SMIME functions

Last time we spoke about mime types content types we saw the whole structure of mime mail and we said that we are going to make that mime more secure because when we talked we dint see any security at al in the mime mail ,and the secure version of the mail is called SMIME and it is the standard version today , and it is secure mime and its function as envelop data means we are goon got encrypt the content of email with keys in other words we a re going to do the symmetric encryption lets say 3 des the key is triple des is going to be from RSA so it says associate keys ,and when we do that that means we do have envelop data ,it means encrypted data, signed , it is encoded message and signed digest that means you have a mail and you are going to hash of the mail and you are going to sign using your private key and the result is going to be encoded ,most probably the encoding scheme will be base 64 and the mail contents encoded, in other words encoded message and signed message are encoded in other words it is encoded if the recipient doesn't have SMIME capabilities it cannot see the received email to avoid that case they have this option , this time the mail is going to be in the clear text message but the signature is going to be encoded and everything is going to be in signed data but only signature is encoded ,whether they support SMIME or not they play the mail to the recipient ,and finally that is signed and envelop data that is next thing signed and message , we are going to calculate the signature and encrypt the signature and the mail, these are actually options ,when you go to option and select security tabs you will see the option clear signed data and signed and envelop data or encrypt the content of the data if you select those options the outlook is going to do these things it depends on your selection you are going to encrypt the mail or you just want to sign the mail or you want to sign and encrypt the mail, second option your message is not encrypted but not encoded this is base 64 and this Is actually encryption to recover the your original message they have to support SMIME if they don't support SMIME then you will have problems so but these are conceptual things and how you are going to embed in mime?.

SMIME cryptographic algorithms

Each one of them will be content type for us, and when we use the signature the hash function we are going to use is sha1 or md5 ,digital signature , is RSA session key encryption RSA or elgamal ,mostly RSA message encryption triple des, AES now ,rc2 40 bits it gives the key size, these were for the export reasons available ,if you export stuffs outside US you want them to use security ,it is nothing to do with todays world as it supports AES and triple des you don't want to support rc2 , no body is going to select that one , and you have the procedure to choose the algorithms, like if you go to outlook and settings options , you will see the encryption and signature part ,first of all you are going to see which signature you are going to use for encryption for encryption you have to import the certificates of the other user and you have to select the algorithm that you have to use may be sha1 or md5 and also for encryption algorithm triple des or AES any option that you have to select but this is a setting ,when you are done with setting all the mails have to use that settings , if you want to change it again before sending the mail ,g o to tool , go to security tab and change the settings and it works in outlook like this and in other email clients it is different , but the main idea will be same , you will be able to select the algorithm for signature and an algorithm for encryption , to create the signature ,there are requirements for SMIME ,for that we must support sha1,s mime must support sha1 and receiver should support backward

compatibility ,must things and should things so two things and must things are the basically we will use for our encryption and digital signature, sha must be used in case some one has used md5 then receiver should support md5 , for encryption encrypt message to form DS sending and receiving must support DSS ,so they are using DSS signature , that is important and it is standard and sending agent should support RSA encryption because we may need RSA signature and receiving agent should support RSA encryption with key size 512 to 1024 bits and this key size is changed not it is 2048 bits now so must have entity is des and should have entity is RSA, and what about encryption of session key must support differ hellman they are going to calculate the entities and should support RSA so we have two options here in other words for key distribution either we are using diffehellman for calculating the session key or we are encrypting or decrypting the session key with RSA when we look at the details we are going to se the header in the header we are going to see that we are encrypting the algorithm with the session key and the entity of the header in the envelop data, this is the email encryption what about in the actual encryption we should support the triple des but AES is the standard now , so SMIME should support AES , if you look at the same table in your book you will seethe different , it will say AES is the must have entity as it is the new thing so , we are going to use AES in the outlook 3des is going to come by default as you see we are going have must have and should have things in SMIME and how am i going to embed envelope and sign data into mime?.how it is going to be the part of he mime structure there were boundaries and in those boundaries these are text message s this is the avg text message and this is video and this audio and we are going to have most probably those kind of stuff saying that it contains encrypted audio or encrypted video or signed message it is going to be different part and all the part in the multipart mime is the envelop data it is going to be encrypted in other words you can understand that this is going to be a type of content type first content type is multipart subtype is going to be signed this mail will have multipart but this will message in two types one is message and the other is signature but this is clear text signature that means the recipient if it doesn't support SMIME can see the messages in other words email is not encoded with base 64 when you see the message the content type the whole message is signed the whole mail is signed and the other type is application and subtype PKCS7, mime, this is very important and this PKCS is standard for public key cryptography imagine you want to store your public key in smart card how are you going to store it what is the communication what is the smart card details when you store there all those things are details that are advices using PKCS standard PKCS 10 is the certification registration request and PKCS 11 is how to store public key s in smart cards we have lot of PKCS standards and major that creates this standard is RSA ,it is very big company if you go to tutorials you will see lot of PKCS standard PKCS 7 is for signed data envelop data and encrypt data that is for those standard and that is going to go to subtype going to PKCS mime and that is the subtype and that means that it is signed SMIME entity or PKCS envelope data is encrypted SMIME entity and PKCS7 degenerate signed data an entity containing only public key certificates you are only sending your certificates and PKCS 7 signature the content type of the signature and the subpart of a multipart /signed message , it is multipart signed message as we said it is the second part of the signature and it is going to send the signing part that is signature PKCS10 mime is certification registration request message ,when you apply or signature in SMIME for example in the past you have to fill up the form OS is handling it now and that form is in the format of PKCS 10 you are not doing anything extra you are requesting a certificate the important thing is that public private key pair there is very less understanding of PKCS 10 and it is not send the private key to the CA, whoever they are

,verisign when you request the certificate ,private does not know your key , only the public key will know ,what will happen is your OS using the crypto api of the os is going to generate public and private key pair and that encrypted system is going to handle it nothing is there with the use you dont know windows 2000 or xp is storing in bla place then you have to look that api of windows xp unix or linux this is user transparent ,type are putting PKCS 10 and they are putting the public key info there and sending it to the verisign when they get this one they are going to send this DS certificate to you but that certificate is going to be generated by you public key and not by private key you are going to verisgin and saying I want a public key verisgn generates the public and private key and verisign creates the public key and sends it to me it doesn't work that way in disclose in the private key there is no private key and those private key are private and CA ,and they are not the one who is generating public and private key ,you are the one whos is doing it and only the public key to ca to get the certificate, In other words mime message will have those parts whether this whole mime message is swapped or im just sending the certificate or signature what im saying is content type this is SMIME something related to security SMIME type and encrypted email and the name is SMIME. P7m ,something like this lets say that I got a certificate from verisign and im sending a signed message to a yahoo email account to your web based accnt that is yahoo it cannot display or verify the signature if that is the case the display of the attachment will be SMIME.p7m , when you see tat this is not a graphical display this is a attachment display because when you receive the signature or if you have the older signature files then you are going to see the signature as a yellow ribbon when you click on that one and the n SMIME is going generated automatically that means digital signature will be developed automatically and then the certificate will be in the right side of the message or in the inbox you will see blue or yellow luck symbol ,if it is blue then it is encrypted data but if its yellow then it has signed or encrypted data , but when you get it from the yahoo accnt you are going o see the attachment and the name of het attachment if SMIME.p7m so that you can immediately understand this is encrypted type so SMIME p7m shows us that this is the name of the file for the encrypted data.