<u>Substitution Cipher</u>

<u>The science of secrecy 01</u>

This is personally the most exciting idea throughout the course at least according to me, we are going to talk about the science of secrecy. If you know what that means let me illustrate this with an example. Assume Romeo and Juliet they want to communicate with each other secretly how would they go about communicating? Assume Romeo wants to send this long a letter to Juliet then he suspects someone in between, may probably tamper with the letter and then see what is written, he wants only Juliet to read it. In case someone else gets hold of the letter they can of course read it but it should not make sense to them. How would he ensure that he encrypts the letter? A very simple method goes as follows. So this is the letter Romeo wants to write for his sweetheart Juliet as you can see it's a love letter, so what he does he firstly writes the letter and then shifts every single alphabet by five units so which means A becomes F, B becomes G and so on so from A to Z this is what happens to the letters and this particular letter that Romeo want to send to Juliet takes this form and now the letter finally looks something like this and Romeo sends it to his beloved Juliet and Juliet gets this and knows what exactly Romeo has done to his original letter basically they have communicated about this protocol before and what Juliet done has the following as you would have guessed obviously she shifts it back five units which means she makes F A G becomes B and so on and there you are she gets the original letter, you see the shift being five is the secret key here it can be five between Romeo Juliet and laila and majnu it can be fifteen now, what if someone gets to know that the method used by the lovers is simply shifting it by some units and mediator comes and catches hold of the letter communicated by this boy friend to his girl friend can he break his code? So this middle man comes and catches hold of the letter sent by our boy to his girl, he knows that the idea here is shifting every single letter by few units so what he does is try all possible shifts, he first tries one shift and tries to see if the text makes sense or not, so whatever you are seeing right now let us take this three lines text as the letter that the boy writes to his girl and then it is shifted by some units that the middle man doesn't know but he wants to crack it. So he tries assigning A to B, B to C, C to D by that i mean he assumes it to be one shift and tries to see if the text that generated makes sense or not as you can see it is not making sense and he tries a two shift and then a three shift and then a four and then a five and then a six and than a seven and finally when he does eight he sees that the shift is actually making sense completely all the words are English words and hence he concludes that the shift this boy is using happens to be eight and there he is, he has deciphered the encrypted text with his little intelligence so what do you infer from this? Such a method is used between two people to communicate can be broken easily by a mediator a middle man, if he knows provided that the technique used is shifting but he doesn't know by what units it being shifted so what he does? He tries all possible shifts; from shift one to shift twenty five twenty six and so on tight? One of them should give him valid English text once he gets the valid English text he concludes he has decrypted the secret. What we saw just now is called the popularly the Caesar cipher in the literature of cryptography. A very well know technique which is not being used mainly because of its simplicity and the fact that anyone can break it, now i am going to teach you a technique which is a little more complicated rather a lot more complicated than what i explain just now the Caesar cipher i am going to tell something else which is lot more complicated, which appears as though nobody can break this. Here is a lot more complicated way of encrypting a given text and here is how it goes. You take every single English letter and assign a complicated symbol to it and a Romeo writes along a letter for his Juliet and simply takes every single letter, every single symbol and instead of using the English alphabet letters he uses the corresponding symbols that is agreed between Romeo and Juliet now according to what i just now illustrated A stand for this symbol, B stand for this symbol and so on up to Z and Romeo converts his letter his love letter to something as complicated looking as this, now its look like it going to be impossible for anybody to crack this isn't it? Who on earth knows what letter is map to what letter right? This looks like a perfect way of communicating. Or is it, is there a way to break even this cipher? Let us take a break and let me tell you all a nice story, a story that looks completely unrelated to what we are talking but is very related. There was this mom who had ten sons all of different heights and one day the sons trying a prank on their mom they wore masks disguising themselves and they come in front of their mom and then challenge her to identify who is who? All ten sons they appear in front of her like this and say mom identify us, they say that in chorus and mom is perplexed because she cannot see the faces of her sons but then i told you something there are all of different heights, so do you think it will be difficult for the mom to identify who is who? All ten sons are masked and they appear in front of their mom and say mom identify us? Hoping that they are they will make the mom perplexed and that she will not able to identify them, little do they know that mom can identify her sons just by identifying their heights she knows that the shortest is this, the second shortest is this, third is this so on and the tallest who is this and she goes on in no time calling out their names, patting on their back one at a time she says athri, brugu, kuthra, vashista, gowthama, kashyapa, angerasa, rama, bheema, shaama over all ten names right? What exactly did she used to identify them, just their heights and what's the moral? The moral is that despite the fact that sons concealed their identity with their mask, mother used some other parameter. So what's the moral of the story, why the story am it's are encryption decryption theory? Do you see a connection? Well there indeed is a connection and this is the connection. You can try to conceal the letters in the form of symbols but then you see English speaks out aloud, what do i mean by this? English has a very peculiar statistical property, sounds complicated? Nothing at all. It i just i just mean the following, the most frequently occurring word letter in English always happens to be this, isn't this a beautiful idea? Its sounds as though it's impossible for anyone to decode a substitution of the letters of the English alphabet with some random symbols, its look like it's impossible to break this code but you see how English speaks out aloud and anybody can very easily decrypt the text. The seemingly looking seemingly complicated looking technique has a huge loop whole in fact it is as easy as a previous one that we discussed. So this subject is called cryptography where the idea is all about making ciphers and also breaking it, almost every single technique that has come about the history is broken and the ones that is currently in place i believe are just in the status of yet to be broken, so the science of secrecy is all about making and breaking the codes, it is reached than what i illustrated just now i invite you all to read more of it i will give you some references to good books for the same you can go ahead and read more of what makes cryptography.