Homework Set 9 (Lecture 33)

Problem 2

Example 25. Bob's public RSA key is $(N,e)=(35,19)$. His private key is $d=19$. For signing, Bob uses the (silly) hash function $H(x)=x \pmod{22}$. Determine Bob's signature s of the message $m=361$.

Solution. $H(m)=361 \pmod{22}=9$. The signature therefore is $s=H(m)^d \pmod{N}=9^{19}\equiv 9 \pmod{35}$.

Problem 3

Example 26. Alice uses an RSA signature scheme and the (silly) hash function $H(x)=x_1+x_2$, where $x_1=3x \pmod{11}$ and $x_2=2x \pmod{29}$, to sign the message $m=1299$ with the signature $s=121$. Forge a second signed message.

Solution. Since we have no other information, in order to forge a signed message, we need to find another message with the same hash value as $m=1299$. From our experience with the Chinese remainder theorem, we realize that changing x by $11\cdot 29$ does not change $H(x)$. Since $1299+11\cdot 29=1618$, a second signed message is $(1618,121)$.