Diffie Hellman key exchange

One of the important algorithm in cryptography is diffe hellman key exchange with this diffie hell man key exchange, what we are going to do is we are going to use the different approach to solve the key distribution algorithm and we are not going to distribute those keys anymore and we are going to calculate those keys in both source and destination and it is the first public key, scheme proposed and these guys are the developers in 1976 and these guys actually published the papers in 1971 but they found the secret keys , but some guys from UK said that they found out this long time ago, and they said they invented and those guys invented this public key protocol and It is practical method for public key exchange of secret key, used in almost every security application that we are using today , RSA and diffie hellman, you are going to see default in every application, in a public key distribution scheme ,it cannot be used to exchange an arbitrary message it is not a encryption algorithm ,rather its going to be encrypted secret key, no longer two participants and it is based on the exponentiation in a finite Galois field easy. Security relies on the difficulty of computing discrete algorithms hard discrete locks, if you this kind of equation y = alpha x in mod n, y is known and alpha is known and n is known but it is very hard to find x, so in diffie hellman security depends on these discrete lock problems how it is going to work is all users agree on global parameters ,large prime number q or polynomial q and alpha is a primitive root of mod q, and each user generates their key and chooses the secret key $x_a<q$, and its going to compute public key which Is y_a = alpha to the power x_a mod q and I am going call a as alice and b as bob and so alice and bob will agree on global parameters, in other words a is transferring alpha a value to bob , in other words, a is selecting x_a information and calculating y_a information in other words, x_a = alpha x_a mod q and bob will collect y_b information and it is going to be x_b =alpha y_b mod q,so what they are going to do after this alice is going to send public key information to bob and bob is going to send public key information to alice. When alice receives y_b its going to be something like this, y_b to power x_a mod q in other word it is going to raise alice, on private key , and bob receives y_a he is going to raise to the private key x_b to power y_a mod q. so what we are going to do I the value of y_b = alpha x_b to the power mod q will replace x_a to the power mod q, we are going to receive mod q and the result is going to be alpha x_bx_a mod q,so lets have a look here y_a value is equal to alpha x_a mod q, and its going to be raised to x_a mod q and if you remove the mod q then the result is going to be alpha x_ax_b mod q you see both of the m are the same and I am going to call it key is being between alice and bob and this way alice and bob calculated the secret and this secret is going to be used as a session key and that is the idea and where is the security ,alpha is known x_a,x_b,y_a,y_b is known but by using this we cannot calculate the x_a or x_b value because of the secret locks and it is very good math and very good algorithm and it does solve the problem that we are facing in cryptography, so shared session key is alpha x_ax_b mod q, when bob receives y_a it is going to replace y_a to x_b mod q ,when alice receives y_b it is goingto rise y_b to x_a mod q. and the result if k_{ab} and it used as session key for private encryption scheme, and attacker must find x_a and x_b value and it is not going to be easy as it is going to find discrete locks. So what I am saying is this, we are having global public elements q and alpha and user is going to select private key x_a and calculate y_a which is alpha x_a mod q. and user b will generate y_b and it is going to be alpha y_b to power x_b mod q and these guys are going to exchange this y_a and y_b and when alice receives y_b it is going to rise y_b to xa mod q. when bob receives y_a it is going to rise y_a to xb mod q,and both of them is going to have k_{ab} which will be alpha to the power x_ax_b mod q, so as you see user to send y_a information to user b and user

b is going to send y_b information to user a . so when they receive y_a and y_b they are going to rise to there corresponding private keys, and the result will be session key and it is pretty simple and effective algorithm and before going to this numerical example I just want to say this ,although this algorithm pretty neat and there is a draw back imagine this scenario where I have a third party in the middle, and iam going to call it trudy the existence of trudy is not known by alice and bob, when it receives alpha and q it is going to create its own key and its going to calculate y_t and that will be equal to alpha x_t mod q. and it is going to transfer it to x. alice will think that y_t is the public key of bob ,and she is going to calculate y_t to power x_a mod q. which will be alpha $x_a x_b$ mod q and trudy will calculate $y_a x_t$ that will be equal to alpha $x_a x_t$ mod q. you see trudy manage to establish a secret to alice and trudy when alice tried to encrypt the message and thinks that it is going to send to bob. By using the bobs secret key and it is going to be bobs secret key. Trudy will be able to decipher it and will be able to change the content of the message and it will change the content of the message. Because alice thinks that alice is talking to bob but alice is talking to trudy , after seeing the content of the messae may be trudy overcame alice and trudy manage to fool alice, and it is trying to fool bob for doing this it is going to select another private key lets say x_{tb} and it will calculate y_{tb} that is alpha x_{tb} mod q and y_{tb} and when bob receives this y_{tb} it is going to release x_{tb} mod q and the result is alpha $x_{tb} x_b$ mod q. and when bob sends y_b information to alice, thinking alice actually trudy will receive this information and when trudy receives y_b information it is going to change this to x_{tb} mod q and the result is alpha $x_b x_{tb}$ mod q. and it will be input key between bob and himself .so by this secret key it is going to encipher the message and send it to bob ,so bob, will decipher the message thinking that it got the message from alice. It is not actually but it is receiving the message from trudy, as you can see trudy fooled alice and bob and this is very important attack in diffie hellman algorithm and we are going to call it man in the middle attack there are two people and this guy is in the middle and this guy manage to fool both parties and this is the only drawback of the diffie hellman algorithm if you are using diffie hellman algorithm then you must be aware of man in the middle attack, this is really important and why that is possible and why trudy was success ful ,when alice and bob exchanged these messages ,alpha y_a and all they don't check the origin in other words they don't, authenticate this parameters and if you can authenticate this exchange then you can avoid the man in the middle attack. So we have version of diffie hellman and we have version of diffie hellman and it is called ephemeral diffie hell man where we exchange these parameters, alpha q $y_a y_b$ by authentication in other words we are authenticating it by exchanging the parameters, so don't forget ,this man in the middle attack is very important in the diffie hellman algorithm ,so lets see an example, lets say alice and bob agreed on the prime number 353 and lets alice chose $x_a = 97$ which is less than q, and bob choses $x_b = 233$ which is less than q and public keys are $y_a = 3^{97}$mod 353 = 40 alice and $y_b=3^{233}$mod 353 = 248 bob public key, so they are going to exchange this one when alice receives 248 ,she is going to rise that one to private key which $248^{97} = 160$, when bob receives y_a that is 40 it is going to rise it to $40^{233} = 160$, so this 160 is now going to be used as secret for symmetric encryption algorithm ,this could be DES key or AES key, this is the idea behind the diffie hellman algorithm all you have to do using the diffie hellman attack is to be careful with the man in the middle attack and also you can see that we are using actually using two distribute the symmetric encryption key one is symmetric encryption keys with the public key of the recipient and the public key and the other thing is the diffie hell man ,but when you are using diffie hellman be aware of man in the middle attack chose to exchange between the authentication or use ephimerel diffie hellman.

Public key certificates

It allows the key exchange without real time access to public key authority, it has certificate binds UserID to Public key, usually with other info such as period of validity right of use etc, it has all the contents signed by public key or certificate authority ,it can be verified only by the people who knows public key or public key authorities