```
In[15]:= (* Diffie Hellman Key Exchange with three users: Alice, Bob, Henry *)

         n = 500; p = RandomPrime[n]  (* Random prime for all users *)
Out[15]= 127

In[16]:= g = PrimitiveRoot[p]           (* Generator for all users *)
Out[16]= 3

In[17]:= a = Random[Integer, p]          (* Alice generates private key a *)
Out[17]= 71

In[18]:= b = Random[Integer, p]          (* Bob generates private key b *)
Out[18]= 123

In[19]:= h = Random[Integer, p]          (* Henry generates private key h *)
Out[19]= 56

In[20]:= A = Mod[g^a, p]              (* Alice generates public key A *)
Out[20]= 43

In[21]:= B = Mod[g^b, p]              (* Bob generates public key B *)
Out[21]= 80

In[22]:= H = Mod[g^h, p]              (* Henry generates public key G *)
Out[22]= 68

In[23]:= kAB = Mod[B^a, p]             (* Alice generates shared key with Bob *)
Out[23]= 51

In[24]:= kBA = Mod[A^b, p]             (* Bob generates shared key with Alice *)
Out[24]= 51

In[25]:= kAH = Mod[H^a, p]              (* Alice generates shared key with Henry *)
Out[25]= 99

In[26]:= kHA = Mod[A^h, p]             (* Henry generates shared key with Alice *)
Out[26]= 99

In[27]:= kBH = Mod[H^b, p]              (* Bob generates shared key with Henry*)
Out[27]= 19

In[28]:= kHB = Mod[B^h, p]              (* Henry generates shared key with David *)
Out[28]= 19
```