一．SM3：

1.Project: implement the naïve birthday attack of reduced SM3
对简化的 SM3 进行（原始的）生日攻击，寻找碰撞！
2.Project: implement the Rho method of reduced SM3
对简化 SM3 的基于 Rho 因式分解方法寻找碰撞。
要求：找到的碰撞越长，分数越高！
3. Project: implement length extension attack for SM3, SHA256, etc.
对 SM3、SHA256 等方案实施长度扩展攻击。
4. Project: do your best to optimize SM3 implementation (software)
在软件上尽最大努力实现 SM3，使得 SM3 的加密速度尽可能的快
确保你理解所写的每一行（不要复制粘贴）通过更快的运行获得更高的分数
5. Project: Impl Merkle Tree following RFC6962
依据协议 RFC6962 实现默克树
构造具有 10w 叶节点的 Merkle 树
可以对指定元素构建包含关系的证明
可以对指定元素构建不包含关系的证明
6. Project: Try to Implement this scheme （具体方案位于 SM3 pdf P18）
尝试实现 PPT 中给出的泛化哈希链方案——HashWires

二．SM4：无！

三．SM2:

注意这个 pdf 比较怪，一张 pdf 类似 A3 纸被等分为 4 份

分别为左上，右上，左下，右下。

1. Project: report on the application of this deduce technique in Ethereum with ECDSA
使用 ECDSA 在以太坊中应用该推断方法的报告（该方法位于 SM2 pdf P5 左下）
适用于验证签名中的公钥是否合法
2. Project: impl sm2 with RFC6979
按协议 RFC6979 实现 SM2.
3. Project: verify the above pitfalls with proof-of-concept code
用概念验证型代码验证上述签名方案的缺陷（在黑客圈中简写为 POC，指观点验证程序）
（简单理解，如果 k 泄露了那么 d 也会泄露：代码实现功能：对于该签名方案在已知 k 的前提下可以在多项式时间内计算出 d）
该缺陷表格位于 SM2 pdf P7 右上
4. Project: Implement the above ECMH scheme
实施上述 ECMH 方案：椭圆曲线哈希族
该方案的描述位于 SM2 pdf P7 左下
5. Project: implement sm2 2P sign with real network communication
在真实网络通信环境下实现 sm2 的 2 部分签名过程。
6. Project: implement sm2 2P decrypt with real network communication

在真实网络通信环境下实现 sm2 的 2 部分解密过程。
56 部分的细节分别位于 SM2 Pdf P8 左上和右上

7. Project: PoC impl of the scheme, or do implement analysis by Google
对该方案实现其观点验证程序或者 Google 进行分析。
该方案主要是谷歌用户的 password 验证系统，位于 SM2 Pdf P8 左下

四．比特币 1：

1. Project: forge a signature to pretend that you are Satoshi
伪造合法签名使得你可以被认为是 Satoshi
ECDSA 未检查签名邮件时伪造签名，位于 bitcon (没有 public 的那个) pdf P31

五．比特币 2：

1. Project: send a tx on Bitcoin testnet, and parse the tx data down to every bit, better write script yourself
在（比特币测试网）Bitcoin testnet 上发送文本，并将文本数据解析到每一位，最好自己编写脚本
位于有 public pdf P9
这两个 PDF 内容基本完全一样，没想到 project 还不一样，有 public 的那个其实也有四中的那个 project 不重复写了，一模一样！

六．以太坊：

1. Project: research report on MPT
MPT 研究报告，Merkle Patricia Trie 方案的描述位于 eth pdf P9

七．零知识证明：无

八．zk arithmetization：无

九．zk-SNARKs：无（P8,有个 project idea，我感觉好像不是作业）

十．王美琴老师：Real World Cryptanalyses

1. Project: Find a key with hash value “sdu_cst_20220610” under a message composed of your name followed by your student ID. For example, “San Zhan 202000460001”.
如果消息格式为姓名+学生 ID，需要找到散列值为“sdu_cst_20220610”的 hash 对象（hash 的原始信息）。例如，“San Zhan 202000460001”。
位于 Real World Cryptanalyses ppt P38

2. Project: Find a 64-byte message under some k fulfilling that their hash value is symmetrical.
在一些 k 下找到一个 64 字节的消息，满足其哈希值是对称的。
位于 Real World Cryptanalyses ppt　P45