[1. 我国的密码分级： 1](#_Toc27274)

[2. 我国商用密码政策： 2](#_Toc15849)

[3. 密码设计的基本方法 2](#_Toc14530)

[4. S盒其他准则 3](#_Toc25414)

[5. AES的设计要求 3](#_Toc25790)

[6. AES整体特点 3](#_Toc9915)

[7. Hash函数的作用 4](#_Toc28997)

[8. 传统密码的优缺点： 4](#_Toc29973)

[9. SM2与传统ECC比较 5](#_Toc16521)

[10. 对RSA数字签名的攻击 6](#_Toc5618)

[11. 比较SM2签名算法与传统签名算法 7](#_Toc31006)

[12. 协议与算法的比较 7](#_Toc17747)

[13. SM2安全性 8](#_Toc24503)

# 我国的密码分级：

①核心密码：

用于保护党、政、军的核心机密。

②普通密码：

用于保护国家和事企业单位的低于核心机密的机密信息。

③商用密码：

用于保护国家和事企业单位的非机密的敏感信息。

④个人密码：

用于保护个人的隐私信息。

前三种密码均由国家密码管理局统一管理！

# 我国商用密码政策：

①统一领导：

国家密码管理局统一领导。

②集中管理：

国家密码管理局集中管理。

③定点研制：

只允许定点单位进行研制。

④专控经营：

经许可的单位才能经营。

⑤满足使用：

国内各单位都可申请使用。

# 密码设计的基本方法

⑴ 公开设计原则

密码的安全应仅依赖于对密钥的保密，不依赖于对算法的保密。

⑵ 扩散和混淆

 扩散(diffusion)：将明文和密钥的每一位的影响散布到尽量多

的密文位中，理想情况下达到完备性。

 混淆(confusion):使明文、密钥和密文之间的关系复杂化。

⑶ 迭代与乘积

 迭代：设计一个轮函数，然后迭代。

 乘积：将几种密码联合应用

# S盒其他准则

非线性度准则：S盒必须有足够的非线性度，否则不能抵抗线性攻击；

差分均匀性准则： S盒的差分性应均匀，否则不能抵抗差分攻击；

代数次数及项数分布准则 ：S盒必须有足够的代线次数和项数，否则不能抵抗插值攻击和高阶差分攻击；

# AES的设计要求

①安全性：可以抵抗目前所有已知的攻击；

②实用性：适应各种应用环境，加解密速度快；

③扩展性：分组长度和密钥长度可扩展，可以适应

社会对保密性不断提高的需求。

# AES整体特点

①分组密码

 明文和密文长度128位，密钥长度可变（128/192/256等，

现在选用 128 位）。

②面向二进制的密码算法

 能够加解密任何形式的计算机数据。

③不是对合运算

 加解密使用不同的算法。

④综合运用多种密码技术

 置换、代替、代数

⑤整体结构

 SP结构，基本轮函数迭代，迭代轮数可变（≥10）

# Hash函数的作用

 Hash码也称为数据摘要、数据指纹。

 具有极强的错误检测能力:

 输入有很小的变化，输出将有很大的不同！

 检测错误，检测篡改。

 用Hash码作消息认证码（MAC），可用于认证。

 用Hash码辅助数字签名：

 缩短签名长度

 增强签名安全

 Hash函数还可用于伪随机数产生。

# 传统密码的优缺点：

①优点

⚫ 理论与实践都很成熟。

⚫ 安全容易把握。

⚫ 加解密速度快。

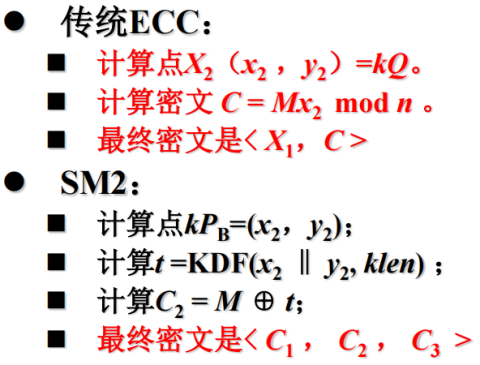
②缺点

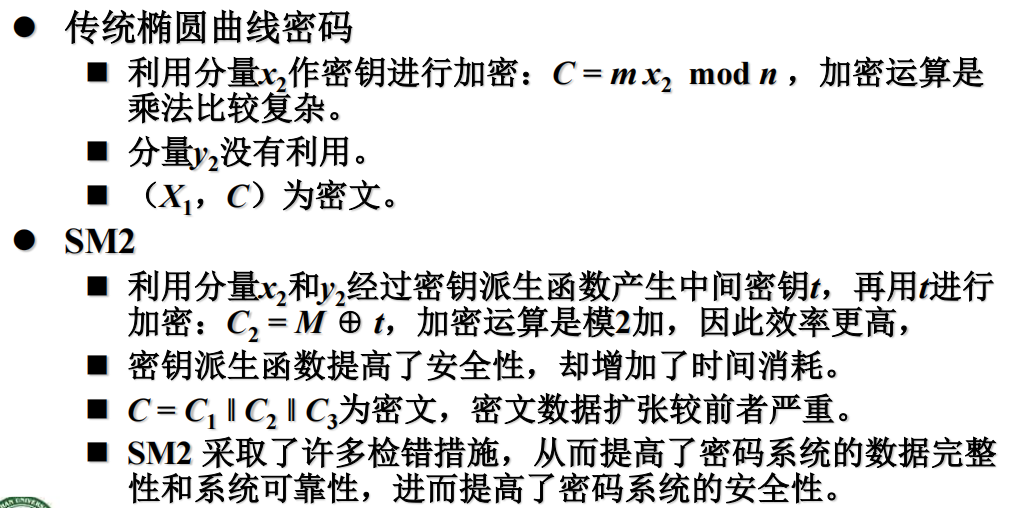
⚫ 收发双方持有相同密钥， Ke ＝ Kd ，密钥分配困难，

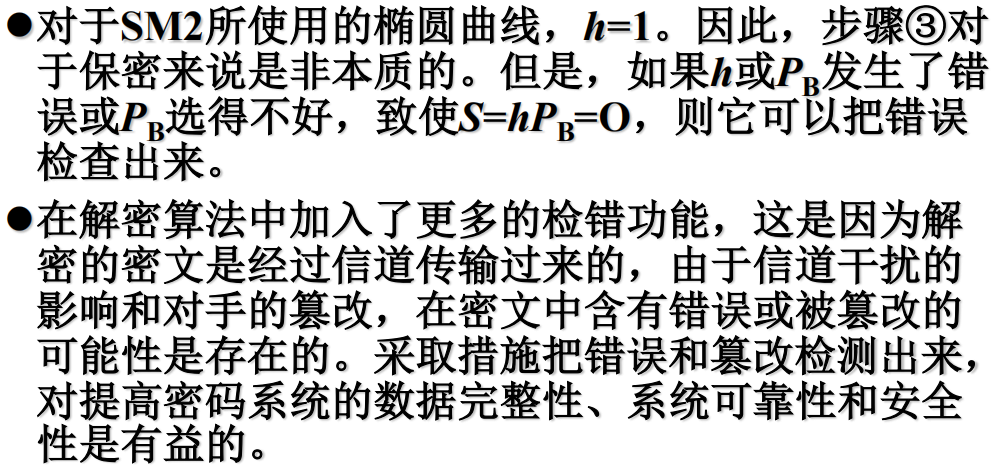
网络环境更突出。

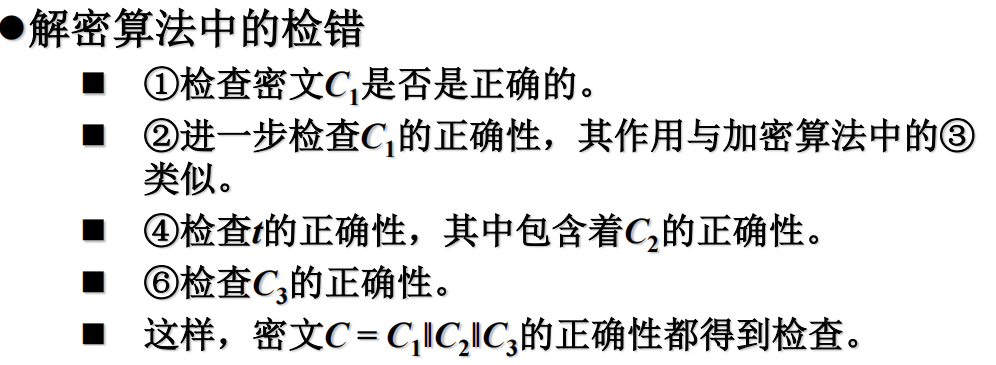
⚫ 不能方便地实现数字签名，商业等应用不方便。

# SM2与传统ECC比较

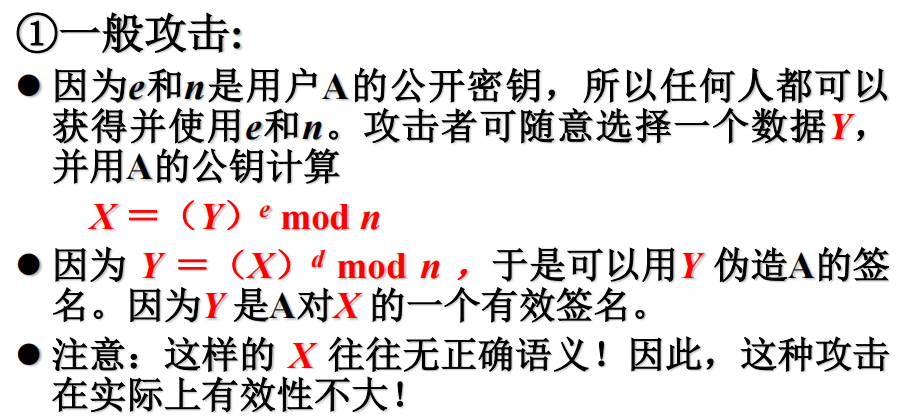


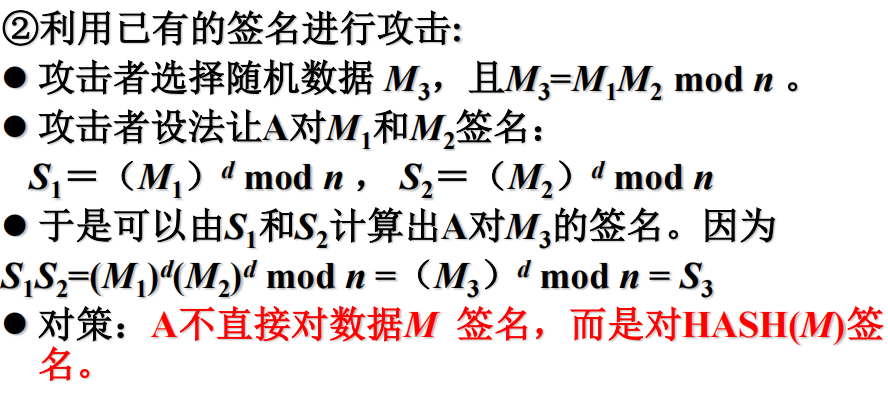


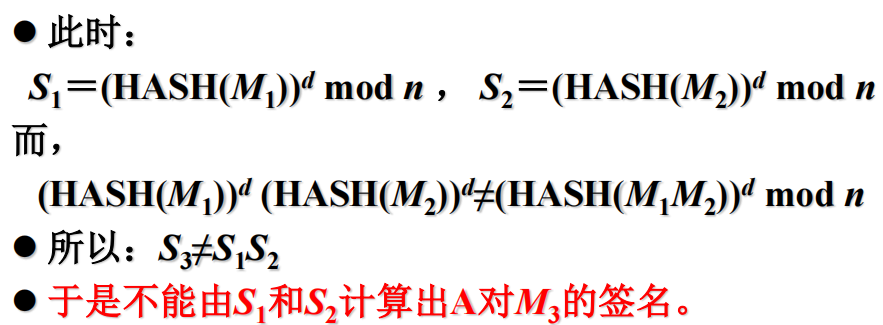


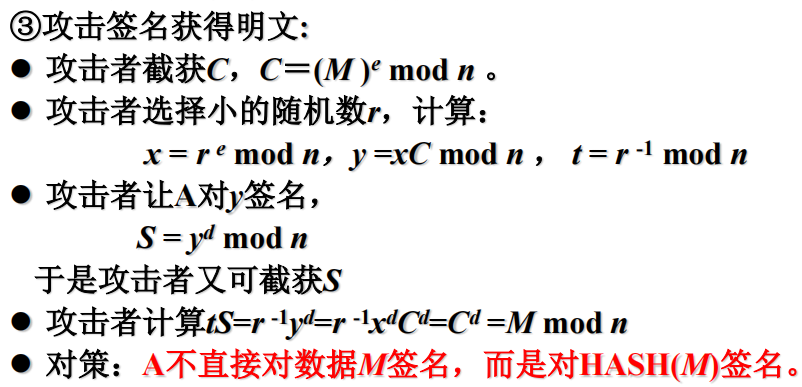


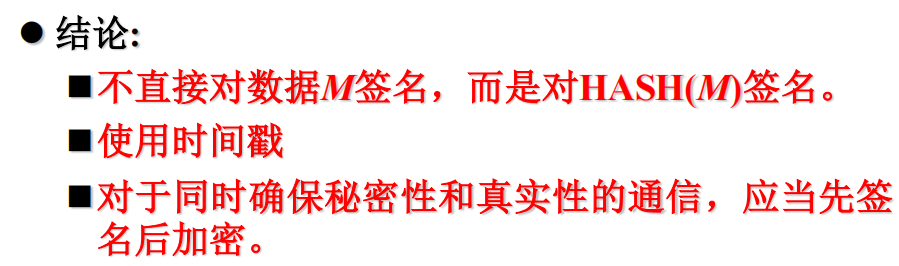
# 对RSA数字签名的攻击



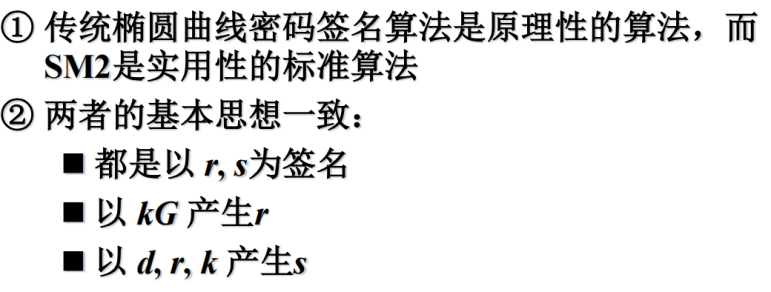


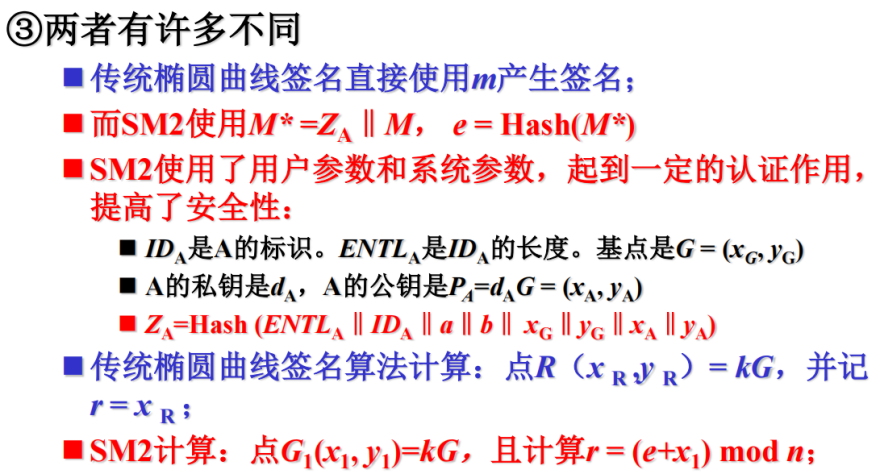


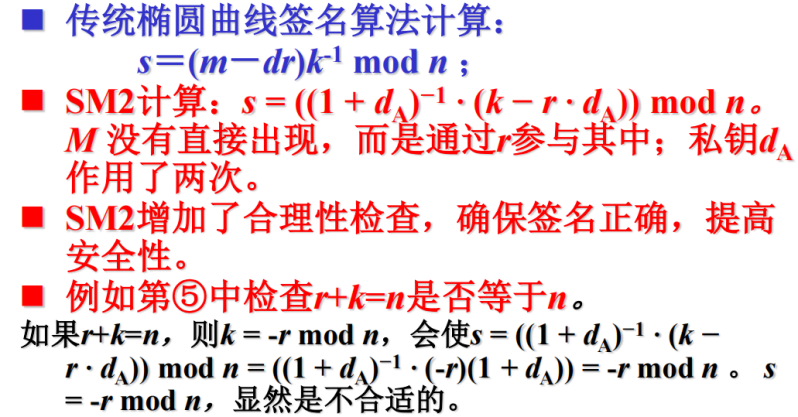




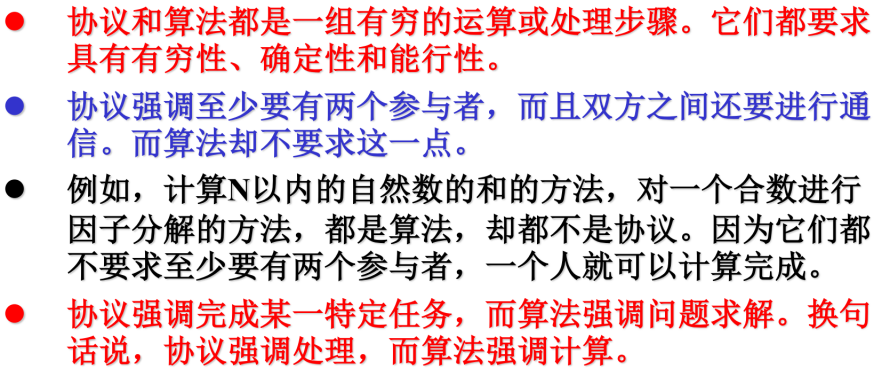
# 比较SM2签名算法与传统签名算法

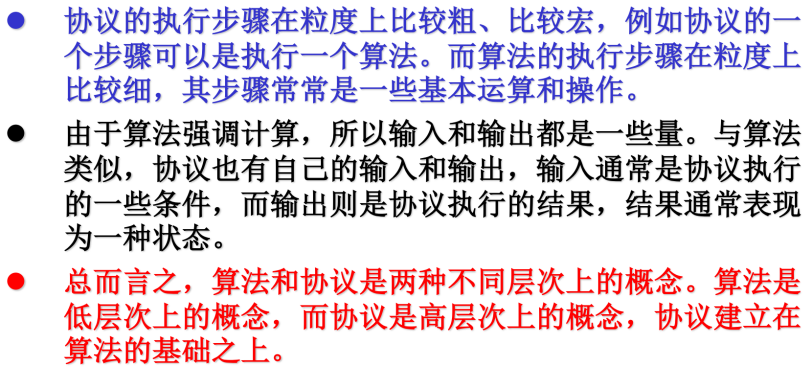






# 协议与算法的比较





# SM2安全性

