Public key cryptography

It is traditionally private secret single keys that's used only one key ,that is symmetric encryption algorithms and if the key is closed. The security compromises and that is symmetric algorithm and if it is symmetric then the parties are equal the meaning of this one we will see later, and I will explain the meaning of it later. Hence does not protect sender from receiver forging a message and claiming is sent by the sender. It provides authentication, it is most significant advance in the 3000 year history of cryptography. So that is that imp basically it is really a threshold , it uses two keys , public and private keys, asymmetric since parties were not equal and in symmetric parties were equal. So why this guys are not equal , I will explain ,uses clever application of number theoretic concepts to function, factorization and discrete log as we saw in previous chapters, complements rather than replaces private key crypto, it is a very important statement that says, to us that symmetric encryption algo' are major algo's to provide confidentiality ,but in public key algo's we are not going to using this to encrypt large encrypt , called bulk encryption ,instead we are going to use, public key algo's to encrypt small data like symmetric algorithm and that's why this is not replacing the symmetric key encryption ,on the contrary it is going to solve the biggest , problem that Is key distribution by using public key algorithm ,so there is not change in the importance of symmetric algorithms and they are still the same, public key cryptography, we call it 2 key, asymmetric key and basically it gives two types of keys, public key and the private key, public which may be known by anybody and which may be used to encrypt, messages and verify the signature and to encrypt the messages I am going to use, the public key, of the destination, or recipient will be used to encrypt the messages, when we use public key there's a new concept that comes which is called digital signatures so , what is the digital signature?..we are not using hash ,what we are going to do is I am going to encrypt the message with sender private key and this doesn't provide any, confidentiality because anyone who knows corresponding public key can recover m, easily. But this does provide that if some one provides the public key, whoever owns must be the one who encrypts this message and is called senders signature, in reality we are not going to encrypt the whole message, we are going to encrypt the summary of the message by some other algorithms called the hash algorithm ,they calculate the digest of the message with private key ,lets go back to encryption part, we are going to encrypt the message with the public key of the destination ,this message can only be decrypted, decryption of the cipher text , can be only be decrypted by using private key of the destination ,so the destination will have public key and private key ,so private key will have a relation ship, this is a mathematical equation, so everytime its going to be a pair, so one public key will correspond to one private key, or one private key will have 1 public key and we don't have one private key correspond to multiple, public keys its one to one, if someone encrypts the public key I am going to go to decrypt the message , this is encryption decryption and signature generation and how am I going to verify the signature, I am going to decipher and I am going to call that s ,and it will be deciphered using public key of sender, if I can get them back then that means that this signature verified and I can say that this message comes from who ever owns the private key ,so with the public key cryptography we can have new technology called digital signature, so whoever encrypts this message cannot decipher the message, what do you think?...that Is the decryption of the private key and the result is going to be private key ,so the sequence says this, whoever encrypts this message ,cannot decipher the message and why is that, because sender doesn't have any idea about the corresponding private of the

destination, so the sender doesn't have any idea of decipher ,there is only one entity that can decipher, who has corresponding private key to this public key, that's why it is said, it is used to encrypt message and verify signature, for the verification of signature we need public key information {question from a student}, every person whoever participate in this scheme will have public and private key pair ,if lets say I have a, b, c each one of them will have private and public key pairs and we are going to make everybody known ,and we are going to make private key secret ,we are not going to disclose this, so whoever, wants to send me encrypted message will have my private key ,so when I receive, any encrypted message with public , I can use it only by private key, to this public key so every time the relation ship will be between these pairs and not between these guys, these are independent everybody will have private and public independent keys ,so we are going to use this public keys to verify signatures, and private keys to decipher the message, creation or decryption of the messages for the private ,for public , encryption and verification we say it is asymmetric because ,those who encrypt the message, or verify the signature ,cannot decrypt or create the signature because signature creation and decryption requires the private key, which is secret, if you don't have that one , you cannot keep it secret and create the messages and that's why these guys are, asymmetric, in symmetric every party was equal and why is that,who ever encrypts can decrypt ,but here whoever encrypt cannot decrypt it is very important property all the algorithm for the property that we are going to see, in public key cryptography will have this one, and it is overall property ,so what we are doing is this ,here is the structure and this guy is trying to send the encrypted message to this guys and lets say this is alice and this is bob and bob will have public key ring and it stores those stuffs, and then it goes and finds alice public key and transfers message to alice and it is going to use its own private key to decipher the message and this private and public key is related ,and it is not secret , and also you will not be able to calculate ,the other key from other one byte by using that relationship ,it is a+b kind of thing but by knowing that relationship it not going to reveal other key from other one ,this is the encryption part and what I am going to do right now is I am having confidentiality services and I can provide it as I have that service and plaintext and over here the plaintext is encrypted ,who ever has the alices message can recover the plaintext, what about authentication ?, this is encrypted by using the sender that is Bob private key, and this is secret key and I don't provide confidentiality , my objective or my aim ,is not confidentiality ,because if I encrypt it like this, then bobs private key is known by everybody, that means everyone can decipher and get the original text back, so I am not providing confidentiality ,what I am providing is authentication, because, when alice verifies this signature that means decryption of message by bob public key can see the message and can understand that this message can come only from bob because only one entity that is bob and it has the public key information and I know the identity of the bob, I can authenticate it anyways and this is digital signature part ,digest is going to reveal any information as its one way function so imagine door can only inside and cannot go outside and that kind of function , we call them one way function , that's why when we use digital signature, actually im using the entire message, which is not the case by the way, this is providing a authentication, so this is an authentication example but we are going to use digital signature in a same way, so what we did, is public key in compare conventional algorithm, in conventional the same algorithm with the same key is used for both encryption and decryption, but here one algo is used for encryption and decryption with the pair of keys and not the single keys basically, one for encryption and decryption ,which will be public and private key ,the sender and receiver should share a pair of keys in the symmetric algorithms

and here sender and receiver should share one of the matched keys other wise they cannot communicate they must know each others public key information , in conventional the security depends on the secrecy of the keys and here one of the two keys must be kept secret. Security depends on security of two keys, public key publicly known and security depends on private key secrecy, it must be impossible or atleast impractical to decipher a message if no other information is available, it is the same for public key , so In that case they are the same, knowledge of the algorithm plus sample of ciphertext must be insufficient to determine the key, in symmetric algorithm all the details are known, we know the ciphertext and we cannot get the key and cipher text and algorithm doesn't reveal any information of the key that you are using, over here knowledge of the algo plus one of the keys plus sample of the ciphertext must be insufficient to determine the other key, in other words I know the algo and I have the cipher text and I know the public key ,and I know one key and I have three parameters and it is very difficult to find private key ,although you know the relationship between public and private key, by using the relationship ,by knowing the algorithm ,by knowing the ciphertext, you are not going to get the private that Is that kind of algorithm and why public key cryptography develop these issues, one is key distribution, these algorithms will solve the key distribution of symmetric algorithm in every security application we are going to see the distribution of symmetric encryption algorithm that we are using for confidentiality all the security protocols are going to use same kind of stuffs, and the digital signature how to verify message that comes from the claimed sender, so digital signature and key distribution, are the major technology we are going to use in public key cryptography for these two reasons these guys are so important and so popular, you are going to see these guys in every security application ,except Kerberos, Kerberos is total symmetric encryption protocol but this SSL, VPN all major guys all are using public key algorithms to distribute keys and also use digital signature ,public invention due to whitefield differ and martin hell man at Stanford university in 1976, these guys came out with the idea and some guys came and said they used this algorithms before , but these guys came from the secret services and they use this concept before differ and hell man , but these guys published the paper in 1976 and everyone knows that these guys are inventors of this concept potential to this classified community because those guys will not share in the public basically, so we are going to see another algorithm which is differ hellman ,but these guys laid the fundamentals of this public key cryptography and if you see in sun Microsystems which is near Dumbarton near palo alto he is there as security consultant, so what are the characteristics of public key algorithm if I say to you guys like example if I give you an assignment and asking you guys to develop a public key algorithm if that is the case how are you going to design the algorithm and what are the characteristics in that case, so lets have a look at those characteristics, first of all it is computationally infeasible to find the decryption key, knowing only algorithm and encryption key, computationally easy to en/decrypt messages when relevant key Is known.

Requirements of Public Key Cryptography

The first requirement is this ,it is computationally easy for party B to generate a pair, that means key generation must be easy ,and it is computationally easy for a sender A, knowing the public key and the message to be encrypted ,M to generate corresponding Ciphertext $K_{ub}(M)$, it should be easy and also it should be computationally easy for the receiver B to decrypt the resulting cipher text using the private

key to recover the original message $M = D_{KRB}(C) = D_{KRB}E_{KUB}(M)$ so this is the easy part of the requirement , and if you and we are in feasible condition and it is going to be this, it is computationally infeasible for an opponent to knowing the public key KU_b to determine the private, so it is impossible to know the public to determine the private key, although you know the relation ship between them in public key cryptography and it says infeasible and it doesn't say impossible there is always a possibility ,infeasible means it will take enormous resources and time basically, and it is computationally infeasible for an opponent knowing the public key and a cipher text C to recover the original message M. it is not going to be easy and encryption and decryption function can be used in either order ,if you are using public key encryption you can only decrypt with public key if you are using private key and you can decrypt the private key with the corresponding public key. Both of them can be used this option is not used in all the application and we are using in e commerce digital signature, as I said if I give assignment design a public key algorithm so whatever you design must comply all these requirements, but im not going to give that assignment so you can be relaxed ,so this is the algorithm details ,so as you can see every algorithm will be complied with this requirements.