Theory of Computation

Homework 5

Due: 2016/01/05

Problem 1. Calculate $(2015|999)$ and $(2016|999)$. **(Answers without procedure will get 0 points)**.

Solution.

We have that

$$\begin{aligned}(2015|999) &= (17|999) = (13|17) = (4|13) = 1,\\ (2016|999) &= (18|999) = 0.\end{aligned}$$

□

Problem 2. Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA. Which of the parameters $e_1 = 32, e_2 = 49$ is a valid RSA exponent? What is the value of the private key d?

Solution.

For a valid parameter e, we must have that $\gcd(e, \phi(pq)) = 1$. Notice that $\phi(pq) = 40 \times 16 = 640$ and

$$\begin{aligned}\gcd(e_1, \phi(pq)) &= \gcd(32, 640) = 32,\\ \gcd(e_2, \phi(pq)) &= \gcd(49, 640) = 1,\end{aligned}$$

hence $e_2 = 49$ can be used as a valid RSA exponent. Also

$$d \equiv 49^{-1} \pmod{640} \equiv 209 \pmod{640}.$$

□