2021-2022春夏密码学回忆卷 任课教师：白洪欢

选择：

- 3重des
- ecc私钥推出公钥
- 乘法逆元
- EC_POINT_set_compressed_coordinates_GFp()函数使用
- MD5填充（报文长度为56的情况）
- aes里面（3，1，1，2）多项式逆元
- rc4种子密钥最大长度
- BN_mod_exp()函数使用
- aes加密中，密钥长为256，求种子密钥长度（？不确定了）
- EC_POINT_mul()函数使用

简答：

- des加密，48位进入sbox得到32位过程
- ecsda证明
- 手写des_cfb_encrypt()函数
- rsa加密信件并用rsa做签名的加密、解密、签名、验证签名的过程

计算：

- Enigma输入输出计算，涉及中间齿轮双跳
- ecc加密解密过程
- aes农夫算法，写出函数，计算0x92*0x0B mod0x11B并写出过程

证明：

- RSA加密算法
- 裴蜀定理：gcd(n，u) = an+bu