Amela mora izračunati vrijednost $A = \mathrm{mod}(g^a, p) = \mathrm{mod}(3^{452}, 751)$ i poslati je Branku. Računanje ove vrijednosti svodi se na računanje $([3]_{751})^{452}$. Broj 751 je prost, tako da je $\varphi(751) = 751 - 1 = 750$. Kako je $452 < 750$, redukcija eksponenta nije moguća, nego prelazimo odmah na metod "kvadriraj-i-množi":

$$([3]_{751})^2 = [9]_{751}$$
$$([3]_{751})^4 = ([9]_{751})^2 = [81]_{751}$$
$$([3]_{751})^8 = ([81]_{751})^2 = [6561]_{751} = [\mathrm{mod}(6561, 751)]_{751} = [553]_{751}$$
$$([3]_{751})^{16} = ([553]_{751})^2 = [305809]_{751} = [\mathrm{mod}(305809, 751)]_{751} = [152]_{751}$$
$$([3]_{751})^{32} = ([152]_{751})^2 = [23104]_{751} = [\mathrm{mod}(23104, 751)]_{751} = [574]_{751}$$
$$([3]_{751})^{64} = ([574]_{751})^2 = [329476]_{751} = [\mathrm{mod}(329476, 751)]_{751} = [538]_{751}$$
$$([3]_{751})^{128} = ([538]_{751})^2 = [289444]_{751} = [\mathrm{mod}(289444, 751)]_{751} = [309]_{751}$$
$$([3]_{751})^{256} = ([309]_{751})^2 = [95481]_{751} = [\mathrm{mod}(95481, 751)]_{751} = [104]_{751}$$

Konačno je:

$$([3]_{751})^{452} = ([3]_{751})^{256}([3]_{751})^{128}([3]_{751})^{64}([3]_{751})^4 = [104]_{751} \cdot [309]_{751} \cdot [538]_{751} \cdot [81]_{751} =$$
$$= [32136]_{751} \cdot [43578]_{751} = [\mathrm{mod}(32136, 751)]_{751} \cdot [\mathrm{mod}(43578, 751)]_{751} =$$
$$= [594]_{751} \cdot [20]_{751} = [11880]_{751} = [\mathrm{mod}(11880, 751)]_{751} = [615]_{751}$$

Dakle, Amela šalje Branku vrijednost $A = 615$. S druge strane, Branko mora izračunati vrijednost $B = \mathrm{mod}(g^b, p) = \mathrm{mod}(3^{131}, 751)$ koja se svodi na računanje $([3]_{751})^{131}$:

$$([3]_{751})^{131} = ([3]_{751})^{128}([3]_{751})^3 = [309]_{751}\,[27]_{751} = [8343]_{751} = [\mathrm{mod}(8343, 751)]_{751} = [82]_{751}$$

Ovdje smo iskoristili činjenicu da smo vrijednost $([3]_{751})^{128}$ već ranije računali. Dakle, Branko šalje Ameli vrijednost $B = 82$.

Po prijemu informacije $A = 615$, Branko računa ključ k kao $k = \mathrm{mod}(A^b, p) = \mathrm{mod}(615^{131}, 751)$. Računanje ove vrijednosti svodi se na računanje $([615]_{751})^{131}$:

$$([615]_{751})^2 = [378225]_{751} = [\mathrm{mod}(378225, 751)]_{751} = [472]_{751}$$
$$([615]_{751})^4 = ([472]_{751})^2 = [222784]_{751} = [\mathrm{mod}(222784, 751)]_{751} = [488]_{751}$$
$$([615]_{751})^8 = ([488]_{751})^2 = [238144]_{751} = [\mathrm{mod}(238144, 751)]_{751} = [77]_{751}$$
$$([615]_{751})^{16} = ([77]_{751})^2 = [5929]_{751} = [\mathrm{mod}(5929, 751)]_{751} = [672]_{751}$$
$$([615]_{751})^{32} = ([672]_{751})^2 = [451584]_{751} = [\mathrm{mod}(451584, 751)]_{751} = [233]_{751}$$
$$([615]_{751})^{64} = ([233]_{751})^2 = [54289]_{751} = [\mathrm{mod}(54289, 751)]_{751} = [217]_{751}$$
$$([615]_{751})^{128} = ([217]_{751})^2 = [47089]_{751} = [\mathrm{mod}(47089, 751)]_{751} = [527]_{751}$$

Konačno je:

$$([615]_{751})^{131} = ([615]_{751})^{128}([615]_{751})^2 \cdot [615]_{751} = [527]_{751} \cdot [472]_{751} \cdot [615]_{751} =$$
$$= [152977560]_{751} = [\mathrm{mod}(152977560, 751)]_{751} = [362]_{751}$$

Dakle, tražena zajednička vrijednost ključa je $k = 362$. Znamo da istu vrijednost ključa mora dobiti i Amela, ali radi kontrole obavimo i postupak kojim Amela dolazi do vrijednosti ovog ključa. Ona ga računa kao $k = \mathrm{mod}(B^a, p) = \mathrm{mod}(82^{452}, 751)$:

$$([82]_{751})^2 = [6724]_{751} = [\mathrm{mod}(6724, 751)]_{751} = [716]_{751}$$
$$([82]_{751})^4 = ([716]_{751})^2 = [512656]_{751} = [\mathrm{mod}(512656, 751)]_{751} = [474]_{751}$$
$$([82]_{751})^8 = ([474]_{751})^2 = [224676]_{751} = [\mathrm{mod}(224676, 751)]_{751} = [127]_{751}$$
$$([82]_{751})^{16} = ([127]_{751})^2 = [16129]_{751} = [\mathrm{mod}(16129, 751)]_{751} = [358]_{751}$$
$$([82]_{751})^{32} = ([358]_{751})^2 = [128164]_{751} = [\mathrm{mod}(128164, 751)]_{751} = [494]_{751}$$

$$([82]_{751})^{64} = ([494]_{751})^2 = [244036]_{751} = [\mathrm{mod}(244036, 751)]_{751} = [712]_{751}$$
$$([82]_{751})^{128} = ([712]_{751})^2 = [506944]_{751} = [\mathrm{mod}(506944, 751)]_{751} = [19]_{751}$$
$$([82]_{751})^{256} = ([19]_{751})^2 = [361]_{751}$$

Konačno je:

$$([82]_{751})^{452} = ([82]_{751})^{256}([82]_{751})^{128}([82]_{751})^{64}([82]_{751})^4 = [361]_{751} \cdot [19]_{751} \cdot [712]_{751} \cdot [474]_{751} =$$
$$= [6859]_{751} \cdot [337488]_{751} = [\mathrm{mod}(6859, 751)]_{751} \cdot [\mathrm{mod}(337488, 751)]_{751} =$$
$$= [100]_{751} \cdot [289]_{751} = [28900]_{751} = [\mathrm{mod}(28900, 751)]_{751} = [362]_{751}$$

Vidimo da je Amela također dolazi do iste vrijednosti $k = 362$.