信息安全第三次实验

1 为了加深对RSA算法的理解，根据已知参数：$p=17, q=11, e=3, M=19$，手工计算私钥d和对应的密文，然后对密文进行解密。

由于p, q为素数，可得

$$\begin{aligned} n &= p \times q = 187 \\ \Phi(n) &= (p-1)(q-1) = 16 \times 10 = 160 \end{aligned}$$

因为$e=3$，$\Phi(n)=160$，$\mathrm{ed} \equiv 1 \pmod{\Phi(n)}$，可得$e$模反元素$d$的表达式

$$3d - 1 = 160k$$

求得d的可行解为107。

由此可得，加密公钥为$(n=187, q=3)$，私钥为$(d=107, q=3)$。

对于$M=19$以及公钥，根据加密公式

$$m^e \equiv c \pmod{n}$$

解得$c=6672$。

对于$c=6672$以及私钥，根据解密公式

$$c^d \equiv m \pmod{n}$$

我们很难直接求解m，原因在于c^d的数量级过于庞大。于此，由于$n = p \times q$，
且p, q为素数，我们可以通过分治的策略降低数据规模。假设$x = 6672^{107}$（即为m^e），
根据费马小定理$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$，可得

$$\begin{aligned} x &\equiv 8 (\mathrm{mod}\ 11) \\ x &\equiv 2 (\mathrm{mod}\ 17) \end{aligned}$$

下面我们可以通过推导所得求出m

$$\begin{aligned} x &= 8 + 11k \\ 8 + 11k &\equiv 2 (\mathrm{mod}\ 17) \\ 11k &\equiv 11 (\mathrm{mod}\ 17) \\ 3 \times 11k &\equiv 3 \times 11 (\mathrm{mod}\ 17) \\ k &\equiv 1 (\mathrm{mod}\ 17) \\ k &= 1 + 17l \\ x &= 8 + 11(1 + 17l) \\ x &\equiv 19 (\mathrm{mod}\ 187) \end{aligned}$$

2 简述对称加密体制和非对称密码体制的各自特点。

最直观的区别：对称加密体系采用公钥、私钥对，非对称加密体系采用单一密钥。