

Løsningsforslag/fasit øving 6 i LO700D, høsten 2005.

Del A - Review questions

- 9.3 Encryption/decryption:** The sender encrypts a message with the recipient's public key. **Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message. **Key exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.
- 9.5** A **one-way function** is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible.
- 9.6** A **trap-door one-way function** is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.

Del B - Problems

(Her er kun fasiten, løsningsforslag ligger på

<http://www.itu.dk/courses/ODSK/F2004/DOCS/solutions-week4.pdf>)

9.2a $n = 33$; $\phi(n) = 20$; $d = 3$; $C = 14$, $M=5$.

9.3 5

9.4 3031

Del C - spørsmål: Bob sender bedriftshemmeligheter til Alice kryptert med RSA og Alice's offentlige nøkkel (e,n) . Anta at du har fått tilgang til det ene primtallet p ($n=pq$). Forklar hvordan dette er relevant for sikkerheten.

Et vesentlig poeng for sikkerheten til RSA er at tallet n er vanskelig å faktorisere i primtallsfaktorene p og q (dvs. umulig innenfor relevant tidsrom og med begrenset regnekraft). Når n og p er kjent, så er i praksis faktoriseringen av n kjent, siden $q=n/p$. Når p og q er kjent, kan man lett finne $\Phi(n) = \Phi(p*q) = \Phi(p)*\Phi(q) = (p-1)(q-1) = (p-1)(n/p-1)$. Når man kjenner verdien av $\Phi(n)$ kan Euklids utvidede algoritme brukes til å finne den hemmelige eksponenten (den private nøkkelen) d :
 $d = e^{-1} \text{ mod } \Phi(n)$

Og da er det trivielt å dekryptere innkommende meldinger c siden man har tilgang til de samme opplysningene som den tiltenkte mottakeren av den hemmelige meldingen;

$$m = c^d \bmod n.$$