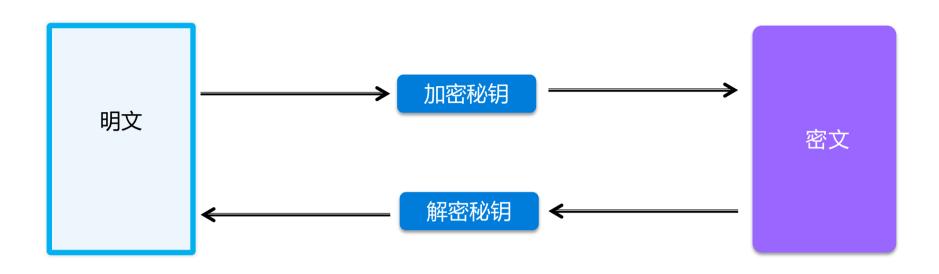
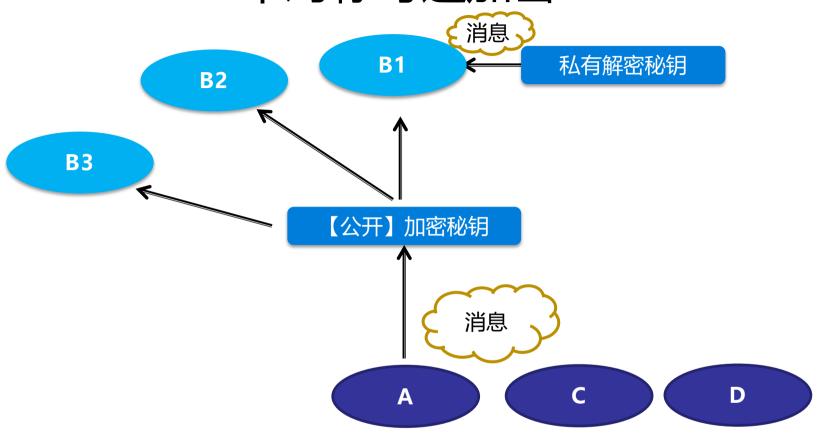
对称可逆加密

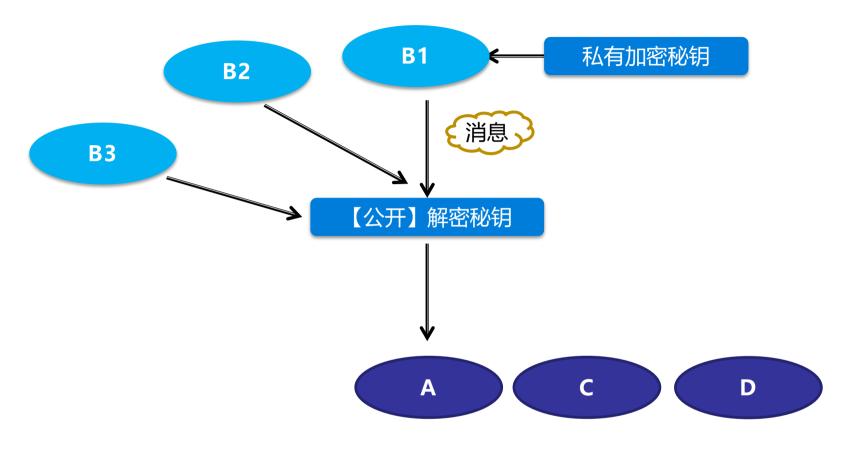


不对称可逆加密-1

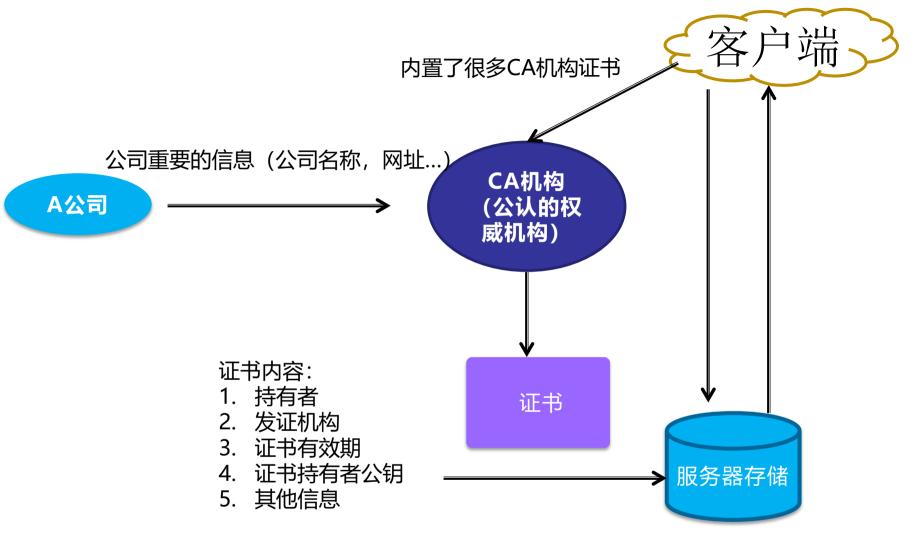


应用: 唯一确定消息接收者(私有解秘钥)记忆诀窍: 私解, 我收

不对称可逆加密-2



应用: 唯一确定消息发出者(私有加秘钥)记忆诀窍: 私加, 我发



以上证书内容必须保证不能被破坏,所以需要MD5摘要。

单向认证



证书3

首次请求

首次返回一个证书(证明证书是真实的)

第二次发送,用公钥加密一段信息,给服务器

,第二次返回,用解秘钥解开加密信息(证明是<mark>证书持有者)</mark>

这时候,可以双工通信

证书

服务器

双向认证

这时候,可以双工通信

证书

服务器

