Thanks a lot to the people who took notes!

Examples how RSA works in practice

package name 'pari-gp'
Pari-gp is a general computer algbra system; this is what Tanja will provide on the laptops if the exam takes place in person. It has all the number theory functions we need and very large precision.
https://pari.math.u-bordeaux.fr/dochtml/html/Arithmetic_functions.html#isprime

Check if p and q are prime (Fermat's primality test):

a^{p-1} = 1 mod p for all a with gcd(a,p) = 1

Example in practice:
p = 103
q = 107

Check base a = 2, 3, 5
Primality test is true -> p probably prime or a Carmichael number
Primality test is false for some a -> p is certainly not prime

Here: all three come back as " p probably prime or a Carmichael number"

We can also check that 103 is prime by checking for prime divsors up to \sqrt(p},
in this case there is none, so 103 is prime.
in gp type
isprime(103)
which answers 1 to say that 1 is prime (check out the documentation for different options)

Next compute n:
n = p*q = 11021

Next compute phi:
phi = (p-1)*(q-1) = 10812

Now, for exponentiation, can we use e = 3? Basically no. (Why? because phi was divisible by 3)
Use e = 5

Compute bezout (=extendend Euclidean algorithm):
bezout(5, 10812)
= (4325, -2, 1))
meaning that
4325 * 5 - 2 * 10812 =1

bezout is Pari-GP's command for XGCD.

To compute XGCD by hand:
Check quotient and remainder
10812/5.0 = 2162.4000000

q = 2162
r = 2

then
5/2.0 = 2.5, so the next quotient is 2
r = 1

d = 2162*2 + 1

Using the algorithm which will appear on the exercise sheet (use that if you don't have your favorite way to compute XGCD -- or to teach it to your calculator):

```
10812     1        0
    5     0        1
    2     1    -2162
    1    -2     4325
```

Check whether e*d mod(phi) = 1
Yup Mod(5*4325,phi)= Mod (1, phi)

Difference mod operator and %
"Mod" operator gives remainder and modulus, residue class
"%" only gives remainder, the integer

Key generation
Create public key: (n,e)
Private key: (n,d)

pgpdump to display pgp key
Format specified in RFC 4880

e = 01 00 01 (binary) means 2^16 + 1 = 65537

Showing Secret/private key in pgpdump:
displays n, e, d, p, q and u in hexadecimal
Recall u = p^{-1} (mod q)

Alice's public key (n,e) = (11021,5)
Alice's private key (n,d) = (11021,4325)

Somebody wants to encrypt a message to Alice

m = 1234 < n
m^5 = ...

Use square and multiply:
5 = 2^2 + 1 = [101]_{2}

n=11021
Mod(m^2, 11021) = Mod(1858, 11021)
Bit is 0, so no mult
Mod(1858, 11021)^{2} = Mod(2591, 11021)
Bottom bit = 1, so multiply by m
Mod(2591, 11021)*Mod(m,n) = Mod(1204, 11021)

(Use %N to refer to output N in pari-gp)

(Pari reduces along the way ... and so should you!)

CRT method:

Example:
Bob has n = 164063, e = 17 and receives
c = 6215
He used p = 359 and q = 457 and got
d = 57617
dp = d % (p-1) (Exponent gets smaller) = 337
dq = d % (q-1) = 161
cp = c % p = 112
cq = c % q = 274
mp = Mod(cp^dp, p) = Mod(89, 359)
mq = Mod(cq^dq, q) = Mod(172, 457) (mp & mq qre useful when calling chinese(), i.e 2 inputs instead of 4)
chinese(mp,mq) = Mod(75120,164063)
chinese=CRT in pari-gp), the inputs to chinese are of the form Mod(a,b); which matches the above

Is the CRT calculation a bottleneck? No, u = p^{-1} mod q is included in key. Then
m = mp + u * p * (mp - mq) mod n
(you can compute this by first computing p * (mp - mq) % q and then multiplying the result of this by u and adding mp, this typicaly means that no reduction mod n is needed.

Remarks:

- *1) important to reduce c mod p and mod q, and to reduce d mod p-1 and mod q-1*
- *2) exponents are mod phi(p) etc., needs that base and p are coprime*

If an attacker disturbs Bob iin the RSA-CRT computation so that he accidentally computes
mp = Mod(165, 359) and then gets plaintext
m' = chinese(mp,mq) = Mod(129046, 164063)

as attacker I know that the correct plaintext is 75120, what can you learn?
Hint:
Mod(75120 - 129046, q) = Mod(0, 457)
Mod(75120 - 129046, p) = Mod(283, 359)

Considering the homework sheet:
The homework sheet will include algorithms for XGCD and CRT if you are not sure how to do these (or

how to teach them to you computer)
Submit homework by email

Postscript
I had messed up in copying the numbers. what I wanted to give you with CRT is
c= 66215,, d = 57617, p = 359, q = 457.
Figure out what the plaintext was.