PGP key rings

As I said we are going to have two key rings , each PGP has the pair of key rings, public key contains public key of other public key users known to this user indexed by key ID, so everytime when that key thing is very good thing in PGP, PGP will go to PGP key tray that try will mention a the key you can see you ca put trust on that key and send the keys in the ring and that ring is called public key ring. If you don't have the public key information of the guy people can send encrypted message to you as you don't want to have any public or private key information . but if the signature is requires you will not be able to verify the signature if you don't know that guy so verification doesn't work. But they can send you confidential message and they can even send you signed message but you cant verify the message ,again one way or the other when you use web of trust, must get my public key information if you go tom y website you will see my PGP information you can send it or mail it to me and people they want to use they need you public key they can download it ,it is very easy to i am port and export it as it will be in text form ,just click that one and it will appear on your public key ring and the other thing is private key ring , first of all when you install the ring you are going to create the key and first of all you are going to install ,private and public key pair for rsa and its going to keep it secret by encryption it by hash passphrase it is going be a passphrase as PGP will force you to select a good passphrase,if you don't put any number within character if you r password is full of character s then it will not accept it ,it will say to put some symbols or numbers into this characters it s going to guide you to select a good passphrase, so you can select long passphrase whole security of this one depends on as it protects your private key, this is the whole idea. Private key ring there is a timestamp and creation of time of the key ,key id its mod 2 to power 64 that is 64 bit information of public key and the corresponding private key and it is encrypted with the key the key is hashed passphrase and they are using some algorithm used in private key and there are some algorithm stored in encrypted form whenever you need this private key you have t o enter this passphrase you will not be able to recover it and then user id , so I receive this email, session key is encrypted with public key and key id is 6, so I receive this email, session key is encrypted with public key and key id is 64 bit ,and then i am coming to this ring and i am going to see the key id is matching with the key id of I received from the email and I need the corresponding private key to get the key and so PGP will ask my password as PGP will ask my password I will enter and PGP will hash the password and PGP will decipher and use it to get the private key and now I have the private key access and I can go back and get the session key as session is encrypted with the private key and session key right now and then i am going to decipher the whole message , compress decompress the whole thing that i am doing i am going to decompress this part and message part and I have to look at the signature part now as signature part has the key id information of the sender so from that key id i am going to find the corresponding public key of the sender and these are public keys of the user I know ,the users are going tobe in this ring so I got the public key information of that guy now and now I have to decipher the information of the encrypted hash, calculate the hash and compare it and if the verification is successful then it is done, see how is ample It is, we are going to add one more thing, for the key distribution these guys have web of trust to, establish web of trust we are going to have field like this key legitimacy ,signature and signature trust, for example do you trust power of this key , I will trust you will say , and signature trust and most probably some body has signed the key and do you trust the signature whoever is signed ,you are going tosend the signature trust and by using signature trust and the owner

trust PGP will calculate the key legitimacy how legitimate the key are in this. What we are doing in this is ,as this is pretty complex and owner will have different trust and signature will have different options what we are doing is practical, if I have 100% trust on this guy and somehow I receive his public key information but I have 100% trust , what i am going to do i am the one who is the owner of the key is going to sign his message , and if I sign then i am the one who is trusting on hi am right and the only trust I already got is owner trust and key legitimacy will not be having any problem and this key legitimacy will be good to use in PGP basically, so if you don't want to deal with all these details then sign the PGP key that you have and PGP will allow you to do that ,if you don't sign then PGP will ask whether are you a valid user or you want to or something like that it is going tobe your call, but if you sign the key yourself then this fields will have not much meaning ,because you are the owner and you are going to give 100% trust to yourself so then this fields are not going tobe big deal ,are you clear?..so lets use this concept with here and that is used to secure the email, email message prepared and hash of the message is signed and sent.

PGP message generation

Hash of the message is signed and sent to the private key ring , you cannot jus go and get the private key ,if you need to access the private key PGP will ask passphrase , in other words when you are signing the message you have to enter the password, so passphrase entered and hashed ,we have the key to encrypt private key , I recovered the private key by decrypting it so that I can encrypt the hash ,but I have to tell the recipient that I use d this corresponding pubic key so I need this 64 bit of the public key which is the pair of private which the id I will put to the signature and everything is going to be appended to the signature , so I have the signature part right now , then I am going to I have to encrypt the message to do that I have to generate the session key using the random number generator algorithm and then I have to encrypt the session key with the public key of the recipient to get the public key of the recipient i am going to go to my public key ring find the recipient with use name and select the public key and get the key id ,use that public key to send the public key and append the public key I used and then appended to the encrypted message and transfer it to the destination now destination will get signed and encrypted email ,two points are missing , compression where should I put the compression ,?..compression is going to be applied before encryption that's why before encryption I have to apply to compress the whole file , radix 64 where i am going to put it?..right here in this output we have to apply radix 64 , now I manage to send the email to destination.

PGP message Reception

Lets recover the email by verifying the email and deciphering the message , I have the encrypted message and encrypted session key I am going to start first one, from receiver i am going to go to my private key ring to find the corresponding private key ,otherwise i am not going to get the corresponding private key , I got the private key and it is going to be encrypted and this time i am going to encrypt my password and hashed to generate the key and decipher the session key and you got the session key and when you get the session key you can have the message and you can have the encrypted digest signature part is verified, to send the signature part you need public key information of the sender and by using the sender key and by using this you are going to go to public key ring and get the public key,

and then decipher this one and check the list 2 octets ,if they do match then you have selected and you actually decipher the hash from the message and if those hash are same then you got the verification, you missed two points, right here there is going to be radix 64 and right here there is going to be zip , before the decryption, this is the whole structure of PGP,{question from student}. It shows the list you are just selecting form the ls it ,as a user interface you are going to see only the public keys and not the secret keys but as a option you can go and select ,one click that mean you have selected a private key that means system will ask passphrase ,and that you have selected you r private key . this is the PGP message distribution.