PPT1: 介绍
P3: 什么是密码
P5: 私钥加密
P7: 私钥加密的语法
P8: 密钥安全 VS 算法保密
P9: 开放密码算法的原因
P10: 攻击方法
P11: 恺撒密码
P12: 移位密码
P13: 重合指数法 (find k)
P14 单表替换法
P17: 统计模式攻击/频率分析
P19 维吉尼亚算法/多表替换法
P20 kasisk法 (find t)
P21 重合指数法 (find t)

PPT2: 完美保密 大题☆
P4 完美保密的定义
P5: 单比特完美保密的证明
P6: 等价形式 及证明
P7: 完美不可区分性 及证明
P8: OTP及证明:
P9: OTP与完美保密的局限性及证明
P10: 真实例子: ZTP
P11 香农定理及证明及应用
P13 $PrivK^{eav}_{A,\Pi}$ 实验
P14 例题

PPT3: 私钥加密的计算性
P12: 例题
P14: 语义安全
P18: PRG
P20: 例题
P24: 归约证明.
P25 F(s) PRG, G PRG?
P27 安全定长加密方案
P?: 不可区分加密证明
处理变长消息

P5: 攻击类型
P7 $PrivK^{mult}_{A,\Pi}(n)$
P11: $PrivK^{cpa}_{A,\Pi}(n)$
P13 PRF
P14: PRF定义
P15: 例题
P16: 由PRF来的CPA
P17: 证明上述构造
P18: 变长PRF的CPA安全
P20: PRP定义
P25: ECB　P26 OFB
P25: CBC　P27 CTR
P28: 证明CTR CPA安全
P30: IV的不确定的目的
P31: 非确定加密三种方法
P32: $PrivK^{cca}_{A,\Pi}(n)$
P33: 理解CCA
P34: padding-oracle 攻击☆

PPT5: 块密码
P5: 混淆扩散范式
P6: SPN
P7: S盒可逆
P8: 雪崩效应
P9: KPA for 块密码 ☆
P11: Feistel 网络
P13: DES
P14: DES大纲 { f / S / key编排
P15: DES的弱key
P20: Double DES
P21: Meet in middle
P22: DESX　P23: Triple DES
P24 AES
P25 DES对AES
P27 线性分析 ☆
P31 差分分析 ☆

P4: $Invert_{A,f}(n)$
P5: OWF/OWP的定义
P7: 例题
P8: HCP
P9: HCP对所有OWF
P10: OWF→PRG
P11: OWF→PRG→PRF
P12: OWF→PRG→PRF→PRP

PPT7: MAC-CRHF
P4: MAC的语法
P5: MAC的安全性
P6: MAC安全的定义 $MacForge_{A,\Pi}(n)$
P8: 例题
P9: MAC的应用
P10: 构造安全MAC (PRF, 定长)
P11 证明安全MAC
P12 变长MAC
P14: CBC-MAC
P16: 变长CBC-MAC → 都基于CBC-MAC
P17: 集合MAC
P18: 哈希fun
P19: 定义CR
P21 例题
P22: 哈希fun的应用
P24: MD变换
P25: MD变换的安全性
P26: 块密码的CRHF
P28: HASH then MAC
P29: NMAC
P30: HMAC
P31: HMAC的安全性
P33: 信息论MAC安全 $MacForge^{1-time}_{A,\Pi}$
P34: 理解信息论MAC安全
P35: 信息论安全MAC构造
P36: SUF 构造
P37: SUF的安全性证明
P38: 信息论安全MAC的限制

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
地址：哈尔滨市南岗区西大直街92号
邮编：150001

PPT8: CCA-ae

P3 $\min^{cca}_{A,\Pi}(n)$
P4: 信息传递方案
P5: AuthA(n)
P6 例题
P8: Enc+MAC的组合
P9: CCA构造
P10: 证明CA
P13: AE理论实践
P14: 安全信道的实现
P15: 不确定性CPA安全
P16: SIV for 确定性加密
P17: wide PRP
P18: 可调加密 (有TCTS)
P19: KDF
P20: PBKDF
P21: IV, nonce, Counter, Salt, tweak

PPT9: PubK

P: NS对称密钥协议
P: Merkle问题 (无TTP的key交换)
P: 公钥加密的定义
P: CPA安全 $PubK^{cpa}_{A,\Pi}(n)$
P: 混合加密
P: 混合加密的安全性
P: 混合加密的应用
P: TDP定义
P: TDP族的定义
P8 例题
P: TDP→公钥加密
P: 证明
P: $PubK^{cca}_{A,\Pi}(n)$
P: 例题
P: 去进的CCA2加密
P: ROM模型
P: 简易例证
P: TDP+RO+PubK
P: TDP+RO+PubK CCA
P: TDP+ZRO

PPT10 RSA

P4: 课本RSA
P5: 同余与模运算
P6: 模运算的应用
P: 群
P: 群的性质
P10: 欧拉定理|费马定理
P11: 无模数下的难题
P15: GenRSA
P16: RSAinv A, GenRSA (n):
P17: 构造TDP
P19: de攻击
P21: 共模攻击
P22: CCA攻击
P24: Padded RSA
P26: OAEP
P27: OAEP Plus
P28: 各种攻击
P29: 故障攻击

PPT11 DH

P3 循环群生成元
P4: 离散对数问题
P6 离散对数群
P7 二次剩余 Z_p^* 子群
P8: DLog$_{A,G}$(n)
P9: CDH, DDH
P10: 密钥交换协议
P11 DH Key交换协议
P12 证明
P14: 三方Key交换
P16: Elgamal加密方案
P17 例子
P18 证明
P21: CCA in Elgamal
P24: 椭圆曲线群
P25: 椭圆曲线点的加法

PPT12 数字签名

P4 数字签名的语法
P5 定义签名安全
P6: RSA签名及其安全性
P: Hash RSA签名
P: Schnorr身份认证方案
P10 证明 签名
P11 Fiat-Shamir变换
P12: DSS/DSA
P13: 不安全性
P14: OTS
P15: Lamport's OTS
P17: 证明
P18: 状态签名
P19: 基于链的签名
P20 树的签名方案
P21: 无状态方案
P25: certificate与PKI环境
P26: 证书吊销权及攻击 语

PPT13: 协议 填空!

P5: 协议种类
P6: 协议攻击
P7: 三次传递与互锁协议
P8: 中间人攻击
P10 双线性映射
P11 Joux's key交换协议
P12: 基于身份的加密
P13: BF IBE方案
P14: 盲签名 P15: 群签名 P16: 环签名
P18: Shamir秘密共享
P19 门限密码
P20 承诺方案
P21: 0知识证明
P24: 0知识证明+承诺
P25 Schnorr协议
P26: 攻击RSA (EXP)
P27 保护隐私查询
P28: Rabin's OT协议 P29: 盲数据查询
P30 安全的多方计算
P31 同态加密
P: 量子计算与模型
P34 量子密钥分发