**Diffie Hellman Key Exchange**

|  |  |
| --- | --- |
| Pros | Cons |
| Communicating parties do not need to have prior knowledge of each other before the communication | Susceptible to man in the middle attack because the key exchange process does not authenticate the communicating party |
| New communication between any party can be established on the fly | Generated key is vulnerable if prime number chosen is small |
| Lesser communication overhead as compared to centralized key exchange centre | Require communicating parties to have capabilities of performing modular arithmetic fast for practical use |
| No single point of failure |  |
| Can be generalized to n communicating parties |  |

**To avoid attack using Baby-Step Giant-Steps method, how many bits should the key be in DHKE protocol?**

After monitoring the time taken to break the key from length 3 to 33, I plot a graph of the data and extrapolate the time for longer key length.

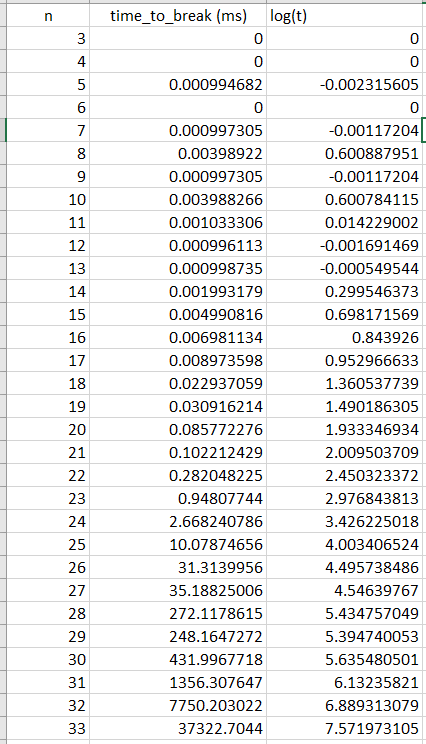
Using the equation y = 0.2483x - 2.2195, where x is the number of bits and y is the log(time), I can now estimate the key length required for DHKE protocol to be safe from my personal computing capability.

Let the maximum time that I am willing to wait for the Baby-Step Giant-Step method to be 30 days=86400 x 30 x 1000 = 2,592,000,000 ms

y= log (2,592,000,000) = 9.41

x = (9.41 + 2.2195) / 0.2483 = 46.8

**min\_x = 47**

****