1.从生成、验证、效率、安全特性等多方面，请简要对比消息认证码和数字签名的异同。

	消息认证码	数字签名
发送者	用对称密钥计算 MAC	用私钥生成签名
接受者	用对称密钥计算 MAC	用公钥验证签名
密钥分发问题	存在	不存在，但公钥需要额外认证(譬如数字证书)
效率	高	低
完整性	支持	支持
认证性	支持(仅限通信双方)	支持(需要可信第三方支持)
不可否认性	不支持	支持

2. 数字证书通常是以文件形式存在，其内容是公开的，那么数字证书内容的真实性如何保障？譬如 Alice 的数字证书，如果把持证人名称改为 Bob，是不是就变成 Bob 的数字证书了，为什么？

答：CA 的数字签名保证了数字证书内容的真实性。

首先，CA 是可信的第三方，数字证书内容是由 CA 确认并颁发，一旦 CA 对数字证书进行签名，就保证数字证书的内容（包括用户公钥）是不可更改的，也就是说，相信 CA，也就相信数字证书里所有内容，包括公钥。如果数字证书内容被修改，那么数字证书验证不通过，这数字证书无效，不能使用。