2021-2022 近代密码学

1. 给出密码体制的完善保密性的定义并举例。
2. 古典密码体制，为 A-Z 编码 0-25，加密算法为 c=7m+3 (mod 26)，求解密算法，并解密 RHEAFS。
3. 什么是双重 DES？什么是三重 DES？解释对双重 DES 的中间相遇攻击。
4. 写出平衡的 Feistel 网络，给出使用平衡 Feistel 网络的分组密码实例。
5. 用 BM 算法计算 000100110101111 的线性综合解。
6. 写出 ElGamal 体制并证明解密算法的正确性。
7. 写出 CFB 工作模式下的 Hash 函数 H。当密钥公开时 H 是弱无碰撞的吗？是强无碰撞的吗？若不是强无碰撞，给出消息 $x \neq y$ 但 $H(x)=H(y)$。

1-6t 15 分，7t 10 分

Lyx