创新创业实践课项目：

成员：

姓名：高畅

学号：202100150084（个人完成）

说明：

本课程共要求完成 21 个项目（老师说 project13 与 project20 重复了，project20 不用做），本人共完成 16 个项目。所有项目涉及编程语言包含：C、C++、Python。

仅本人为一个小组，**所有上传的项目都有详细的项目简介、具体说明、实现结果、实现方式。可以在每个项目对应的文件夹的 readme 查看。（若不想一个一个查看，可以下载下面名为“总”的 word 文档，里面汇总了所有项目的 readme，可以一起看）**

完成的项目有：

*Project1: implement the naïve birthday attack of reduced SM3

*Project2: implement the Rho method of reduced SM3

*Project3: implement length extension attack for SM3, SHA256, etc.

*Project4: do your best to optimize SM3 implementation (software)

*Project5: Impl Merkle Tree following RFC6962

*Project8: AES impl with ARM instruction

*Project9: AES / SM4 software implementation

*Project10: report on the application of this deduce technique in Ethereum with ECDSA

*Project11: impl sm2 with RFC6979

*Project15: implement sm2 2P sign with real network communication

*Project16: implement sm2 2P decrypt with real network communication

*Project17：比较 Firefox 和谷歌的记住密码插件的实现区别

*Project18: send a tx on Bitcoin testnet, and parse the tx data down to every bit, better write script yourself

*Project19: forge a signature to pretend that you are Satoshi

*Project21: Schnorr Bacth

*Project22: research report on MPT

未完成的项目：

*Project6: impl this protocol with actual network communication

*Project7: Try to Implement this scheme

*Project12: verify the above pitfalls with proof-of-concept code

*Project13: Implement the above ECMH scheme

*Project14: Implement a PGP scheme with SM2