Demystifying networking

Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 73
From Secret Box to Encryption

Now, as you have seen in our previous lectures that the information that goes around is in clear text. I mean if anybody captures that information that is available to be read in the way it is and for example, if you are sending your passwords. So, if the passwords are captured in clear text, anybody who captures it could know your password. So, it is prone to something called eavesdropping which is basically that somebody is trying to listen over the conversation. So, in networks what they have done is, they have use something called encryption.

Encryption is basically changing the human readable form using some mathematical function. A very basic example or the first time when encryption was used was some something at the time of the roman emperors and these are called the Caesar Cipher. So, how it would happen is. So, instead of the alphabet A, they would use C which is the third alphabet. So, the entire message would be coded in such a way where the alphabet they have to use suppose they have to write A B C. So, they will write C D E.

So, this was one of the earlier ways of using an encryption. So, later it started evolving by changing the delta which is here it was 3. So, they would use say 4 or for each communication they would change just a number of shifts that they have to do and they would just communicate the number.

Yeah.

So, that became the secret that they were sharing instead of the entire key and even this was prone to leakages like somebody could leak out what the key was and again the encryption could be broken. So, in the current scenarios what we see is a very much more complicated forms of encryption. So, we have two types of encryptions one is called a symmetric and the other the other is calle asymmetric. Symmetric is the one we saw like in Caesar Cipher. Symmetric means your encryption or coding uses the same key and decryption which is a decoding uses the same key.

So, it is the symmetric use of keys whereas in asymmetric encryption what we see is, we use a different key for coding it and different key for decoding it, as you said encryption and decryption.

So, that was the example that we saw in Aditi and Balraj’s case. Along with encryption, public private key pair or what we just saw, the two key pairs as done as you are talking about the public part and the private part. So, this can also be used to authenticate.

We will be looking at these three terms called confidentiality, integrity and availability, these are the three key terms of what security is about and there you will see how this encryption and a few other techniques can be used to achieve those and along with this we could also use a hybrid method which is like we can use asymmetric and symmetric. So, that could be in a way that if you were to send the symmetric key earlier that we sending which was prone to eavesdropping.

So, what we could do is send key using the asymmetric encryption and then the measure of the majority of the communication could happen using the symmetric and why to do so, because symmetric encryption is something which is not that process in intensive as compared to asymmetric. So, you could just send the key by Asymmetric and we could have the communication in a Symmetric manner.