

1. Beräkna $\log_2(6)$ och $\log_3(6)$ i \mathbb{Z}_{11} , om logaritmerna existerar.
2. Låt $g \in \mathbb{Z}_p$ för något primtal p , och antag att $a \equiv b \pmod{p-1}$ för heltal a och b . Visa att $g^a = g^b$.
3. Alice och Bob vill enas om en nyckel med hjälp av Diffie-Hellman-nyckelutbyte. De väljer att räkna i \mathbb{Z}_{17} och använda $g = 2$ som bas. Alice väljer den privata nyckeln $a = 5$ och Bob den privata nyckeln $b = 7$. Vilken information skickar Alice och Bob till varandra, och vilken gemensam nyckel enas de om?
4. Lös följande ekvationer:
 - (i) $x^5 = 16$ i \mathbb{Z}_{21}
 - (ii) $x^7 = 11$ i \mathbb{Z}_{13}
5. Du avlyssnar Alice och Bobs konversation som krypteras med RSA. Du får förutom den publika nyckeln $n = 15$ och $e = 3$ veta att krypterade meddelandet är $c = 13$. Dekryptera meddelandet!