1. 上午上了四节英语课；
2. 下午上了田老师的分组密码学，讲了两篇论文，一篇是没有在随机预言机模型下的短签名，基于q-SDH假设证明其安全性，又提出了一个弱签名方案，在强假设和弱假设下，老师说强假设来证明其安全性更有说服力。另外一篇是在解决K-CAA问题的基础上来证明其安全性，又相继的扩展了k-wCDHP问题和K+1EP问题。在这节课上，我学到了，老师说一篇论文要抓住核心，基于什么问题？怎么来证明？
3. 接下来将继续看一下这两篇论文，然后看关于车联网无证书签名的一篇论文。