Lab 6 report – Wang Zijia 1002885

**Part II:**

* **What’s the advantage and disadvantage of DHKE?**
  + Advantage:

1. The sender and receiver don’t need any prior knowledge of each other.
2. Once the keys are exchanged, the communication of data can be done through an insecure channel since the attacker is unable to get the shared key or their secret keys from the known information.
3. The sharing of the secret key is safe since the attacker is unable to compute the shared key.
   * Disadvantage:
4. The algorithm cannot be used for any asymmetric key exchange but only for symmetric key exchange.
5. Similarly, it cannot be used for signing digital signatures
6. Since it doesn’t authenticate any party in the transmission, the DHKE is susceptible to a man-in-the-middle-attack.

**Part III:**

* **Generate 16-bit shared keys using the DHKE protocol. Try to calculate the shared key based on the known p, alpha, and public keys**

print("------------ 16 bit shared key ----------------")  
"""  
test 2  
16 bit  
Generate 16-bit shared keys using the DHKE protocol and  
calculate the shared key based on the known p, alpha, and public keys.  
My private key is: 6949  
Test other private key is: 29088  
"""  
p = 44269  
alpha = 38219  
A = 22065  
B = 39294  
sharedkey = 37775  
a = baby\_giant(alpha, A, p)  
b = baby\_giant(alpha, B, p)  
guesskey1 = primes.square\_multiply(A, b, p)  
guesskey2 = primes.square\_multiply(B, a, p)  
print('Guess key 1:', guesskey1)  
print('Guess key 2:', guesskey2)  
print('Actual shared key :', sharedkey)

* **Increase the number of bits to break slowly. To avoid attack using Baby-Step Giant-Steps method, how many bits should the key be in DHKE protocol?**

I increase the length of the shared key from 16 bits to 30 bits.

The key length of 25 bits will increase the computation time significantly, and as the length of the shared key increases, the computation time is getting longer.

When the key length is 29 bits, the computation is still in progress even after several minutes.

Thus, in this case, I would say that to avoid attack using Baby-Step Giant-Steps methods, the key should be at least 30 bits in DHKE protocol since with this length of the shared key, it is not easy to get the result.