为什么说信息安全是信息时代永恒的需求？

信息成为当今最具活力的生产要素和最重要的战略资源，以计算机网络为核心的信息系统成为国家的重要基础设施。信息安全是信息的影子，哪里有信息哪里就存在信息安全问题。无论在信息科学技术发生新的突破之前和突破之后，信息安全始终是一个重要的问题。因此，我们可以说，信息安全是信息时代永恒的需求，不确保信息安全就不能确保我们赖以生存的人类社会和网络空间的和谐、安定、繁荣和进步。

网络空间安全学科的内涵是什么？

网络空间安全学科是研究信息获取、信息存储、信息传输属于和信息处理领域中信息安全保障的一门新兴学科。

网络空间安全学科的理论基础有哪些？

数学是一切自然科学的理论基础，当然也是网络空间安全学科的理论基础。

信息论、控制论和系统论是现代科学的基础，因此也是网络空间安全学科的基础理论。

网络空间安全学科的许多问题是计算安全问题，因此计算理论也是网络空间安全学科的理论基础，其中包括可计算性理论和计算复杂性理论等。

密码体制的分类

按照明文的处理方法分类

分组密码：将明文分为固定长度的组，用同一密钥算法对每一块加密，输出也是固定长度的密文。

流密码：又称序列密码，每次加密一位或一字节的明文。

按照密钥使用方法分类

对称密码算法：又称传统密码算法或秘密密钥算法、单密钥算法

非对称密钥算法：又称公开密钥算法或双密钥算法。

除“一次一密”外，所有的都不是无条件安全的。

实际可用的密码应尽量满足：

破译密码的代价超出密文信息的价值

破译密码的时间超出密文信息的有效生命期

计算上安全：满足上述两条标准中的任意一条即可。

DES

1、可逆性证明

见DES的PPT

2、对合性证明

同上

3、3DES

PPT补充：3密钥的3DES，密钥长度168位，采用加密-解密-加密（E-D-E）方案

PPT2密钥的3DES图中加密密钥使用顺序改为k1,k2,k3，解密密钥顺序改为k3,k2,k1

HASH

安全HASH函数要满足哪些条件？为什么？P178-180

1、单向性：单向性是指由Hash码不能求出相应的输入数据，若Hash函数不是单向的，则攻击者可以从截获的数据求出Hash函数的逆，获得秘密值

2、抗弱碰撞性：不能找到与给定数据具有相同Hash值的另一数据。如果该性质不成立，那么攻击者可以截获一条数据M及其加密的Hash函数值，然后替代M

3、抗强碰撞性：抗生日攻击这类攻击的能力。找到任何满足H(x)=H(y)的偶对(x,y)在计算上是不可行的。

4、随机性：随机性应当通过我国国家密码管理局颁布的《随机性测试规范》的测试，也可参考美国NIST的随机性测试标准。

海绵结构P192

在海绵函数中，输入数据被分为固定长度的数据分组。每个分组逐次作为迭代的输入也反馈至下轮的迭代中，最终产生输出Hash码。海绵函数允许输入长度和输出长度都可变。由于具有这个各灵活的结构特点，海绵函数能够用于设计Hash函数（固定输出长度）、伪随机数发生器（固定输入长度），以及其他密码函数。

海绵结构包括两个阶段，吸水阶段和挤水阶段。

在吸水阶段，每一轮迭代处理前都要给r位的数据分组填充c个0，使数据块长度变成b位。这一过程很像海绵吸水，这里的“水”就是填充的c个0

在挤水阶段，每一轮迭代处理前都要从长度为b的状态变量s中取出r位的分组，并丢弃其余的c位分组，这一过程很像海绵挤水，这里的“水”就是丢弃的c位分组。

SM3基本框架：见PPT

公钥密码

基本概念：见PPT 或课本P209

为什么ELGamal密码要求参数K是一次性的？

PPT：公钥密码2

数字签名

说明对于RSA的数字签名，为什么先加密后签名不安全？

签名在传播途中可能被人为地篡改，攻击者截获D(E(M,KeB),KdA)并阻断该签名到接受者的传输，再根据KeA得出E(M,KeB)，从而计算出D(E(M,KeB),KdC)即用自己的私钥签名后发给接受者。

HASH函数在数字签名中的作用

课本P249

认证

什么是认证？认证和数字签名的区别是什么？

见认证PPT

身份认证的方法有哪些？各有什么优缺点？

口令，磁卡、智能卡和USBUSB-Key，生理特征识别（详见PPT）

报文源、报文宿、MAC等见PPT

设计题

1）动态口令（网银）（有一个攻击者不知道的输入）

时间输入，用户ID（每个用户不同，可以不保密），银行设置的系统密钥（所有用户共享）（硬件保护，永远不能读出），做HASH

解决时间误差：把时间往前调，往后调，若相同则成功，服务器跟着偏移

2）校园卡与刷卡器

刷卡器中保有系统密码，由系统密钥和用户ID生成用户密钥（校园卡中有一个用户ID），再进行身份认证。

3）PING码（U盾中）：U盾在认证人

U盾中装有一个很长的签名用的私钥，它的启用是由一个很短的口令保护（长了人记不住）

存在问题：解决：限制输入次数

4）Windows密钥管理（域控制服务器：控制多台设备）

A想访问B，但不信任，都信任S，S生成会话秘钥，只能使用8小时

A与S之前通信要加密，用事先确认的密钥，A向S表示想访问B，S查A是否有权限，S给一个密文给A，是用S和B间的密钥加密。

S给A会话密钥，A把密文给B

B验证密文是否是S，密文解密后是会话密钥、A的ID

缺点：只适用于小规模，因为服务器要一直开介绍信

不适合互联网环境（互联网环境中基于PKI实现）

A、B两者间的可信通信

认证：仅身份认证+产生后续通信的会话密钥

数字签名：仅完成身份与消息的绑定

（漏洞：A可以抵赖或自己没有发这个消息，因为B有可能伪造）

①A,B共享密钥k

A (消息+k消)hash签名 B

B用k验签

②A有公钥，B有私钥

A 私钥对消息签名+消息 B

用公钥验签，万一A抵赖则提供给第三方

证书

①证书给谁

②目标方的公钥是什么

③第三方用私钥对①②的签名

RSA根证书在更新的过程中，需要所有证书拥有者更新公钥

如何让证书拥有者相信公钥的发布方是RSA？

1990年 发布19901年公钥和2000年公钥的哈希值（发布消息和公钥哈希的结果）

2000年 发布2000年公钥和2010年公钥的哈希值

以上：用公钥密码提供身份认证，适用于：用户特别多

PKI：公钥密码基础设施

CA：证书颁发机构

RA：注册认证机构

CRL：证书吊销列表

签名私钥绝对不能备份，坏了就重新申请再发布公钥

失窃了“挂饰”，告知权威第三方通知所有人旧证书不可行