simple RSA digital signature example

1. In secret, Alice picks primes p_A, q_A 101513, 103687, computes $n_A = p_A q_A = 10525578431$, computes $\phi(n_A) = (p_A - 1) * (q_A - 1) = 10525373232$, picks $e_A = 10516948735$, and computes $d_A = e_A^{-1} \pmod{\phi(n_A)} = 4067691823$. What numbers does Alice publish?

2. How can Alice check that d_A is correct?

3. In secret, Bob picks primes p_B, q_B 103171, 103979, computes $n_B = p_B q_B = 10727617409$, computes $\phi(n_B) = (p_B - 1) * (q_B - 1) = 10727410260$, picks $e_B = 9907600121$, and computes $d_B = e_B^{-1} \pmod{\phi(n_B)} = -3860397619 = 6867012641$. What numbers does Bob publish?

4. Now assume Alice wants to send message $m = 8123478199$ to Bob. So she looks up Bob's public RSA values n_B, e_B and encrypts $m' = f(m)$ in the usual way. What number m' does Alice send Bob?

5. How does Bob recover m from m'?

6. So far this is just the usual RSA. Now, let's see a digital signature: Alice will sign the message she just sent to Bob, i.e. she will confirm that only she could have sent it. So Alice computes $s = m_A^d \pmod{n_A}$, then computes $s' = s_B^e \pmod{n_B}$, and sends s' to Bob. What number is s? What number is s'? How does Bob recover s from s'?

7. Finally, how does Bob confirm that s is Alice's signature of m?

1. Alice publishes n_A and e_A.

2. To check that d_A is correct, verify that $d_A * e_A = 1 \pmod{\phi(n_A)}$.

3. Bob publishes n_B and e_B.

4. Alice sends Bob $m^{e_B} \pmod{n_B} = 1662187982$.

5. Bob recovers m from m' using $m = m'^{d_B} \pmod{n_B}$

6. $s = 8345304319$. $s' = 6120354784$. Bob recovers s from s' using $s = s'^{d_B} \pmod{n_B}$.

7. Bob verifies that $s^{e_A} \pmod{n_A} = s'$. Only Alice could have found this s'.