SMIME envelope data

Ok lets have a look at the other entry it is content transfer encoding how we are going to encrypt the data but right here we said that if the data is encrypted it's a binary data and smtp cannot send it so I have to convert into it shows which method im using to convert into text , it says base 64 ,and the content attachment is SMIME .p7m so in the attachment you are going to see this this par t the envelope data we are going to see encrypted data converted into text, so what we are doing is this, first of all system generates a random key for encryption of this data , lets say in your setting you selected triple des with 3 keys what is the key size that you require 3 times 64 bits, so you are going to generate that random number and you are going to use it to encrypt the whole mime message , which is voice video ,enrich text and all on the top of the encrypted data you are going to have an information header and that header is ,recipient ,info, over what we are doing is we are using the id of public key ,of the recipients and public key certificates , everything is going to be in the public key of certificates for that one say that I used that public , remember in PGP we were sending the id of the key right now we are sending the id of the certificate because each user might have more than one certificate, and then an identifier of algorithm , like triple des this is come from the algorithm saying that which algorithm you want to use they are going to say the name of the algorithm into that part and this is important session key that we used for encryption , but destination doesn't know that key but I have to have the means to distribute the keys and we said we have two ways one is differ hell man and rsa public key of recipient how do I know the public key of recipient , from this recipient I received the certificate from the certificate, when we receive the email there is a option that we can import the certificate and we can import that certificate to your system that means you can encrypt anything basically , by using the public key of the recipient im using the rsa public key of het recipient , so this whole thing is called recipient info , its going to be header in this part, you guys tell this header will be in encrypted form or something else, its in encrypted form as we don't see the info, because it will be encoded, if it was in encrypted form there is no way the recipient to recover the session key , this data is going to go in the encrypted form to the destination and the destination knows that this data is encrypted and its going to go to first part of data that is encoded info and to decode the info one of the data to select the info and use the public key to recover the session key and understand that idea of algorithm is triple des and that is the key that is going to be used am I right over here , is something not logical to you guys?..what is said is this , when you find the public key then you are going to go and recover the corresponding private key my logical is no that good in this ,why we should know triple des over here imagine I don't know what will happen, well the thing is I said the setting says that I used triple des and im sending it in the implementation of SMIME so other entity knows already when you select SMIME that info is going to go there somehow , but his one ,the idea of algorithm is related to this encryption is it rsa encryption ?is it eljamal encryption this session key encryption is which encryption? Im going to use the private key to decipher the algorithm but I don't know the algorithm which algorithm im going to use to decipher the algorithm as this rsa could be a public key could be differ hlleman ,could be used in rsa or could be used In eljamal, that id of algorithm shows the id of the algorithm used in session key , it doesn't show the encryption used in the email , so this could be rsa ,eljamal or differ hellman , we discovered session key this way by using the session key I already decoded the message and I will decrypt the message I m going to see the multipart or the single part and I m going to display that one one the recipient email

account {question from a student}. When you generate the key , generally in version 3 they say it is a rsa key this is difehellman key you can understand from there at the same time it doesn't mean like this this is rsa key and it cant be used in eljamal it is a public key and you can use it ,it's a way to show that encryption to show that encryption is based on public key , just a general condition, general idea of the algorithm so I recovered the multipart now the message is multipart and so what ever I do with the mime im going to do with recipient side and we provide confidentiality right now , for the email by the way when you receive this one ,remember PGP when you receiver the message to decipher it you need to enter passphrase without enter in the passphrase you cannot access but here in SMIME if you click on that one it will automatically display the message and display in mime format ,it is not going to ask anything from you ,clear in other words someone is sitting you are already logged in to your system and someone is using and someone is using your outlook when they click on those mails they are going to se the content of the message, if you look at the definition the encryption provides confidentiality and also authentication because they are going to share a secret key , but sharing is not over here as they don't share any distributed key they don't share anything so you may argue about authentication part if someone changes the content of the decrypted part im going to easily detect that one ,in other words im going to provide integrity , confidentiality and integrity definitely and authentication we can discuss about that one lets go back to the previous message ,they can decipher the message ,what about signing the message in signing the message requires access to the private key ,SMIME is not going to ask any password from me its jus t going to say that the application is trying to aces crypto api that guys is accessing the private key and create the signature what was signature generating in PGP ,when ever you have to access anybody private key then you have to enter password but in SMIME not required because if some one blocks into your outlook they can send message, sign message and impersonate message your identity and they can see all the encrypted message content this is the difference between PGP and SMIME and people are arguing this is a standard and why people haven't put passwords and stuffs because this is pretty obvious because you have PGP have passphrase and protection why its not here, no body knows and there is discussion most probably they dint was really secure email , they jus t want ted to monitor the things basically everything depends on the password you use to login or login to your email account but in PGP even though they know your password they account verify the signature or create the signature and decipher the message with PGP because that requires passphrase but in SMIME you don't have to have that kind of security because when you are in everything is over system is generating ,system is deciphering all you have to do is just click on the the mail everything is done one behalf you and this was envelop and signed data and pkcs.p7s, signed data and the name is SMIME data and the name will be SMIME.p7m and this is going to be the signed data why im not able to see anything clearly? Because signed data has encoded mail and encoded signature when they encode the signature its going to mail something like this its not encryption it is encoding and it doesn't provide confidentiality and at the top this guy have info it is called , the signed data, block message digest algorithm to create the signature , calculation of the hash is done with the signer info I was about to talk about signer info ,signer info will have , this entries, signer public key, certificate so the certificate will go with the message they are going to include actual x509 certificate that's why you are going to include the signed message on the right had corner you can see the certificate attached to you mail when you click on that one you can see the details of the certificates , and the identifier of the message and the identifier of the algorithm to digest of het message so which signature we are using

dss or rsa,because we have different option and I calculated hash and it is going to be encrypted eiher rsa or dss it s going ot be the name of the signature algorithm or encrypted message digest part, as you see sha 1 nandmd 5 im using and signer public key certificaete is goingto ebe sent and the signature algorithm is dss or rsa these are the info im going to have this is signer info at the top of it when I receive this message as a email hwat im going to do ?..actually what happens? When you click on the mail its going to decode and get the id of the message digest algorithm and from this public key certificate you can understand that this private key can be used to verify the signature, am right ?.. I am sending the public key certificate of the signer does it help anything? How you are going to verify the signature, ?..im going to use the public key and that's why im sending the certificate if I don't havethe public key information you cant verify the signature ,in the verification we used privaete key of the signer but the verification requires public key ,but the recipient doesn't know which one is corresponding public key and that's why we are sending the certificate so this way Im gpoing to tell therecipient that this Is the public of that recipeitn so for signature verification use this public key remember in PGP we were sending id of the pub lic key 64 bit but here im not sendi ng the id im send the certificate its going toverify the signature and this is signed data and im goingto have both of them signed and envelop data and im going to have both of them , im goingot sign the data nad everything is goingto eb encryprted

SMIME clear signing

In the clear signing the mail itself will not be encoded with the base 64 , look at here multipart isgn protocol lis application pkcs 7 signatuer and mic algoriotm which si message digest algorithm sha1 and boudnry is 42 and it starts from here 42 and text clear text so that actually the text or clear mail is going to go here and the second part is signed , signautuer SMIME 7 pkcs 7 all the signature is going to go there and I sent this to destination and destination doesn't know SMIME so weare goingto see the clesar mesagfe but if the destination has the SMIME abiltiythen the clear sign meage is goingto be seen and the signature will be verified and this is clear signed ,p7s for this one, while you receive this one then it is clear signed attachemtn we have all of the studff envelope data ,signed data and clean signed data and it could be envelope and signed data these are going to be the option for you when you are doing the configuration of the email client so this way we got the SMIME right now the email can be secure in tow ways either using PGP or SMIME and you may use PEM , privacy enhanced mail it is not around anymore because of privacy enhanced concept ,PEM is another option for secure the email , but todays standard is SMIME and defacto standard is PGP so this two major things are making this smtp protocol secure.