2018 - Tallteori MAT-1300

Fra Obliger:

1. Beskrive Pollard faktoriseringsalgoritmer
2. Anvende Eulers teorem innen RSA kryptering
3. Kjenne til historiske kryptosystemer som Vigenère- og blokkshiffrering
4. Ha inngående kjennskap til RSA offentlig nøkkel kryptering og signering
5. Forklare hvorfor nøkkelen ikke røpes under utvekslingen i Diffie-Hellman nøkkelutveksling
6. Bruke teorien om kvadratrøtter modulo heltall til minimale kunnskapsprotokoller

For eksamen:

1. Løse lineære kongruensligninger
2. Beherske Euklids utvidede algoritme til å finne inverser modulo heltall
3. Kunne anvende kinesisk restteorem
4. Beherske rask (modulær) eksponensiering
5. Kunne anvende Hensels lemma til å finne løsninger til polynomligninger mod p^k
6. Beherske Fermats og Eulers teorem
7. Vite: pseudoprimtall, Carmichael tall, sterke pseudoprimtall og Euler pseudoprimtal
8. Regne med multiplikative aritmetiske funksjoner
9. Vite: "sum av divisorer", "antall divisorer", "Eulers Phi-funksjon"
10. Kunne utføre Möbius Inversjon av aritmetiske funksjoner
11. Gjøre rede for hvilke heltall som har primitiv rot, og regne antall av dem
12. Kjenne hva orden av heltall mod n er, og regne den ut
13. Finne primitiv rot for små heltall og kunne bruke primitive røtter til å løse enkle ligninger
14. Forklare hva en kvadratisk rest og ikkerest
15. Kunne bruke kvadratisk resiprositet til å regne ut Legendresymbol
16. Kunne anvende Jacobisymbolet og resiprositetteoremet til å regne ut Legendresymbol
17. Beregne kvadratrøtter av a modulo n når n er et produkt av to primtall