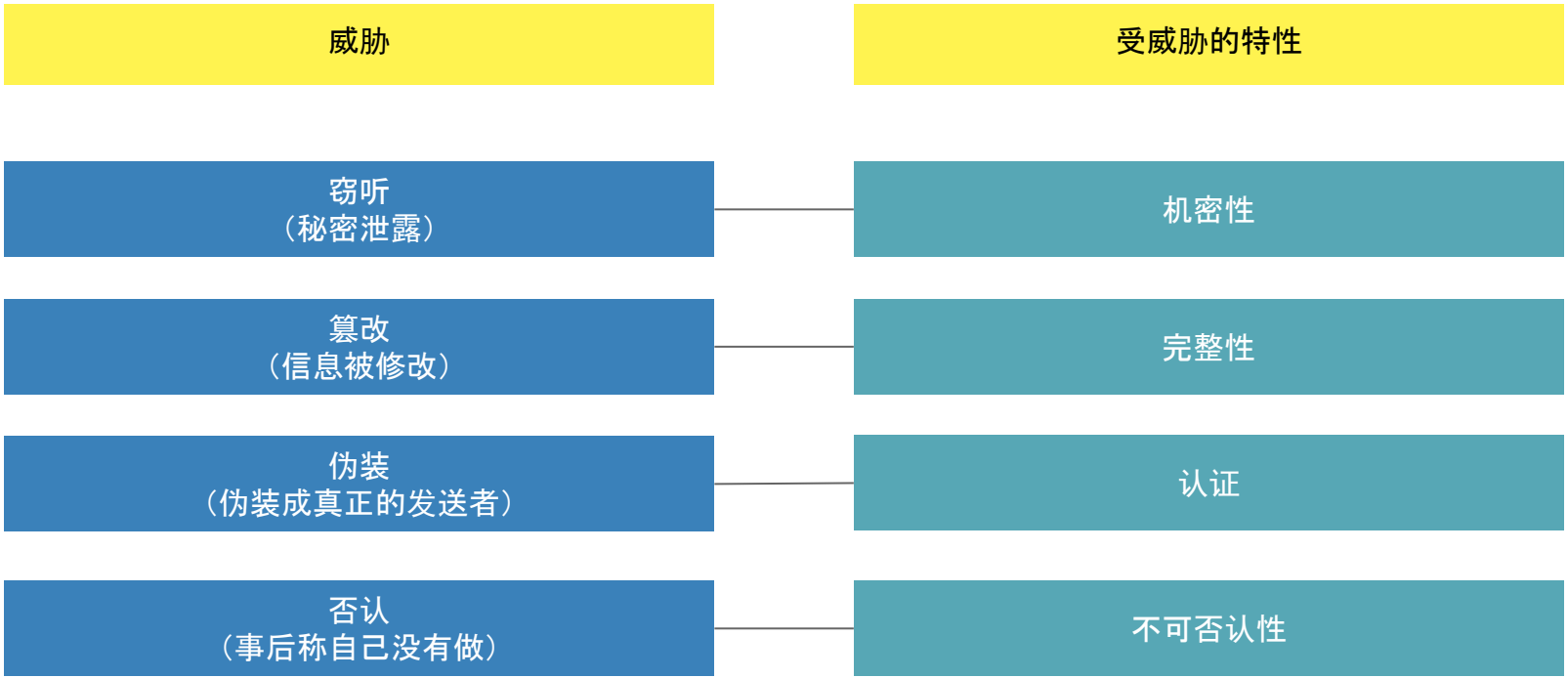
主要目标是提供在**不安全的信道**上的**安全通信机制**

开发人员
应该了解多少密码学相关的常识？

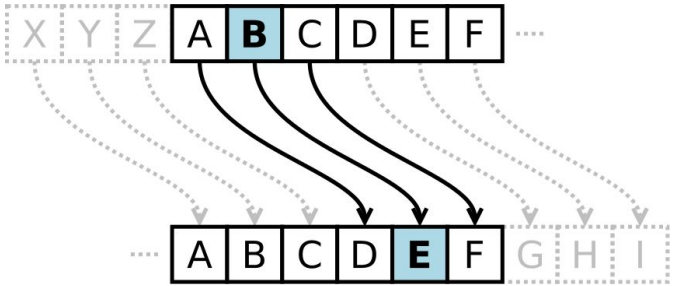

密码技术
ThoughtWorks®

加密与解密

消息传输中的威胁


威胁
受威胁的特性
窃听
（秘密泄露）
机密性
篡改
（信息被修改）
完整性
伪装
（伪装成真正的发送者）
认证
否认
（事后称自己没有做）
不可否认性

凯撒密码



古罗马凯撒大帝行军打仗时候用来传递军事情报的方法。

明文：
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

密文：
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替 换成密文。

例如，当偏移量是3的时候，

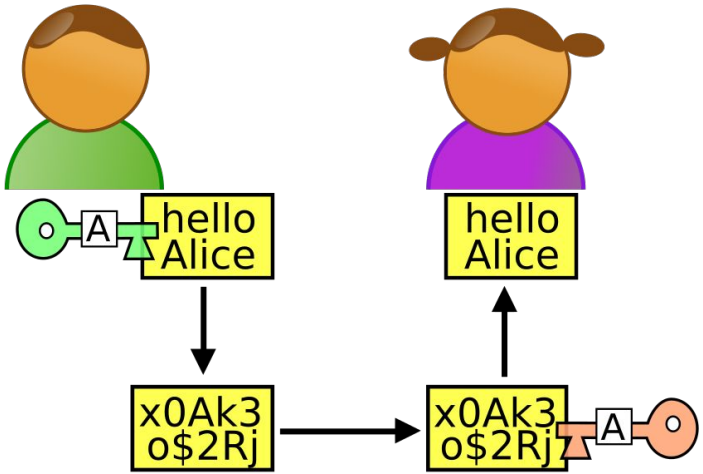
明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ
密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC

https://en.wikipedia.org/wiki/Caesar_cipher

古典密码体制与现代密码体制

古典密码体制	V.S.	现代密码体制
基于算法的保密性		基于密钥的保密性

对称密码算法



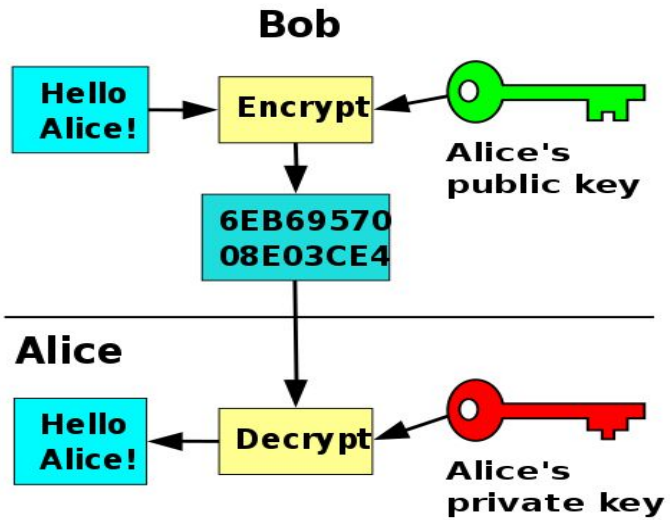
加密与解密时，使用同一个密钥。

DES	可在现实的时间内被暴力破解	不应用于新用途
3DES	处理速度不高	不应用于新用途
AES	安全快速	推荐使用

问题：在秘密通信之前，如何传送或者协商密钥？

https://en.wikipedia.org/wiki/Alice_and_Bob

非对称密码算法



加密与解密时，使用不同的密钥。

使用公钥加密，使用私钥解密。

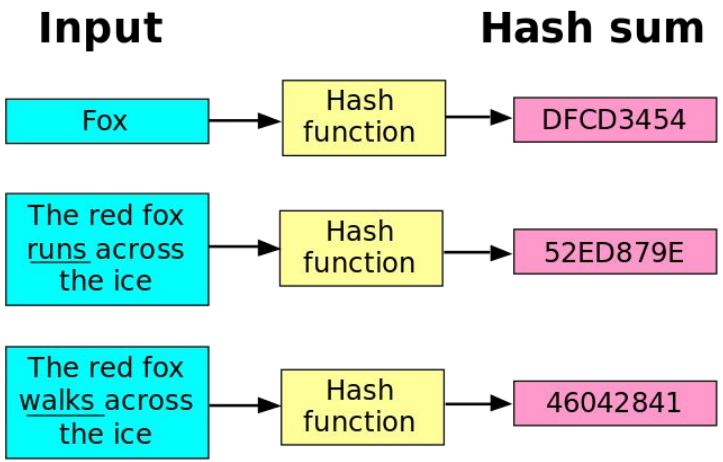
RSA	利用了质因数分解的困难度
ElGamal	利用了模N求离散对数的困难度
Rabin	利用模N下求平方根的困难度
椭圆曲线密码	利用乘法运算的逆运算非常困难

https://en.wikipedia.org/wiki/Alice_and_Bob

对称密码算法和非对称密码算法

	对称密码	非对称密码算法
是否需要协商密钥	是	否
运算速度	快	非常慢（是对称密码算法的的1%）
常见的使用场景	加密数据	主要用于密钥交换、数字签名、加密少量数据

散列算法



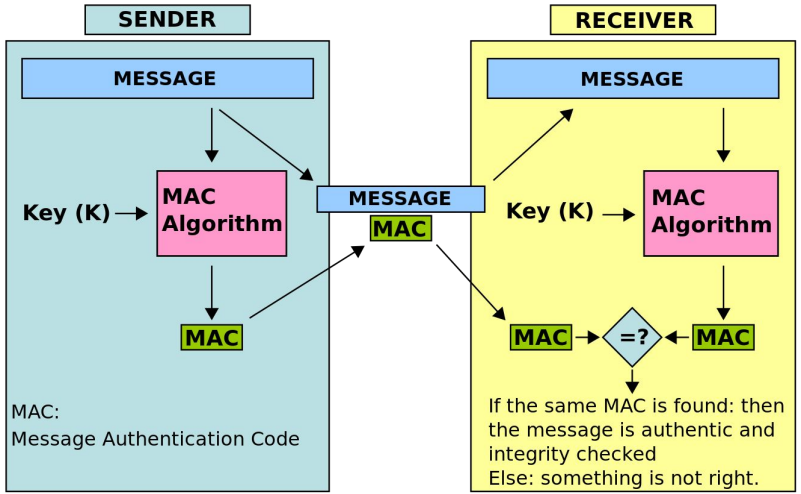
https://en.wikipedia.org/wiki/Cryptographic_hash_function

一种从任何一种数据中创建小的数字"指纹"的方法，用来检查消息的完整性。

- 根据任意长度的消息，计算出固定长度的散列值
- 能够快速计算出散列值
- 消息不同，散列值也不同(强碰撞性)
- 单向性

MD5	强碰撞性已被攻破	不安全
SHA-1	强碰撞性已被攻破	不推荐使用
SHA-2	强碰撞性尚未被攻破	安全，可以使用
RIPEMD-160	强碰撞性尚未被攻破	不推荐使用
SHA-3 (Keccak)	尚未出现对其形成威胁的攻击方法	安全，可以使用

消息认证码

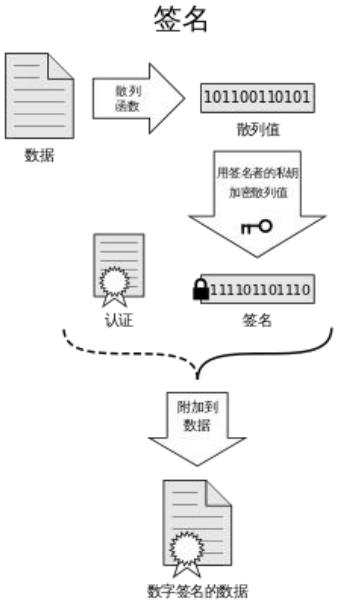


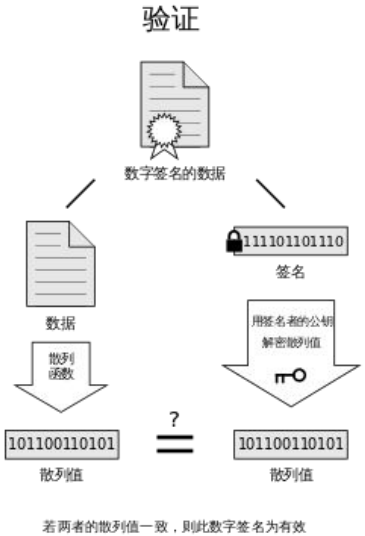
一种与密钥相关联的单向散列函数。

HMAC	使用SHA-2等单向散列函数实现
AES-CMAC	基于AES实现

https://en.wikipedia.org/wiki/Message_authentication_code

数字签名





只有信息的发送者才能产生的别人无法伪造的一段数字串。

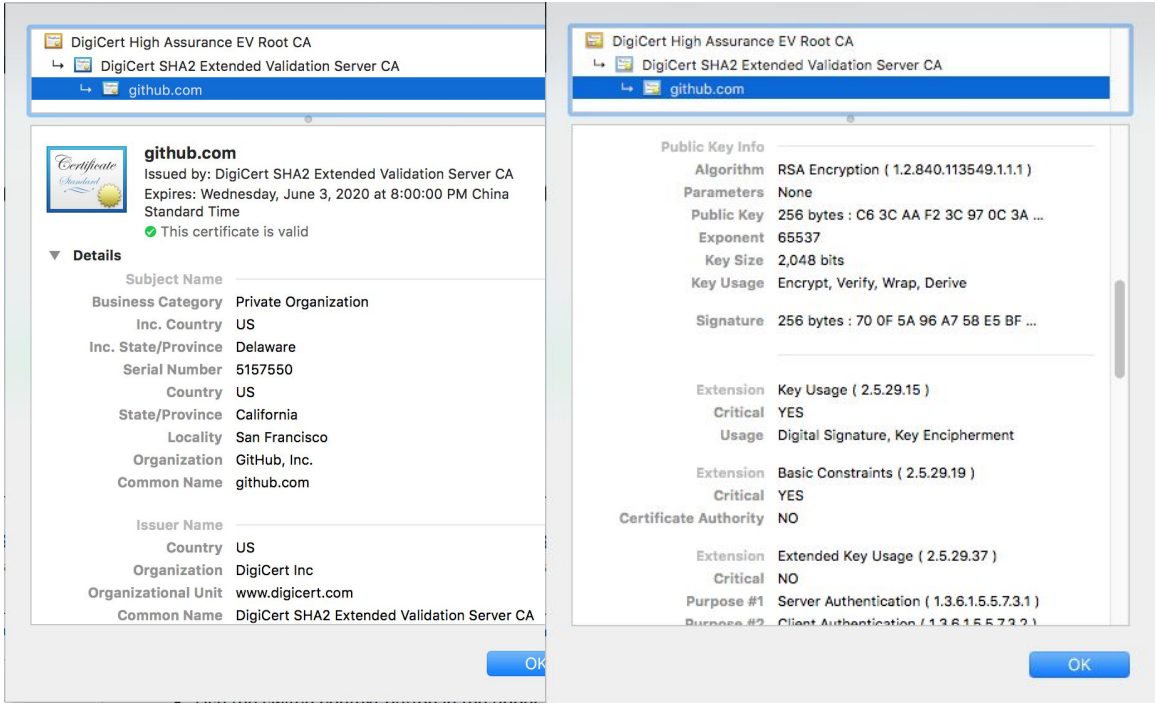
这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明，用来识别出消息是否被篡改。

通常使用非对称密码算法。私钥加密用于生成签名，公钥解密用于验证签名。

对消息签名	实际上不常见
对消息的散列值签名	推荐

https://zh.wikipedia.org/wiki/%E6%95%B8%E4%BD%8D%E7%B0%BD%E7%AB%A0

数字证书



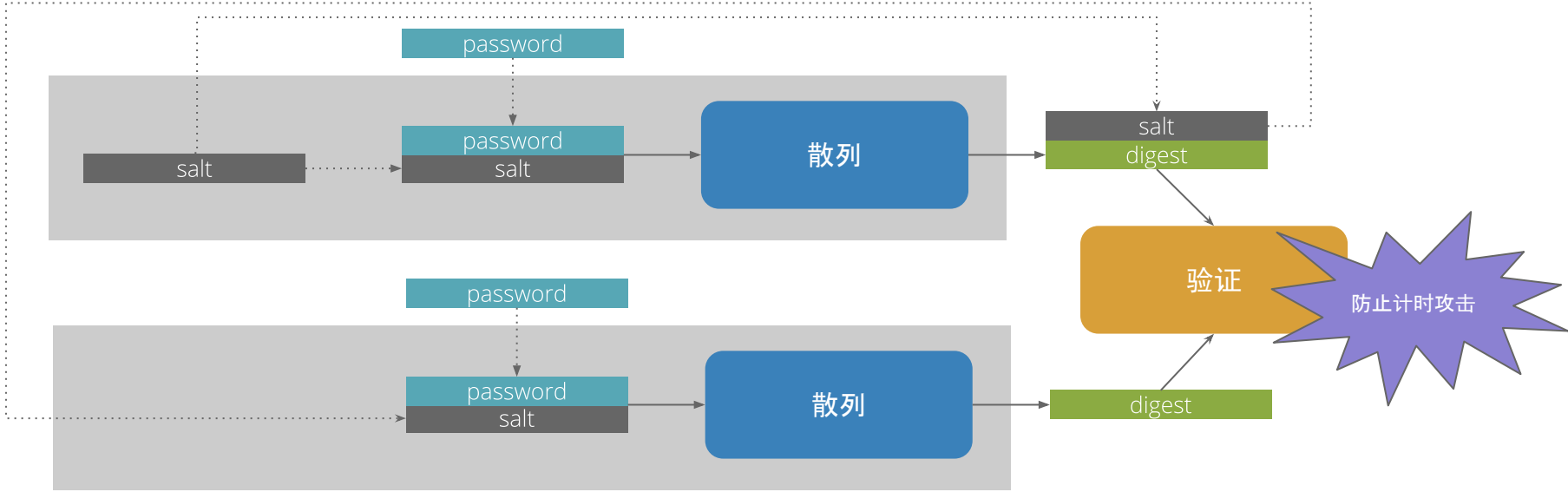
数字证书，也称为公钥证书或者身份证书。

一个用来证明公钥所有权的电子文档。通常包含了**公钥**的信息、**所有者**，以及**认证机构的已经认证过的数字签名**等。

公钥可以是公钥所有者生成，也可以是认证机构来代为生成。


应用场景举例
ThoughtWorks®

保存与验证密码



- 不要保存密码明文，只需要保存密码的摘要值用来验证即可
- 通过加盐值来提升字典攻击的难度
- 如果使用 bcrypt，那么不需要加盐值

TLS握手（举例）


客户端
服务器
服务器的公钥
对称密码的密钥
消息认证码的密钥
对称密码的CBC模式的IV
对称密码的密钥
消息认证码的密钥
对称密码的CBC模式的IV

TLS握手（举例）


客户端
服务器
ClientHello: 客户端随机数，密码套件清单等
ServerHello: 服务器随机数，密码套件，服务器证书等
服务器的公钥
主密码由客户端随机数、服务器随机数和预备主密码生成
ClientKeyExchange: 经过加密的预备主密码
主密码
主密码
对称密码的密钥
消息认证码的密钥
对称密码的CBC模式的IV
ChangeCipherSpec & Finished: 握手结束
对称密码的密钥
消息认证码的密钥
对称密码的CBC模式的IV
（切换到应用数据协议）

TLS协议中使用的密码技术

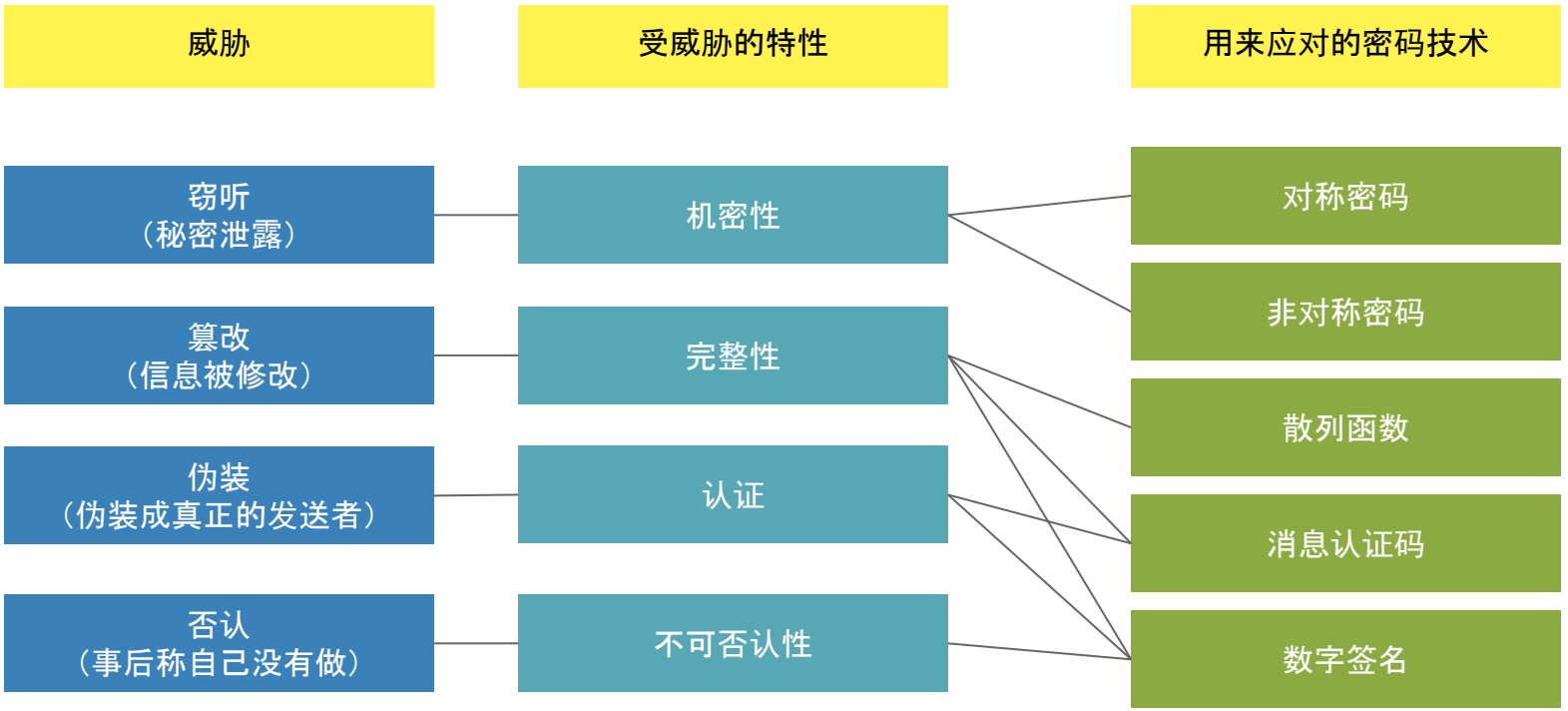
密码技术	作用
公钥密码	加密预备主密码
单向散列函数	构成伪随机数生成器
数字签名	验证服务器和客户端的证书
伪随机数生成器	生成预备主密码 根据主密码生成密钥(密码参数) 生成初始化向量

回顾

开发人员

应该了解多少密码学相关的常识？

威胁与密码技术


威胁
受威胁的特性
用来应对的密码技术
窃听
（秘密泄露）
篡改
（信息被修改）
伪装
（伪装成真正的发送者）
否认
（事后称自己没有做）
机密性
完整性
认证
不可否认性
对称密码
非对称密码
散列函数
消息认证码
数字签名

密码与信息安全常识

不要使用保密的密码算法

使用低强度的密码比不进行任何加密更危险

任何密码总有一天都会被破解

密码只是信息安全的一部分

谢谢

如有任何问题，请联系

evzhang@thoughtworks.com