AES round

So lets have a look at the AES algorithm and you are going to have clear understanding when we look at the algorithm . we said that 128 bit is my state ,first column is going to be represented here in the shaded form bytes. Second column with this 4 bytes and 3rd column represented with this shaded ones. 4th with these guys. Each cell is going to go to substitution table and it is going to be substituted. Lets say this is the state ,$S_{0,0}$ will be going to s box and will be substituted with some thing else and $S_{1,0}$ will be substituted with something else, it is just a round information and not the whole algorithm so that is why I have just a state right here that is I XORed with the key everything and I got the data block back. Then I am going to go to S box and I am going to replace with all the bytes. I don't have these amount of S boxes ,I have only one big S box. So these S box are the same S box . if I another state there should be another thing which is called shift rows. So lets have a look at shift rows rules and you guys tell me what is happening with the 4th column, and 1st shell. What is 3rd column first shell, there is nothing and what about second column first shell, again nothing. And 1st column 1st shell there is nothing, so you can immediately say that in first row there is no change. So in shift row 1st row will not be shifted ,so lets have a look at the 2nd row. Second cell in the third column becomes second cell in the 4th column so what I am saying is this. For the first cell there is no change. So In this first cell no change ,but in the second cell we said that this guy becomes this guy. And lets look at the second column and third cell and that will become and that will become second column second cell, so lets look at second column second cell that becomes first column 2nd cell. If the last one becomes like that then we can generate the rule ,so lets have a look at the last one. 1st column second cell becomes 2nd cell in the 4th column. So shifting is this side, so it is 1 byte left shift circle. Lets have a look at the 3rd cell in the 4th column third shell in the 4th column becomes 2nd cell, so lets have a look at the 3rd cell in the 3rd column and it becomes third cell in the first column, if you check this then this is two byte shift to the left .so lets have a look at 1st column 4th cell and that will become 1 st column 4th cell you might say 3 byte shift to the left , which is circular shift. And we are going to the new state right now and that state is given by matrix multiplication, and we are going to have matrix multiplication ,at the given standards and we are going to multiply that matrix with that standards and that is, this is multiplication and all the multiplication and it is going to be done with $gf(2^n)$ polynomial m(x) which will allow us to x basically. 1st row is not having any shift, second row is 2 byte shift to the left and the 3rd one is three byte shift to the left, this is just a representation and it's a rule given by, design, after all the shift is done we got the new shifts in other words new 128 bits, permuted. And I am going to do the multiplication and that is the crucial part and that is the time consuming part of AES algorithm and field arithmetic multiplication , I am going to explain that later. Now iam going to add this to the input and it becomes another state and I am going to add this state to the next round and in the next round I am going to do the same things. You see it's a pretty simple algorithm and not that complicated.

International Data Encryption Algorithm (IDEA)

The other algorithm is idea, we are not going into details of the algorithm , I am going to give you general idea about idea, it is small symmetric block ciphers designed by Lai and Massay in 1991 and what are the characteristics of algorithm is it uses 128 bit key size and it doesn't have NAS ,means s box for subustitution and it has 3 different math operations that is exclusive OR or 16 bit binary addition or

16 bit binary multiplication ,so 3 primitive math operation so it is used in PGP, it does use this idea algorithm ,so when you use PGP or when use idea ,one of the encryption algorithm is IDEA.

Blowfish

Another algorithm that we are going to use is the Blowfish, and blowfish means what??..its a fish and it blows itself under danger so that other predator cannot, eat it and the other important information is the best sushi and it is the dangerous sushi and if the chef is not good enough you may die as it is poisonous fish actually ,so they prepare in such a way that it doesn't affect you , but if the chef is not good enough, be careful, and one of the famous restaurants is also called blowfish in Sunnyvale or in SFO, why I am saying this one, if I explain the algorithm then its going to blow itself, for the protection and just to get the sbox construction we are going to have 500 and something encryption just to construct s box, so it will be dynamic and function of the key ,when you change the key it will increase the size of the algorithm, so basically it improves security ,if you look at the DES, everything was fixed, block size ,stream size and number of algorithm everything was fixed, if you look at the keys then it is the key size and the number of algorithm and everything was fixed and if you look at the block size now, in blow fish it is going to be variable key size and not on the 3 options so it is going to start from 32 bit to 448 bit and you can select any of them, even 127 bit could be your key and 63 bit could be your key, so its going to be variable and so they are going to come up with ideal dynamic s boxes. So when you use different keys the s box that you are going to use inside the algorithm is going to be different and that is the idea behind the blowfish and that is variable security by variable key sizes, so new concepts variable key size and dynamic s boxes and that's why while we are constructing the s boxes, we are going tohave blowfish and that is the idea of blowfish and it is implemented by bruce schneier and these guys are in mountain view or Sunnyvale and they have a very good book called , applied cryptography, and you can see all the application of inside the crypto algorithm, detail description of it, and that company became very famous as these guys are becoming very famous and they are giving a security consultancy for big companies basically, so they are in the bay area, so they developed that blow fish and they have electronic newsletter called cryptogram ,which is very good and if you get registered to it ,you will get all the new crypto and security information basically. And whats going on kind of stuff, and those cryptograms are really a good source of information and developed in 1994 and we also saw two fish which was also developed by this guys, this is a impressive algorithm only thing is 500 encryptions to construct the sboxes and has been implemented in various products basically.

RC5

Is owned by RSA, they have head quarters in boston and one of the branches in silicon valley, and this is the biggest company as far as the security is concerned ,they have the power and if they say that this thing shouldn't be used in world then it will not be used and designed by Ronald rivest and he is the one of the person working in RSA. And used in various RSA products and it can vary in key size like in blowfish, varying data size , so this time block size is not fixed and it could be something,and varying number of round you see right now we are going to make block size dynamic , number of rounds dynamic and key size dynamic,variable I can say its not going to be fixed it is very clean and it is implemented for cpu implementations because it has only shifts and exclusive or operation but still it

has secure, and these guys are highly secured still we are going to see rc4 and with rc4 you are going to see that these guys are something else. These are family of ciphers and we don't have something like RC5 we have more than one rc5 ciphers w, r, b w shows the word size which means data size, data could be 2w and number of rounds will be 0 to 255 and number of bytes of key will 0 to 255 times 8 will give you 2000 something bits for the block size, normal version that we are going to use is 32/12/16that means block size is going to be 64 bits number of rounds is going to be 12 rounds and number of bytes will be 128 bits and if you want you can go and select someother options as well. So it's a really a secured algorithm. It is suitable fast, adaptable to processor with different word length ,it depends on the variable data size ,if you are using 64 bits microprocessor, you may say that my algorithm is 64 bits and you may that my algorithm is suitable for 64 bits cpu use, variable key length ,simple ,very low memory requirements very high security and data dependent shifting or rotations ,all these makes this algorithm more stronger.

Cipher Blocks modes of operation

We know the AES algorithm we know the DES algorithm I am not going to use to encrypt the data, I am going to use those algorithm in some specific standard modes ,defined by the standard organizations something like this ANSI X3. 106 -1983but it is valied for AES,we are going to use the DES algorithm ,or AES algorithm in some modes, when we look at the encryption algorithm we are not going to see just des or AES together but we are going to see DES in blabla mode and AES in bla bla mode , so everytime this algorithms will be used in mode names and we have 5 different modes defined in ANSI as a standard we are going to use it as a standard ,5 for DES and 5 for AES ,so lets have a look at these modes ,because these modes are going to be very important for us in the security protocols , the definition of the modes will come from ,it doesn't mean anything, you are going to ask questions about DES or AES, you are also going to ask questions on these modes also, so lets have a look at these modes.

Modes of operation

The first mode of operation is called ECB (Electronic Codebook). In ECB, each block of 64 bit is encoded independently using the same key. Each block will be encrypted independently using the same key. So guys these are directly used in the algorithm ,so it is called Electronic Codebook(ECB). So what I am saying is, first of all , message will be broken into independent blocks, as this is block cipher and we are going to do it anyways. It will be 64 bits. And then each block is a value which is substituted like codebook, because block cipher is big cipher remember ,each block is encoded independently of the other blocks. That means current plaintext will be encrypted with the DES by using Key K1 and we are going to get current cipher text block. It's the same thing again you are going to get the plaintext block , then encrypt it with DES with key K1 and get the Cipher text block. We are going to use this for security transmission of the single values, why we will use only single values, lets have a look at the encryption so that we will get to understand why we will use single values ,so here we have plaintext , the first block will be encrypted with the plaintext and the result will be ciphertext.