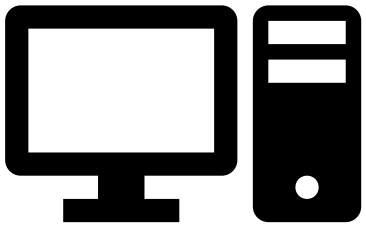


Safety

name:dixi

key:123

HTTP

HTTPS

HTTPS

可以理解为HTTP+SSL/TLS， 即 HTTP 下加入 SSL 层，HTTPS 的安全基础是 SSL，因此加密的详细内容就需要 SSL，用于安全的 HTTP 数据传输。

HTTPS

SSL/TLS

其前身是 SSL（Secure Socket Layer，安全套接字层），它最初的几个版本（SSL 1.0、SSL 2.0、SSL 3.0）由网景公司开发，1999年从 3.1 开始被 IETF 标准化并改名，发展至今已经有 TLS 1.0、TLS 1.1、TLS 1.2 三个版本。SSL3.0和TLS1.0由于存在安全漏洞，已经很少被使用到，目前使用最广泛的是TLS 1.1、TLS 1.2。

HTTPS

SSL/TLS

公私秘钥

证书

PKI

对称/非对称加密

Transport Layer Security—传输层安全

1.Client Hello—TLS版本、加密套件、随机数one

2.Server Hello—TLS版本、加密套件选择、随机数two

公钥　　私钥

3.Certificate—server的基本信息、公钥；数字签名

4.Server Key Exchange

5.Server Hello Done

随机数1
+
随机数2
+
随机数3
=
会话秘钥

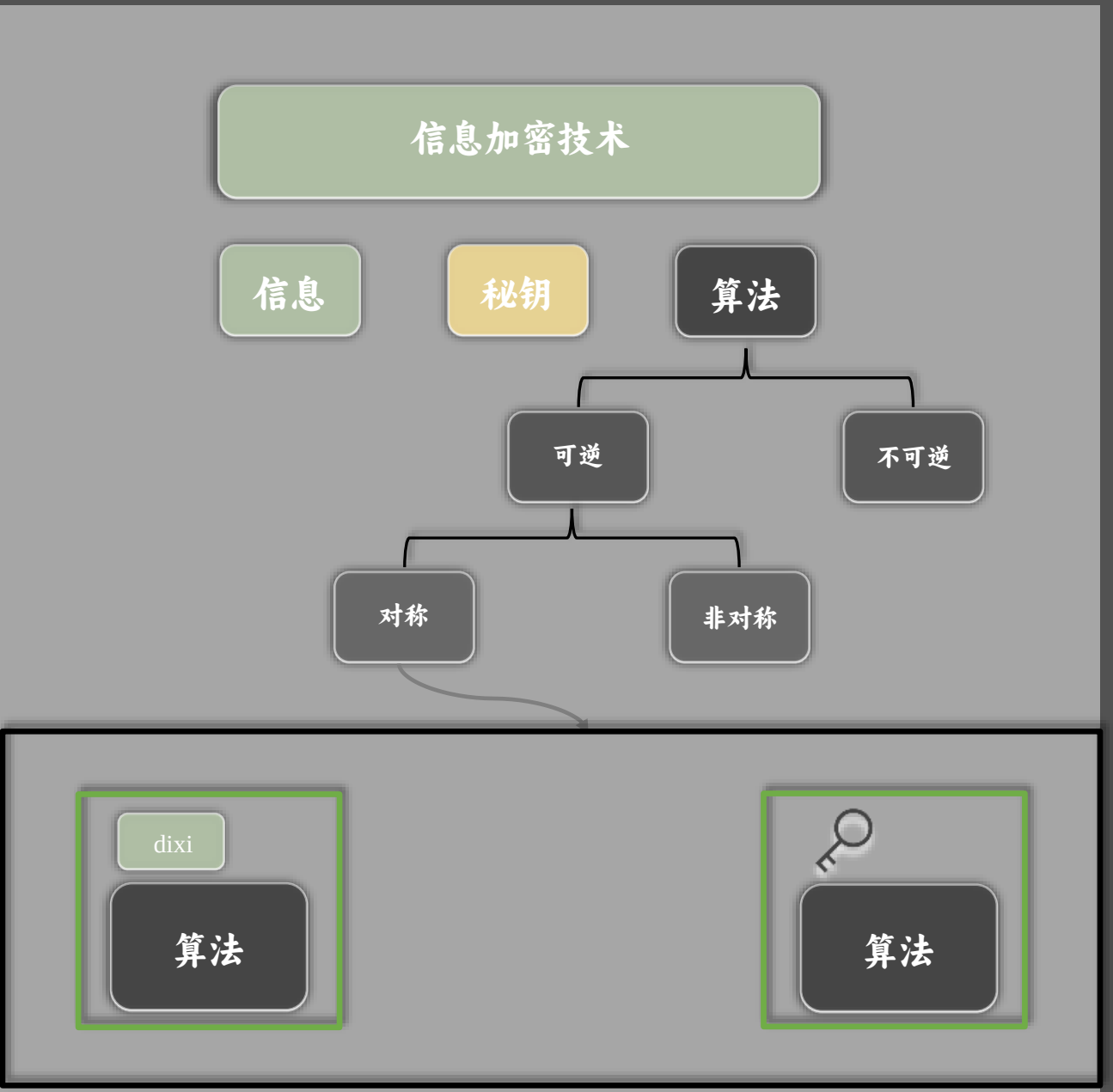
6. Client Key Exchange—随机数three公钥加密，Pre Master Key

7.对称性加密数据传输

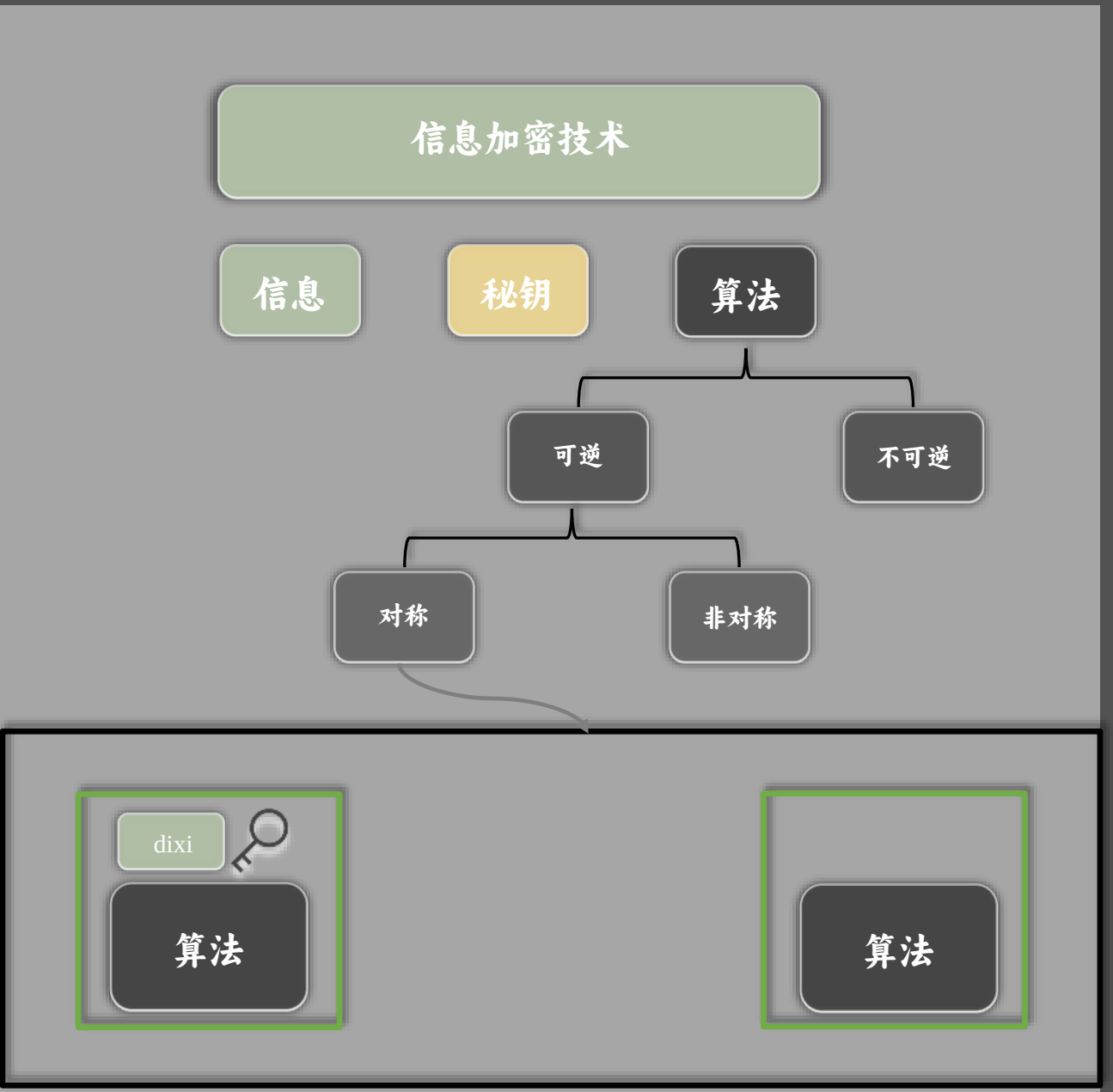
随机数1
+
随机数2
+
随机数3
=
会话秘钥

PKI

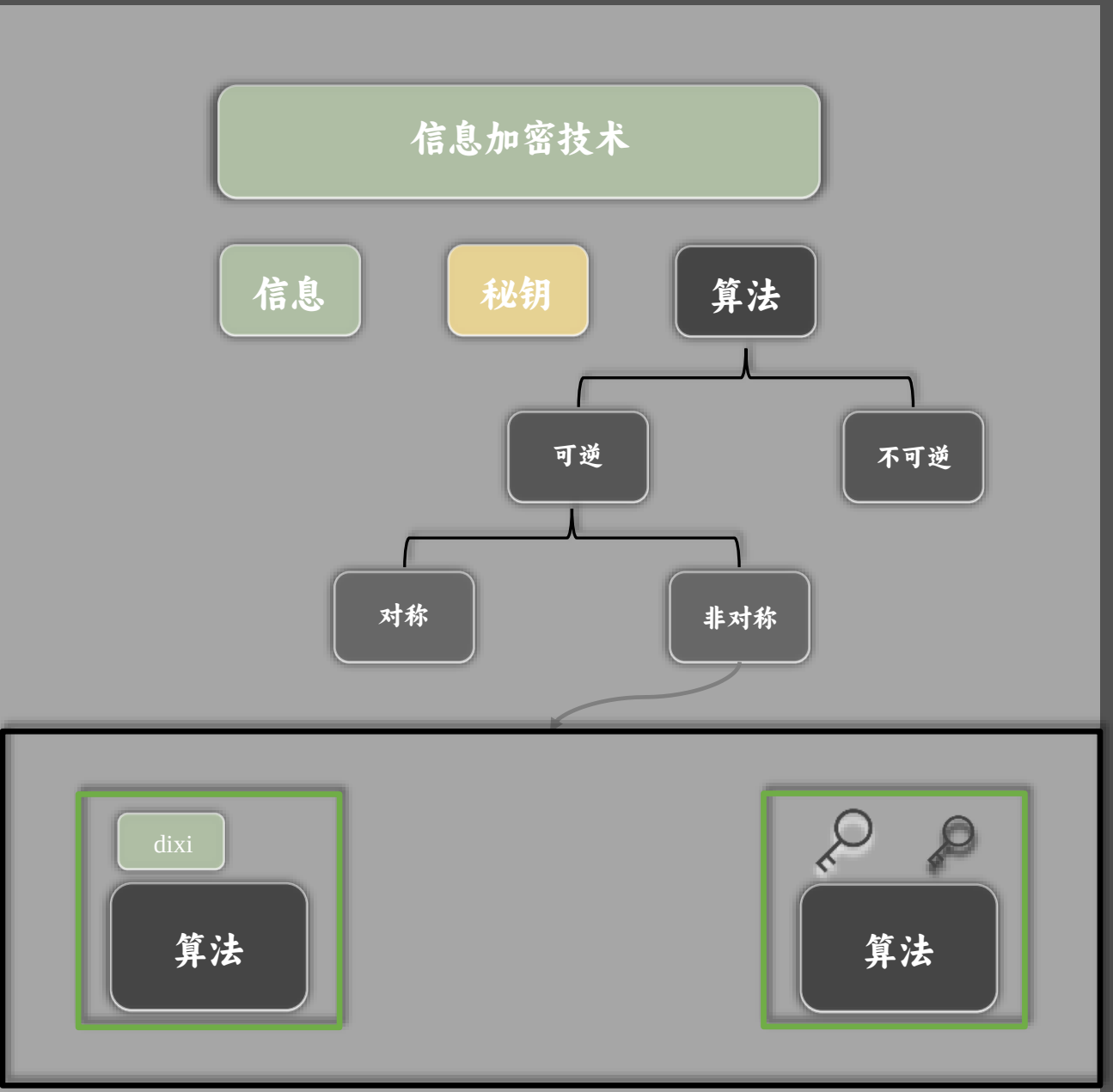
PKI-Public Key Infrastructure(公钥基础设施)



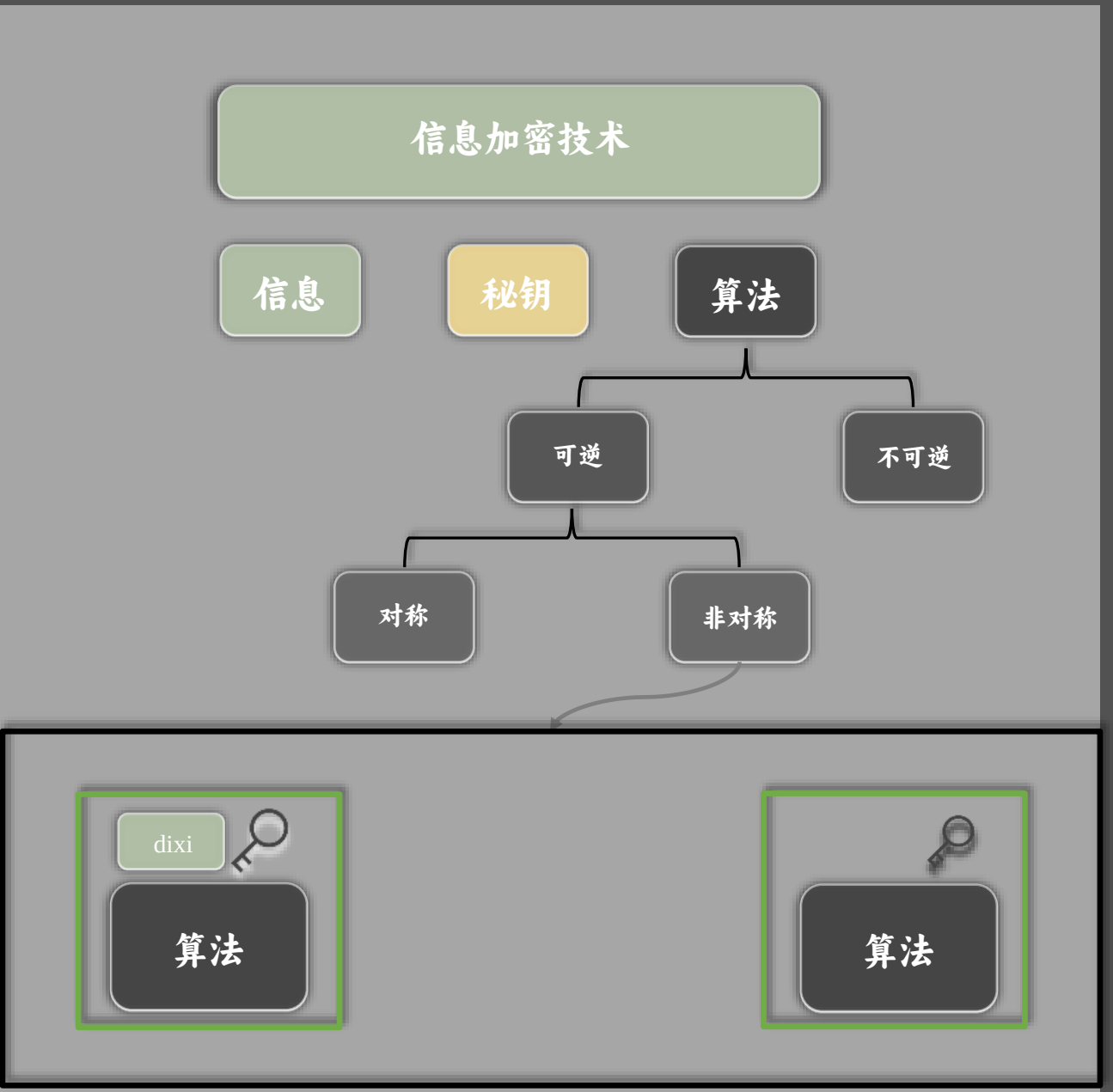
PKI-Public Key Infrastructure(公钥基础设施)



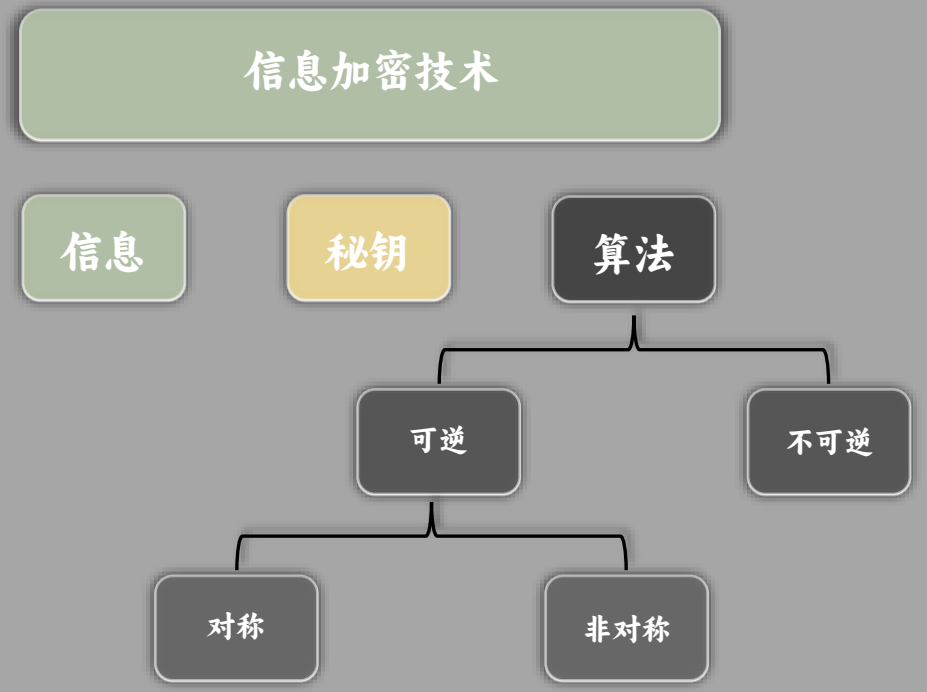
PKI-Public Key Infrastructure(公钥基础设施)



PKI-Public Key Infrastructure(公钥基础设施)

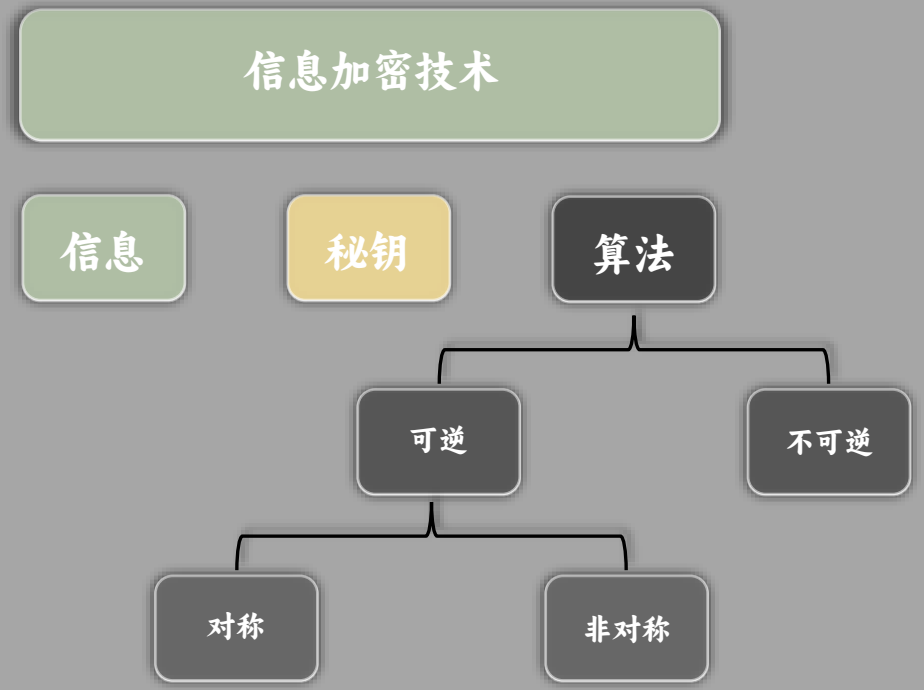


PKI-Public Key Infrastructure(公钥基础设施)



证书

PKI-Public Key Infrastructure(公钥基础设施)

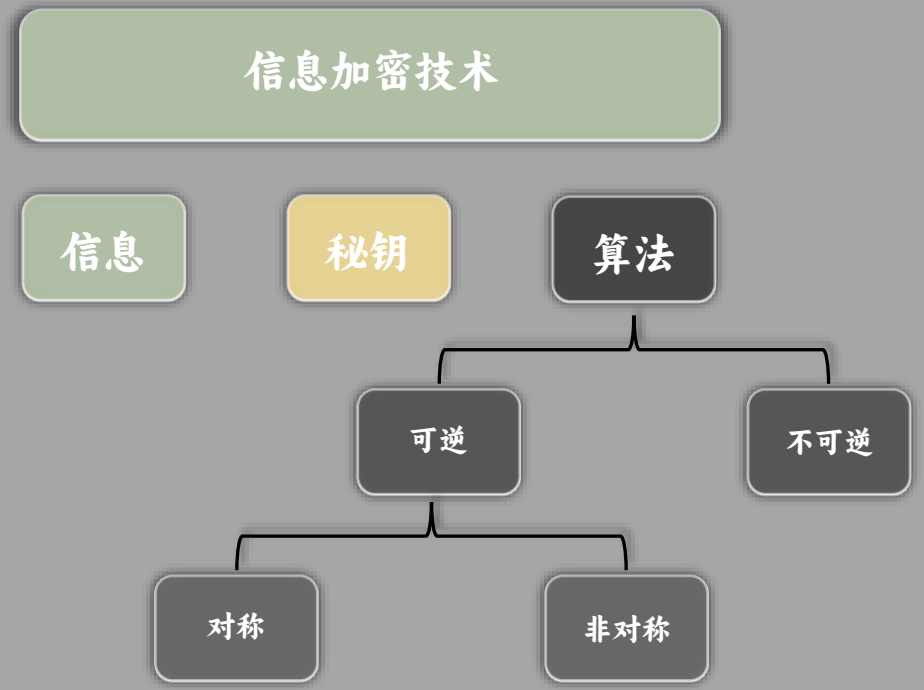


申请方基本信息

申请方公钥

授权方数字签名

PKI-Public Key Infrastructure(公钥基础设施)

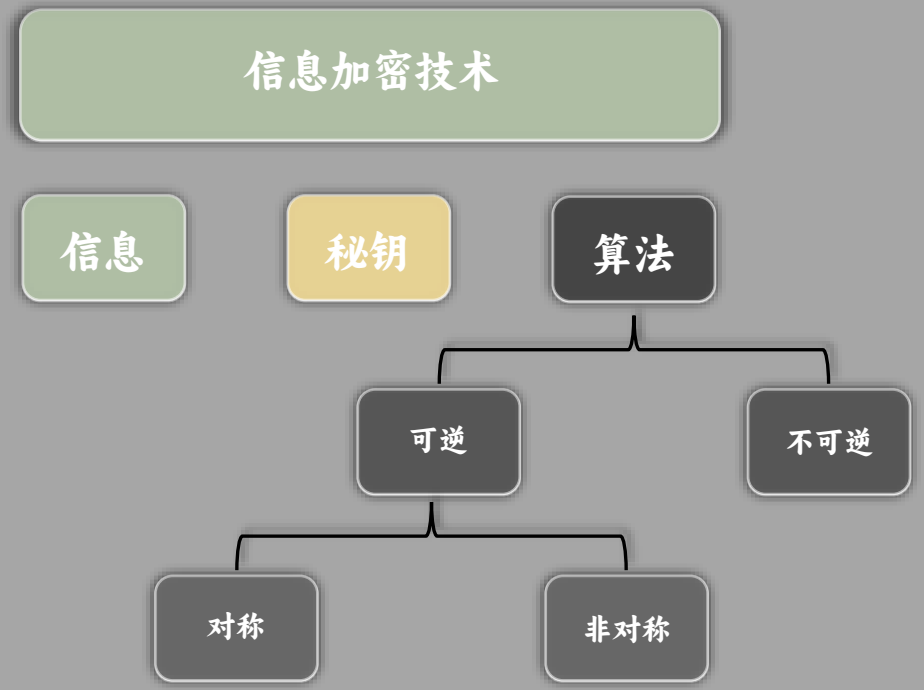


授权方数字签名

申请方信息

认证方不可逆加密算法

PKI-Public Key Infrastructure(公钥基础设施)



授权方数字签名

摘要/指纹

认证方私钥

申请方信息

认证方不可逆
加密算法