Lukuteoria
Harjoitus 10/2007

1. Dekryptaa koodi 1213 0902 0539 1208 1234 1103 1374 kun kryptaus on suoritettu Pohlig-Hellmann-eksponenttisalakirjoituksella avaimena luvut $p = 2591$ ja $e = 13$.

2. Dekryptaa koodi 2206 0755 0436 1165 1737 kun kryptaus on suoritettu RSA:lla kryptausavaimena luvut $e = 13$ ja $n = 2747$.

3. Oletetaan, että RSA kryptausmetodia käytettäessä valitaan lohkon koko virheellisesti siten, että jollekin lohkolle P pätee

   (a) $n \mid P$,

   (b) $P > n$ ja $\text{syt}(P, n) = 1$.

   Miten tämä vaikuttaa ko. lohkon P dekryptaukseen?

4. Olkoot $a, b \in \mathbf{Z}$ siten, että $\text{syt}(a, m) = 1$ ja $a \equiv b \pmod m$. Osoita, että $\text{ord}_m a = \text{ord}_m b$.

5. Osoita, että luvulla 12 ei ole primitiivijuuria.

6. Osoita, että 3 ja 5 ovat primitiivijuuria modulo 14 eikä muita ei-kongruentteja primitiivijuuria ole.

7. Olkoon $a \in \mathbf{Z}$ ja $m \in \mathbf{N}$ siten, että $\text{syt}(a, m) = 1$. Osoita, että

   $$\text{ord}_m a = \text{ord}_m \bar{a},$$

   kun $\bar{a}$ on luvun a käänteisluku modulo m.

8. Oletetaan, että luvulla $m > 2$ on primitiivijuuri r. Osoita, että

   $$r^{\frac{\phi(m)}{2}} \equiv -1 \pmod m.$$

   (Vihje! Lemma 6.1.5).