Using RSA for authentication

RSA has a nice property that many public key algorithms don't.

The encryption and decryption algorithms commute.

Thus I can "sign" a message as follows.

- Suppose I have secret key d and public key (e, n).
- Suppose my message is b. With $0 \leq b < n$
- I'll compute $a = b^d \bmod n$ and send you both b and a.
- On receipt, you "encrypt" a to get $b^{'} = a^e \bmod n$ and check that $b' = b$.
- Only someone who knows d could (feasibly) have calculated a from b, n, and e.