信息安全作业 2

190110429-何为

1. **Alice 和 Bob 使用 Diffie_Hellman 协议协商共享密钥，得知使用的素数 q=13，原根 a=2。如果 Alice 传递给 Bob YA=12，则 Alice 的随机数 XA 是多少？如果 Bob 传递 Alice YB=6，则共享的密钥 K 是多少？**

答:

由离散对数得：$Y_A = a^{X_A} \ (mod\ q)$，即$2^{X_A} \ (mod\ 13) = 12$，遍历$0 < X_A < 13$，得$X_A = 6$，

当 Alice 收到 Bob 的密文$Y_B = 6$后，可以计算$K = (Y_B)^{X_A} \ (mod\ p) = 6^6 (mod\ 13) = 12$，所以共享密钥$K = 12$。

2. **如果攻击者截获了 Alice 发给 Bob 的消息 C 为 10，并得知加密密码是 RSA（公钥：e=5，n=35），那么明文 M 是什么？**

答:

首先需要对 n 进行质因数分解，得到$n = 35 = 5 \times 7$，所以$\varphi(n) = (5-1) \times (7-1) = 24$，所以可以得到密钥$d \equiv e^{-1} \ mod\ \varphi(n) = 5^{-1} \ mod\ 24 = 5$。

通过密钥可以对密文 C 进行解密$m = c^d \ mod\ n = 10^5 \ mod\ 35 = 5$，所以明文 M 为 5。