Lab 6

Diffie-Hellman Key Exchange

4 Hand-In:

What's the advantage and disadvantage of DHKE?

Advantages:

- Both parties involved do not have to have any prior knowledge of each other.
- Resistant against passive attacks - sharing of the parts of the secret key can be done even across insecure channels.
- After keys are exchanged, communication of data can be done over insecure channels.

Disadvantages:

- Messages can be repudiated.
- Cannot be used for digital signatures.
- No authenticity - vulnerable to active attacks like man-in-the-middle attack.

6 Hand-In

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

Shared key length	Time taken by Baby-Step Giant Step method to crack / s			
	Trial 1	Trial 2	Trial 3	Average
16	0.019940	0.0097172	0.013002	0.014220
20	0.041569	0.093612	0.033141	0.056107
25	5.82233	0.24674	6.0227	4.0306
30	51.336	108.12	156.61	105.35
31	32.592	306.03	21.735	120.12

Table 1: Data collected on time taken to find shared key when key length is varied

Based on Moore's Law, the average time should increase by a factor of 2 with the increase of each bit. Hence, we can plot the graph below, which plots $\log_2$(avg time taken) against key length.

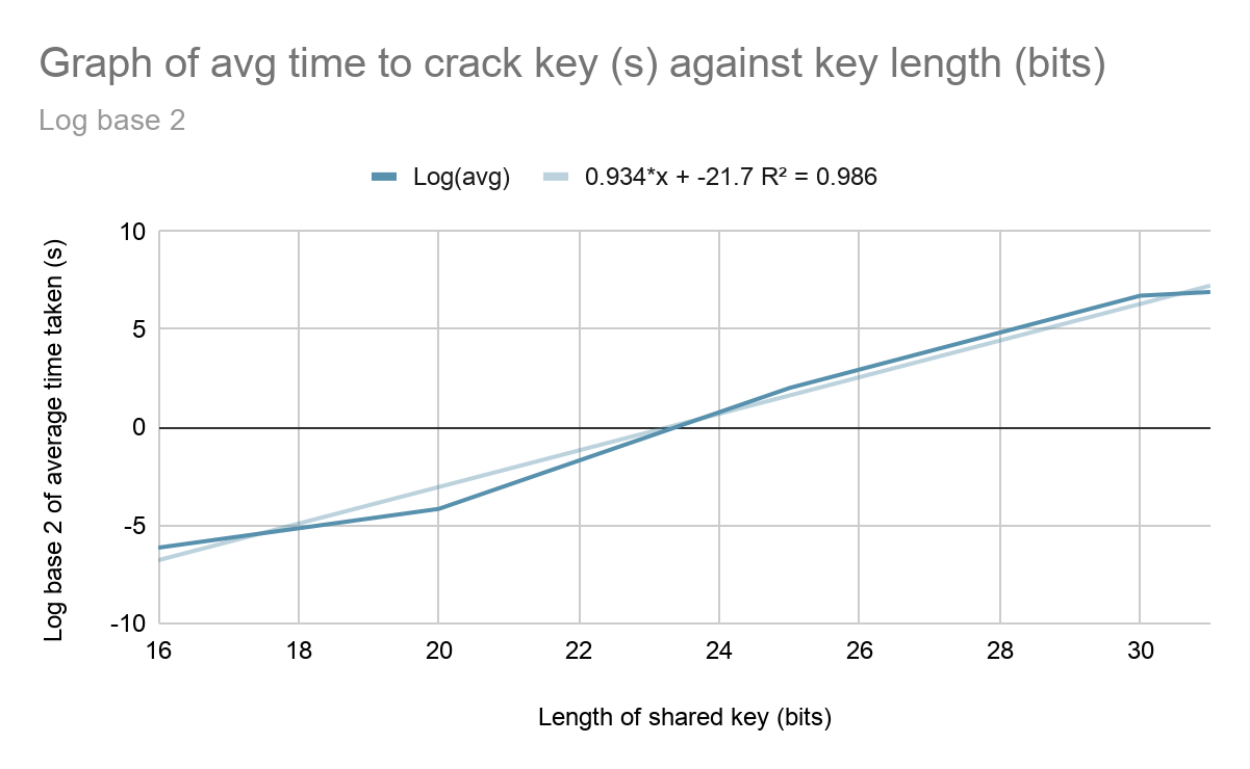

Figure 1: Logarithmic graph of average time taken to crack shared key against key length

For the key to be very secure, it should take an average of the age of the universe or more time to crack. Based on Moore's Law, the trendline plotted in the graph can be extrapolated to find the key length where average time taken would be the age of the universe, which is estimated to be 10^{22} seconds.

$$log_2(10^{22}) = 0.934x - 21.7$$

$$x = \frac{1}{0.934} * (log_2(10^{22}) + 21.7)$$

$$= 101.48$$

Hence, assuming that hackers use computers which have computing power similar to my computer, use python, and several other factors kept constant, the key in DHKE protocol should be more than 101 bits long.

However, as my computer is not the best, python is not a very efficient programming language and the nonoptimal code used for this assignment, it is advised by the Logjam that DHKE keys should be at least 2048 bits.