Cryptography

Cryptography can be characterized by types of encryption operation used. The first is the substitution, we are going to see the details, the next is the transposition, we are going to see the details and the other one is the product. Most of them, are going to be product ciphers, product ciphers are nothing but they use both substitution and transposition cipher.The next kind of characters that is used is the number of keys that is used. The keys may be single key or private and two key or the public. These single keys are symmetric encryption algorithm and the public keys are public key cryptography. The next one is the way in which the plaintext is processed. It will not take the single algorithm instead it will take the whole algorithm, You are not going to get the two megabyte file and encrypt the entire two megabyte file in the algorithm . every algorithm might be will be either a block cipher or get the block of the message and encrypt it and get the another block of the message and encrypt it again, create another block of cipher text again ,like that. The stream cipher, the encryption will be bit by bit, create one bit then encrypt and then again, encrypt another bit like that. Or byte by byte, do 8 bytes at one time and another 8 byte in the next time.It cant hold large 2megabyte kind of data all at once. We are not encrypting the data in the one go ,we are encrypting the data one by one. So its block and stream ciphers. {question from a student}.. Stream is going to be faster than the block ciphers. But you are not going to have too many stream ciphers. The major cipher is called, (ver….) cipher. It going to be the XOR operation ,you are going to XOR the keys and you are going to form the operation. RC4 generate keys for (ver…) cipher and you may xor stream cipher to block cipher. But the major things about the block cipher is its going to generate exclusive OR cipher. But you are going to XOR the operation of the plain cipher to the block cipher. So most of the ciphers that we are going to use will be the block cipher. {Question from a student}..The source codes are not generally encrypted, because if you encrypt the source code then you are loose the program, there are other ways to make the software secure. And one of the mechanism is called (c……..).. I don't know whether you are aware of that. But we are going to create executable for , and we don't have any kind of such stuffs right now. But when we are talking about algorithms, then there are some algorithms that you may actually create and execute it, but executable itself and encrypted, but you are not going to do that for the whole, but you are going to do that for some functions of that program, for software security, basically. {question from a student}. There are software developed available from the executables and they are trying to develop the source code and they are doing that. And that is not that complicated stuff, if you have the proper tool basically. It depends on what type of cpu you are using basically. That's called software piracy and the major thing for software piracy is to generate the source code from the executables. And then they are doing that and generally they are easy by the way.In java they are doing it and in C they generally do it. For those kind of techniques they develop softwares for the software security. You are doing code obfuscation they cannot understand, exactly what you are doing. {question from a student}. Its obfuscation, It's a very good technology, if you go to website, you will get code obfuscation tool kit for java and you can now only play around. And also you can implement those stuffs in your company If you are working on those kind of stuffs.Tell them you are working on those kind of stuffs , so that you can use those stuffs, to make it more secure, it is developed for java.

Type of crypto analytic attacks.

It is going to be another important thing for us. That's going to be, cipher text only attacks, known plaintext, chosen plaintext, chosen cipher text, chosen text attack. If you look at the cipher text only attacks, you know the algorithm and only the ciphertext, so by knowing only the ciphertext and the algorithm, you are going to find out the statistical relation to find the plaintext. Only thing you have is the names of the algorithm and the names of the ciphertext. And the known plaintext is the You know the plaintext or you suspect the plaintext or you suspect the ciphertext, or in other words you have both plaintext and the cipher text. In other words, you are going to find the algorithm . that's called known plain text attack. So chosen plaintext ,you are going to select the plaintext and you are going to find the algorithm again. And in the chosen ciphertext you are going to select the ciphertext and obtain the cipher text, this time to attack the cipher and so chosen text select either plaintext or the ciphertext to encrypt or decrypt the attack on cipher. So these are, the five types of the cryptoanalytic attacks. As a intruder, they are going to do these kinds of attacks.

Brute force search

One of the major attacks that I am going to talk about is the brute force search. This is the straightforward search, they are going to try all possibilities, of the key, lets say, your key is 8 bits and how many combination I have for 8, total 8 right, I will try them all and one of them will the real key, so that is brute force attack. Most basic attack, proportional to the key size unfortunately, and assume or either know or recognize plaintext basically. When you have the key then you have to check whether the text you have is whether a plaintext or not . So if the key size is 32 bits, then how many options do you have, 2 to the power 32. That means ,4.3 billion possibilities. Imagine you have a computer with one million microprocessors on it. Each microprocessors take one GB CPU speed. If you try this 4.3 billion possibilities then it will take only 2.15 milliseconds. Or if you have for one encryption in one microsecond, then you will take 35.8 minutes, I microsecond and one encryption .So in today's world having one million microprocessors is not a big deal anymore. 1GB microprocessor CPU cost how much money??.. 100$ or something, so one million of that thing will cost you 100 million dollars or something. 100 million dollars is not a big deal for CIA kind of institution. They easily spend that money, as government has spent 800billion dollars for that Iraq war. It's a huge amount of money. Infront of 800 billion 100 million is nothing, so you can spend on that machine. So if you are using 32 bit size then they are going to find your machine in 2.15 milli seconds. Then if you are going to take 56 bits then its going to take 10 hrs. 56 bits was the standard for the long time . and that's the best key size basically, if this 56 bits, its going to take 10 hrs . And we use that 56 bits for 10hours basically. With this computer its going to take too much time. We increased the key size and we made it 128 bits, today's standard. Today standard key size is 128 bits and with 128 bits how many, key I have its 3.4 *10 to the power 38 ,if we try many possibilities, and you are going to have 5.4 into 10 to the power 38 years. 10 to the power 38 is more than a billion years. Its going to take more than a billion years if you have 1 million processors, to try all the 128 combinations and today's combination, is 128 bits ,so it is not easy to find the key in other words. For this brute force search, if we increase it to 168, its going to 5.9 into 10 to the power 38 this time, it Is huge this time, but if we use only 26 characters ,then permutation of those characters might take upto, million years. And we are going to see that in substitution ciphers. So today's standard is 128

bits and yesterdays standard was 56 bits, but this 56 bits is no longer secure ,so we are having this 128 bits encryption.