网络安全技术课堂作业五

> 朱浩泽 1911530 计算机科学与技术

1. $C = M^e \mod n = 89^7 \mod 187 = 166$
2. $\phi(187) = 10 \times 16 = 160$

   $d = e^{-1} \mod 160 = 23$

   $\therefore M = C^d \mod n = 163^{23} \mod 187 = 89$
3. $C = M^e \mod n = 88^7 \mod 187 = 11$

   $\because 88 \mod 11 = 0 \wedge 187 \mod 11 = 0$

   $\therefore C\text{可以分解}n = 187$