Hash function and digital signature

Last time we discussed what's the basic use of hash function what we did with that hash function were this in the first function we calculated the hash of the message and appended to the message and encrypted along with the message and which service they are providing , one is called confidentiality and other one is authentication because of same key for whole encryption in other works authentication comes with the whole encryption of the hash , and in second scenario I am encrypting only hash of the message and message is in clear form and I m appending encrypted message to the hash and which service I m using here ,only authentication because of the SHAred secret key and the other scenario ,has of the message is encrypted with , secret public key or private key of the sender, and the meaning of this one is ,what is the technology ,encryption of the hash with the private key that gives digital signature I m having digital signature that's why can provide authentication and the fourth scenario what I did I encrypted hash of the message and appended the signature and all of them are encrypted this way I m still having confidentiality and authentication ,in last scenario what we did is we put the secret and we did secret as the part of the message ,s o the hash calculation was the function of message and secret , imagine that first line of your message is secret that is s ,that is appended to the message and this way I did something important ,what is that?..why I calculated the secret hash , again this was the technology and this is going to b the standard and we made hash algorithm MAC algorithm and remember the difference between hash and MAC, MAC is the function of secret key and MAC didn't use any secret key but right here right now, itseems that hash is using the secret that means hash is becoming a MAC, so im using hash algorithm as MAC algorithm that's why it is providing that authentication that is secret and the last part is im again going to calculate the MAC and everything that is going to be appended will be a secret message ,when we encrypt the message what we are using is confidentiality when we calculate the hash of the message , I m having not integrity, authentication, {question from a student}.

Hash function properties

What are the properties of those hash function ?.. we don't have 100 of them designing of these hash function is not easy as these are one way functions or we call it trap door function it is not easy to develop these kind of function ,so if I say go and develop hash function for those algorithms what we are going to do ,requirements are , hash function will produce fingerprint of the file or message and it is going to condense the variable length message M and to a fixed size finger print and its should be applied to any size message and there shouldn't be any limit, you should not say that I cannot calculate the hash of one megabyte data , there is not that kind of limitation .

Requirements of hash function

This is a very important hash function ,in other words if I ask you guys to design a hash function then you should be designed according to its requirements first of all there should be no limitation , but there are some bits ,because in some algorithms it will be 2 to power 512 bits ,it is huge so you may it is unlimited but if you more than that size you are not able to solve the problem ,that is called hash of message it is easy to compute h, that is h(m). the trouble is this ,if you know h, or if h is given ,and you are trying to find x or message so that's why this three and 4 shows it's a one way function ,so you cannot recover

the message back from message h, that is important , this is one way property of hash algorithm , every hash algorithm should be one way function. And this two things are very important and given the message , I am going to find the other message and these two message will provide the , and this 2 will produce the same hash, so I have x and I have y, this 2 messages hashes will be same and this is called weak collision resistance, what about the other one which is strong collision resistance , it is infeasible to find any x,y which will be of same hash. So that's called strong collision ,what is the difference between two?..one is x given you have to find y, and the other is they have given both the functions. It will produce the same result and that is the difference , so given is the x and we have to find y, but in 6 nothing is given two functions are given which will produce the same hash, so one is strong and the other is weak collision ,most of the hash function that we are going to use ,we will check both strong and weak collision, and it is broken based on same collision and if you can find the same message that produce the same message, hash you cannot use the hash algorithm for the security and we are going to use those kind of stuffs, so don't forget ,weak collision and strong collision, and one way problem and hash will produce fixed length output.

Simple hash function

It is simple hash function as name says, and it doesn't require anything, it is just xoring the function ,but also a cryptographic function like SHA algorithm so there are going to be crypto algorithm and we are going to see in the next chapter ,opponent must generate 2 to power m by 2, desired message to hit the same hash output and we can use block cipher as hash function ,how am i going to do that?..block cipher are reversible, that means if you cant decipher it you cannot use the block cipher, but hash function requires are one way function and how are you going to have hash function to have a reversible function, lets have a look at it, $H_0 = 0$, and zero pad of final block, and we are going to get this h_{i-1} will be encrypted with this, and message will be the key for that block $H_i = e_{mi}[h_{i-1}]$, which is the current block of the message , so 0 is going to be encrypted with message first block what ever the algorithm that you are using ,like you say if you use 128 bit size then you are going to use that message, that's going to be my key and that key is going to be my next operation , its going to be the input to the message and I am going to encrypt the next block and I am going to get h_2 and I am going to use the final hash and I am not going to use any secret key, iam going to use message basically to calculate the hashes ,secrecy is not a big deal here as we are dealing with authentication and the algorithm and 64 bit is not a good thing and 64 bit is very small in todays bits, todays standard is 160 bits ,but its changing this is already accepted as standard and the size of the hash will be 512 bits ,if you are using the 512 bits imagine the birthday attack , you may need 2 to power 256 ,huge number possibility are iterations you should take any collisions basically

SHA

SHA originally designed by NSA and NIST ,this is NSA design and 1000's of people of working , they apply the brightest kind of brains ,and the way they approach ,if you go to NSA and I f they employ then you are something else, so they employ people who are above average. They created this and one Chinese guy managed to break it.1000 of people designing the stuff and controlling the stuff and one guy stopping all of them, cryptography is such kind of thing, you cant be really sure of what you have

created. ,but we know that SHA 1 was a good algorithm ,US standard for use with DSA and full form of DSA is digital signature algorithm and also RFC3174 , you can see the details of that algorithm and the algorithm that they are using is SHA1 , the standard is secure hash standard and the name of the algorithm is standard and name of the standard is DSS. And SHA1 , design of SHA 1 Is based on design of MD4, which is message digest ,md5 is still use, SSL protocol is used to calculate md2 and md5 ,2 hashes ,SHA1 is for backward compatibility and md5 is today's standard that means md5 is in use ,but the md5 is rapid in speed and SHA1 will be replaced .it produces 160 bit hash values and the birthday attack 80 different values and its quiet large. Recent 2005 is also security of SHA 1 raised concern and that's why SHA1 standard is changing right now its becoming SHA512 for all the security application ,I think its going to be valid in 2010 or 2012, just have to check it. Lets put it this way, SHA512 is going to replace SHA1 .

SHA1 overview

I am not go into details so that you will understand what kind of algorithm they are what we are doing is we are spiting into 512 bit block except last block and last block is going to be 448 bit , remaining 64 bit is going to be used to define the message size which 2 to power 64 ,in design we said there shouldn't be any criteria but 2 to power 64 is quite large so it falls into that category imagine 64 bit, it is more than that, append 64 bit length message to this remaining 64 bit, we are going to have 5 buffers and total 160 bit and I a m going to call it abcde these are register like microprocessor total 160 bit ,this is the initial values ,first of all you need to add those values ,hexadecimal values given by the standards, so these numbers are standards and we are going to process m

message in 16 word 512 bit chunks and we are going to expand 16 to 80 by mixing and shifting and we are going to use 4 rounds of 20 bit operation on message block and buffer and we are going to add output to input form a new buffer value and it doesn't make much sense lets have a look at the figure and I have the message and I shifted into 512 bit blocks so my message size is 512 bits last block is maximum 448 bit message and remaining 64 bit is length of the message and I am going to take the first 512 bit and I am going to take the iv value of the register value and iam going to do something and I am going to create 160 bit value output for the first block and this 160 will be the new value to the buffer , so these new iv is going tot be replaced and this time for the second round and this is going to go like this and finally I m going to have 160 bit output and I m not going to replace that output with the new output and iam going to take it has fingerprint and hash for the message and that is the whole architecture of the algorithm .