**第2期\_纪要**

【基本理论知识类】

**时间 | 2020年10月23日星期五**

**参与人员 |王立军、张驰、郭子帅、裴中岳、康世明、李未**

**分享人：李未、康世明**

**主持人：刘凯**

**记录员：王立军**

 **会议议题**

1. 分享人1：李未——SM2算法原理分享
2. 分享人2：康世明——SM3算法原理分享

**会议思路**

1. SM2算法

分享了SM2算法椭圆曲线加密的数学原理

二、SM3算法

分享了SM3算法的原理及要点，本质上即先将明文数据扩展到512的倍数，再迭代压缩得到长为256bit的哈希值

讨论：

1.SM3用途：检验完整性

2.公司sm2签名速度：400次/s,

3.进行sm2算法之前先进行哈希算法（sm3）,在保证原明文完整性的前提下，极大的提升SM2算法的加密速度

4. 对称加密和分组加密中的四种模式(ECB、CBC、CFB、OFB)原理讨论：

明文参与了SM4算法则密钥一样

明文不参与SM4算法则密钥不一样

1. 交流会要点整理
   1. 基本确定了拓展的基本理念和制度
   2. 分享并讨论了SM2、3、4算法的原理及应用注意点
   3. 第3期人员安排及主题确定：
      1. 刘凯：密码标准体系
      2. 张弛： VPN
      3. 主持人：王立军
      4. 记录人：康世明

* **问题及任务跟踪**

1. 拓展会命名
2. 拓展产生资料汇总及研究生库的管理
3. 第4期分享人及主题确定

注：会议后要将上述问题整理到问题跟踪表中。