汇报要求：

1. 由组长或某个组员介绍课题执行情况，可以包括算法原理、需求分析、软件设计、关键算法、软件测试或性能分析；10分钟左右

2. 每个组员介绍自己在课题中的主要工作，每人1-2分钟，可以合在课题执行情况介绍中讲解。

3. 最终课题小论文在6月20日之前提交，发到我的qq邮箱：59681241。

汇报顺序：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 课题名称 | 组长 | 组员 |
| 1 | 祖冲之算法的实现 | 苏一博 | 陈子琦、黎蕴锋、夏靖森、谯凯 |
| 2 | 祖冲之算法的实现 | 何睿 | 蓝浩诚、陆圣珩、戴芙蓉、潘衍伶 |
| 3 | AES算法的实现 | 程子岩 | 黄毅、黄子健、王承杰、辜心 |
| 4 | SM4算法的实现 | 王建业 | 郑烁、彭煜、倪星宇、郑涵、白杰 |
| 5 | RSA算法的实现 | 唐金森 | 唐雨彤、张靖霖、董佳宇、邹凯 |
| 6 | 大整数分解的实现 | 叶澄锋 | 杨榆丰、徐浩宸、雷程宇、姜人楷 |
| 7 | RSA算法的实现 | 卿正 | 吕志伟、唐灿、周付鹏、任泽琛、冷鹏飞 |
| 8 | 大整数分解的实现 | 金辉 | 金煜昊、刘忠奇、王宏阳、欧文旭、王庭翔 |
| 9 | ECC算法的实现 | 杨语澈 | 宋文凯、陈彪、李博超、许熠 |
| 10 | SM2加密算法的实现 | 杨映雷 | 曹洪水、黄飞羽、宾翊轲、陈奎、张骁 |
| 11 | SHA-1算法的实现 | 肖凌志 | 刘靖、周玉川、张澜潇、李卓然、纪尹钦 |
| 12 | SM3算法的实现 | 陈子明 | 陈曦、罗嗣达、张妍、刘振宇、严航 |
| 13 | 求解离散对数算法的实现 | 资重阳 | 何幸、张宇、易道宇、杨珮文 |
| 14 | DSS数字签名算法的实现 | 胡书成 | 许智伟、王桂石、潘怀宇、冯睿琪、董英杰 |
| 15 | DSS数字签名算法的实现 | 吴忻苒 | 倪雅琼、伯岁月、冯思乐、何佳芩、李好 |
| 16 | PKI系统的实现 | 潘文韬 | 张亚男、白锋硕、张驰、蔡志轩、刘泽楷 |
| 17 | PKI系统的实现 | 郝若帆 | 胡旺洋、朱思宇、李松浩、赵子号、孙逸翔 |
| 18 | Diffie-Hellman密钥交换的实现 | 胡远杭 | 杨懿斐、裴钰洋、孟林晓宇、魏贤、廖泽宇 |
| 19 | Diffie-Hellman密钥交换的实现 | 王瑞 | 杨诚然、潘泳锋、贾毅凡、李思远、洪宇凯利 |
|  |  |  |  |