In Sage we can also see an example of RSA signing/verifying:

sage: p = random\_prime(10000); p

1601

sage: q = random\_prime(10000); q

4073

sage: N = p\*q

sage: R = IntegerModRing(N)

sage: phi\_N = (p-1)\*(q-1)

sage: e = 47

sage: gcd(e, phi\_N)

1

sage: d = xgcd(e,phi\_N)[1] % phi\_N

sage: # Now by expoenentiating with the private key

sage: # we are effectively signing the data

sage: # a few examples of this

sage: to\_sign = randint(2,2^10); to\_sign

650

sage: # the signature is checked by expoenentiating

sage: # and checking vs the to\_sign value

sage: signed = R(to\_sign)^d; signed

2910116

sage: to\_sign == signed^e

True

sage: to\_sign = randint(2,2^10); to\_sign

362

sage: signed = R(to\_sign)^d; signed

546132

sage: to\_sign == signed^e

True

sage: # we can also see what happens if we try to verify a bad signature

sage: to\_sign = randint(2,2^10); to\_sign

605

sage: signed = R(to\_sign)^d; signed

1967793

sage: bad\_signature = signed - randint(2,100)

sage: to\_sign == bad\_signature^e

False