Message Authentication code

As shown MAC provides confidentiality ,can also use encryption as secrecy , and it Is costly and encryption is a big deal because encryption is costly ,it is going to slow down the resources, if its slow downs the resources this inside as you saw is not simple in DES and AES ,it requires a lot of calculation , and we are not going into that one, we are going to see hash functions

Hash Function hash functions are like crypto algorithms like MD5 and other crypto algorithms ,condense the message ,again we are going to have fixed size, usually assume that hash functions is public and not key , so hash doesn't not require any secret key to calculate the hash function it does provide integrity and not sure authentication, hash is used to see changes in the message, about the source of the message and the identity of the sender. It I a little bit limited we are going to use this hash function for digital signature, so digital signature are based on hash function, nothing to do with encryption these are one ways trap door you cannot recover the message back, in other words, you can enter the room , but you cannot live out of the room. So that is the stuff, so lets have a look ,there is a message there is a hash function hash of the message is going to be calculated with the hash function and append it to the message and hash and message will be transmitted to the destination and destination is going to decipher the message by using the same hash function that we used in the sender side, its going to use the same hash function to calculate the hash of the function from the plaintext and its going to compare calculated hash and received hash and if it's the same then hash function is ok, message authentication will come from encryption and not from hash, I am doing some calculation for the source A ,in this function this output depends on this function and I am using the same hash function and the I musing the same hash function from only this message, I deciphered and I recovered the message and in this decryption I recovered the plaintext and I will use the same plaintext and to see if this plaintext is same as the other if it is not the same then these two hash functions is not going to match but if these are going to be dame then these are going to be same that means they are going to be some change in the message, in the previous slide we are going to look at the hash function to look at the changes in other words I am going to provide integrity I don't have confidentiality, purpose of providing hash is to provide confidentiality If I need it one, it depends on your security requirements, over here im encrypting it and over here it is confidentiality and integrity, you don't use a secret key, first of all you don't use the MAC key and MAC key requires the whole encryption of the message and encryption is so costly ,you are going to calculate it, although algorithms are not so simple , I am going to show you some examples its going to be much better than MAC. Second scenario in the hash function is the hash of the function is going to be encrypted this time and encrypted hash is going to be appended to the message and it is called digital signature and if it is symmetric digital algorithm that you are using , that means it is symmetric digital signature we don't use symmetric digital signature to much , and I am going to transmit that to the destination and it will calculate the message hash In the plaintext and decipher the match and if there is a match then there is good integrity and also authenticate the source because of the secret that are shared and these are examples of the digital signature that we are going to use, so hash is going to be calculated right here and hash of the message will be encrypted with the private key of the sender ,remember we have private key and public key in public key cryptography , private key is the secret and public key is known by everyone ,so the sender will send the private key ,because when

you say the key then the digital concept is going to be totally different and private key will be used in digital signature, so private key will be appended to the message and on the other side hash is going to be recalculated in the received side and will be recalculated using the sender public key ,that process is called verification of signature then this guy recover the hash of the message ,recalculated hash or recovered is all the same, so integrity and authentication is there ,because only this entity who has secret key information can create that signature, you don't have to have confidentiality all the time that's why I am telling you what is security requirement, if its not confidentiality then you are not going to spend time making messages confidential ,sender private and over here sender public key, that is the idea behind public key cryptography, whoever encrypts the message cannot decipher the message ,whoever encrypts with the public key of the sender of the receiver cannot decipher the message , the concept is totally different that symmetric algorithm which say who ever encrypts can decrypt the message , another usage is we are calculating the hash and encrypting the hash and appended with the private key and the whole message is the encrypted with the session key right now we have the confidentiality authentication and integrity ,so three services, over here what iam doing is I m appending secret to the message and that is s, and then I am calculating the hash , now hash of the message is function of whole message and hash looks secret and looks like MAC and that's why it is important and I am making hash as MAC algorithm and im using it as hash algorithm and we have hMAC, is the major that we are going to see in every protocol and the idea is going to be the same and structure of different and hash output will be different and that output will be shared with destination so that one is appended to the message and transmitted to the destination and its going to calculate hash and the secret key shared and calculation of hash and this output should be same as the received one if there is not cahgne in the content ,but this way I do provide, integrity and authentication ,when we look at ssl protocol fro example integrity and authentication will be done on hMAC and ipsec hMAC .