STOCKHOLMS UNIVERSITET
MATEMATISKA INSTITUTIONEN
Avd. Matematik, Christine Jost

Uppgifter Kryptering - Facit
Algebra och kombinatorik

1. $\log_2(6) = 9$ och $\log_3(6)$ existerar ej.

2. Eftersom $a \equiv b \pmod{p-1}$ är $a = b + k(p-1)$ för något heltal k. Då är $g^a = g^{b+k(p-1)} = g^b \cdot (g^{p-1})^k = g^b$ i $\mathbb{Z}_p$, eftersom $g^{p-1} = 1$ i $\mathbb{Z}_p$ enligt Fermats lilla sats.

3. Alice skickar $A = g^a = 15$ till Bob och Bob skickar $B = g^b = 9$ till Alice. De enas om den gemensamma nyckeln $A' = B^a$ respektive $B' = A^b$, nämligen $A' = B' = 8$.

4. (i) $x = 4$
   (ii) $x = 2$

5. $m = 7$