Gauge Hartwell

3 March, 2021

CS427

Homework 14

1. Let g^{ab} be the key derived from the second DHKA instance.
   Eve can learn the keys used in the first and third DHKA instances by computing the following:
   First instance key: $(g^{a-1})^{b-1}$
   Third instance key: $(g^{a+1})^{b+1}$

   Eve knows g^a, g^b, g, p, g^{ab}
   Let the first instance key = g^w and the third instance key = g^z, where w = (a-1)(b-1) and z = (a+1)(b+1)

   w = (a-1)(b-1) = ab – a – b + 1
   So $g^w = g^{ab - a - b + 1} = g^{ab} * 1/g^a * 1/g^b * g$

   z = (a+1)(b+1) = ab + a + b + 1
   so $g^z = g^{ab + a + b + 1} = g^{ab} * g^a * g^b * g$