Kryptologi og RSA – løsningsforslag til opgaver

Jonas Lindstrøm Jensen, (jonas@imf.au.dk)

Løsninger

1. JGL OGF FKI.

2. JFN OFH FJK.

3. STADIGT FLERE DANSKERE OPLEVER AT DERES COMPUTERE BLIVER ANGREBET AF VIRUS ORME OG ANDRE ONDSINDEDE PROGRAMMER SAMTIDIG ER ANTALLET AF FORSØG PÅ AT FRANARRE DANSKERNES KODER OG HEMMELIGE OPLYSNINGER VED HJELP AF FALSKE EMAILS OG HJEMMESIDER STEGET MARKANT

4. (i) 1, (ii) 6, (iii) 1.

5. (i) og (iii).

6. 4, 12, 120.

7. $C = 9$, og vi kan $u = 3, v = 1$.

8. $p = 5$ og $q = 11$ så $\phi(55) = 40$, og vi kan derfor vælge $u = 23$ og $v = 4$. Da $2^{23} = 8388608 \equiv 8 \pmod{55}$ er den oprindelige besked 8.