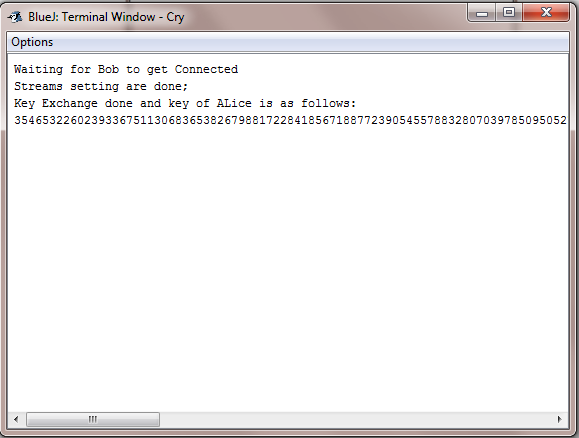
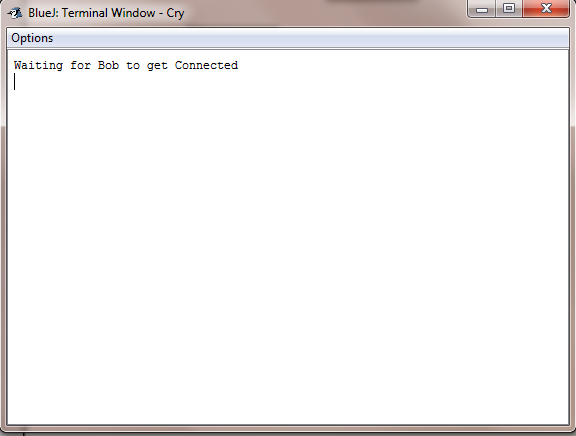
Aim:- To Understand the working of Diffie Hellman Key Exchange

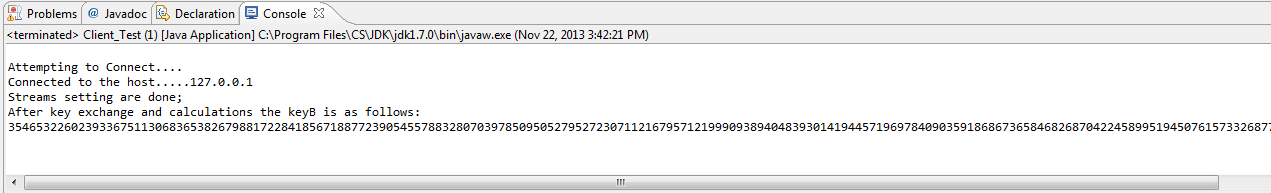
Objective:- Implement the Diffie Hellman key exchange in java.

Screen shots and Working of the program.

First the program is created in the Client-server Analogy of Java. To get the real feel of the algorithm,

Alice is portrayed as Server Program in java. Whereas Bob is a Client program in java. For the program to run first the server side needs to be executed. As shown below it will give you the message that waiting for bob to get connected. And then after they exchange the keys the figure is shown as follows.





Q2 Key Exchange values

secretA=2139028689061647233092237608363983953254005036722809375824714947394619006021875625512431718657

secretB=9473946190060218756255124317186573105075074546238828817121274630072161346956439674.

msg1.modulus=133294399882575758380143779458803658621711224322668460285458826191727627667054255404674269333491950155273493343140718228407463573528003686665212740575911870128339157499072351179666739658503429931021985160714113146720277365006623692721807916355914275519065334791400296725853788916042959771420436564784273910949

(generator)

msg1.base=276931556780344213902868906164723309223760836398395325400503672280937582471494739461900602187562551243171865731050750745462388288171212746300721613469564396741836389979086904304472476001839015983033451909174663464663867829125664459895575157178816900228792711267471958357574416714366499722090015674047

msg1.valueA=70793544088900140958310739609597330403892775517475280763470545486356341187941367717401148133003385912780868109139536623425641272607780530418541221599812959248316506069823956448455992003534445222611081921379843521254802113480264653010292262488802932111493695520281578694245432989165539882198168517280544556806

msg2.valueB=45500872595966250615027437294507175325091026053824963141872611754677787833223226373629072860986934570855208924199236591844935762441817011890983579286870026097038429902229911702503450230276498494165160003904851769401327383634514923445739158624920122299835992242466335472130505819916309952655345200890764724415

keyA=3546532260239336751130683653826798817228418567188772390545578832807039785095052795272307112167957121999093894048393014194457196978409035918686736584682687042245899519450761573326877314889401945202112207610843078407419501792590946720388225800608306627416274254403784255704758417493628586686143892054770596651

keyB=3546532260239336751130683653826798817228418567188772390545578832807039785095052795272307112167957121999093894048393014194457196978409035918686736584682687042245899519450761573326877314889401945202112207610843078407419501792590946720388225800608306627416274254403784255704758417493628586686143892054770596651

Q3

One can make the channel secure after exchanging keys by as follows:-

* Use single session key as input from key exchange.
* After getting the keys from initial communication also need to add the following:-
  + Symmetric cipher for message confidentiality.
  + Message Authentication Code to maintain message Integrity.
* Have a Key Derivative Function to generate keys that introduces randomness in keys.
* Only one key should be used once i.e. once per Direction.

Q4 a) Explanation of Attack of Eve

Note:- This is a scenario that Diffie Hellman Algorithm the measures to make the channel secure are not present and therefore there is an adversary attack.

Diffie Hellman is a secure protocol in key exchange and there is no doubt that it achieves confidentiality. The only thing it requires is Integrity. Suppose an adversary Eve is Intercepting the communication between Alice and Bob. Eve will change the message and then forward to Bob. Suppose Alice selects its secret key and does the calculation and forwards that’s to bob. Eve intercepts in between and instead forwards his calculation with her secret number to bob. Now Bob is not aware of this and simply accepts the key. And they follow the next procedure of key exchange. Now Eve has the keys for both of them and can decrypt the data traffic between as the data traffic has to flow through Eve.

Eve

Bob

Alice