Ueli's Security Agency

This proof relies on the assumption that our "universe" $\mathcal{U} = \mathbb{Z}$.

Shared secret: m

public keys: a, b (coprime)

big prime: p

$A = R_p(m^a)$; $B = R_p(m^b)$

We know a, b, p, A and B.

a and b are coprime $\Rightarrow \gcd(a,b) = 1 \Rightarrow \exists u, v \in \mathbb{Z}\,(u \cdot a + v \cdot b = 1)$.

Evidently, u must be positive and b must be negative or vice versa. Without loss of generality, we will assume v to be negative. We now define $u, v \in \mathbb{N}$ as the positive integers satisfying $u \cdot a - v \cdot b = 1$, whereby our new v is just the absolute value of our old v.

$$u \cdot a - v \cdot b = 1$$

$$\Rightarrow u \cdot a = 1 + v \cdot b$$

From the definitions of A and B, we derive:

$$m^a \equiv_p A$$

$$m^b \equiv_p B$$

Hence, through algebraic manipulation, we get:

$$m^a \equiv_p A \Rightarrow (m^a)^u \equiv_p A^u \Rightarrow m^{u \cdot a} \equiv_p A^u \Rightarrow m^{1+vb} \equiv_p A^u \Rightarrow m \cdot m^{vb} \equiv_p A^u \quad (1)$$

$$m^b \equiv_p B \Rightarrow (m^b)^v \equiv_p B^v \Rightarrow m^{vb} \equiv_p B^v \quad (2)$$

Putting ② in ①, we derive:

$$m \cdot m^{vb} \equiv_p A^u \wedge m^{vb} \equiv_p B^v \Rightarrow m \cdot B^v \equiv_p A^u \qquad ③$$

What is left to do is to compute the multiplicative inverse $(B^v)^{-1}$ of B^v modulo p. As p is prime, B^v definitely has such an inverse. Computing $(B^v)^{-1}$ can be done using the extended euclidian algorithm, as:

$$B^v \cdot (B^v)^{-1} \equiv_p 1$$

$\Rightarrow B^v \cdot x \equiv_p 1$ (where $x = (B^v)^{-1}$)

$\Rightarrow \exists w \in \mathbb{Z} \, (w \cdot p = 1 - B^v \cdot x)$ (we now define w as the integer satisfying the formula)

$\Rightarrow w \cdot p + x \cdot B^v = 1$

$\Rightarrow \gcd(p, B^v) = 1$ (here, the extended euc. alg. can be used to determine the linear combinations of p and B^v that add up to 1. The factor that B^v is multiplied with is equal to its multiplicative inverse)

Now, we can use ③ to derive

$$m \cdot B^v \cdot (B^v)^{-1} \equiv_p A^u \cdot (B^v)^{-1}$$

$$\Rightarrow m \equiv_p A^u \cdot (B^v)^{-1}$$

In other words, $m = R_p(A^u \cdot (B^v)^{-1})$, as $m < p$.

Answer: $m = R_p(A^u \cdot (B^v)^{-1})$, where u and v are positive integers such that $ua - vb = 1$ and $(B^v)^{-1} \cdot B^v \equiv_p 1$.