crypto study guide chapters 6,7

1. be familiar with chapters 6,7 and public key crypto handout
2. Here is a toy RSA example with hashing and digital signatures. Alice and Bob use the usual RSA public key cryptosystem. They convert text to numbers like this:

```
 a b c d e f g h i  ...      msg: 'send cash'
 1 2 3 4 5 6 7 8 9 ...

   s  e  n      d  _  c      a  s  h
[  s  e  n]   [ d  _  c]   [ a  s  h]
[ 19  5 14]   [ 4 27  3]   [ 1 19  8]

 19*32^2 +      4*32^2 +     1*32^2 +
  5*32^1 +     27*32^1 +    19*32^1 +
 14*32^0 +1 =   3*32^0 +1 =  8*32^0 +1 =
    19631         4964          1641    base 32*32*32
```

Alice and Bob's public hash function $h(t)$ maps each resulting number t to $(t * t) mod 23$, and then converts it into a character using the above method. So here, `f p r`.

Alice's public info: modulus $n_A = 12916667$, exponent $e_A = 769$.

Bob's public info: modulus $n_B = 12873719$, exponent $e_B = 401$.

Alice knows $n_A = 3581 * 3607$, so $\phi(n_A) = (3581 - 1) * (3607 - 1) = 12909480$.

Alice uses `exteuclid(12909480,769)` from github

`https://github.com/ryanbhayward/algs`

`12909480 * -186 + 769 * 3122449 = 1`, so her secret exponent d_A is 3122449.

Bob knows $n_B = 3583 * 3593$, so $\phi(n_B) = (3583 - 1) * (3593 - 1) = 12866544$.

Bob uses `exteuclid.py`

`12866544 * -159 + 401 * 5101697 = 1`, so his secret exponent d_B is 5101697.

Alice wants to send and sign Bob the message `send cash`. What operations does Alice perform? And then, what operations does Bob perform?

(a) Alice converts her text message into numeric form:
`chars2num('send cash') = [19361  4964 1641]`

(b) Alice hashes message:
`hash([19361 4964 1641]) = 'fpr'`
then converts into numeric form: `chars2num('fpr') = [6675]`

(c) Alice signs hash using her secret exponent `d_A` : `pow(6675,dA,nA)` 1866650.

(d) Alice encrypt message, signed hash, sends to Bob

```
sen   19361  pow(  19361,eB,nB)    2770380
d c    4964  pow(   4964,eB,nB)    721679
ash    1641  pow(   1641,eB,nB)    3682320
fpr 1866650  pow(1866650,eB,nB)    2787744
```

3. Bob receives 2770380 721679 3682320 2787744 from Alice. Now what?

(a) Bob decrypts, using his secret exponent:

```
pow(2770380, dB, nB)   19361
pow( 721679, dB, nB)    4964
pow(3682320, dB, nB)    1641
pow(2787744, dB, nB) 1866650
```

(b) Bob recovers message, signed hash

```
   19361     sen
    4964     d c
    1641     ash
 1866650     fpr

message:    send cash
signed hash:   fpr
```

(c) Bob unsigns the hash

`pow(1866650, eA, nA)  6675`

(d) Bob verifies the hash

`chars2num('fpr') 6675`