

Introduction to Information Security

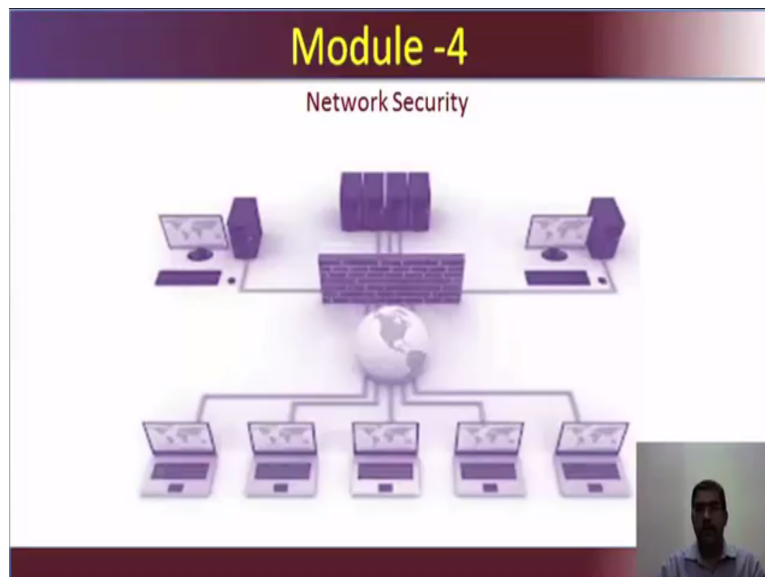
Prof. Dilip H. Ayyar

Department of Computer Science and Engineering

Indian Institute of Technology, Madras

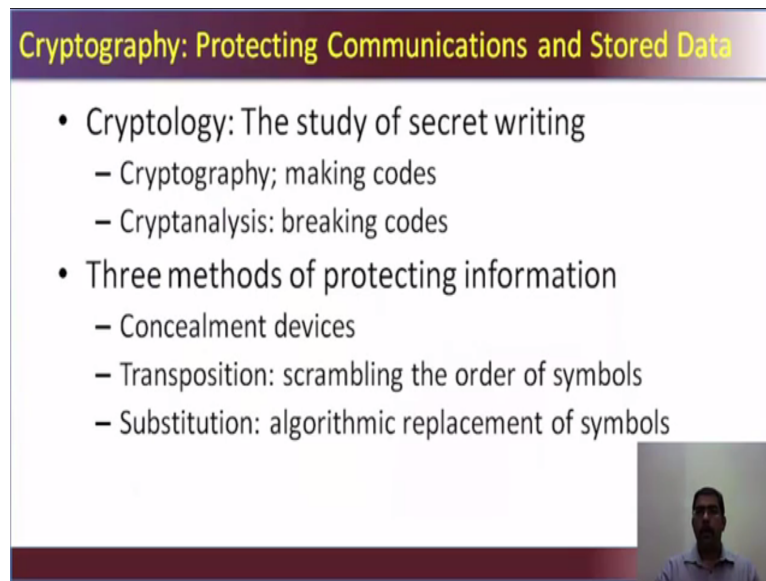
Lecture – 41 Network Security

(Refer Slide Time: 00:10)



Welcome to module 4, this deals with network security. As you all know network in itself is a huge area of study, you need a separate module to learn about the basics of networks itself. What we are trying to do here is bring you some of the important concepts that are required in network security. And also how to do network assessments. Let us start module 4.

(Refer Slide Time: 00:42)

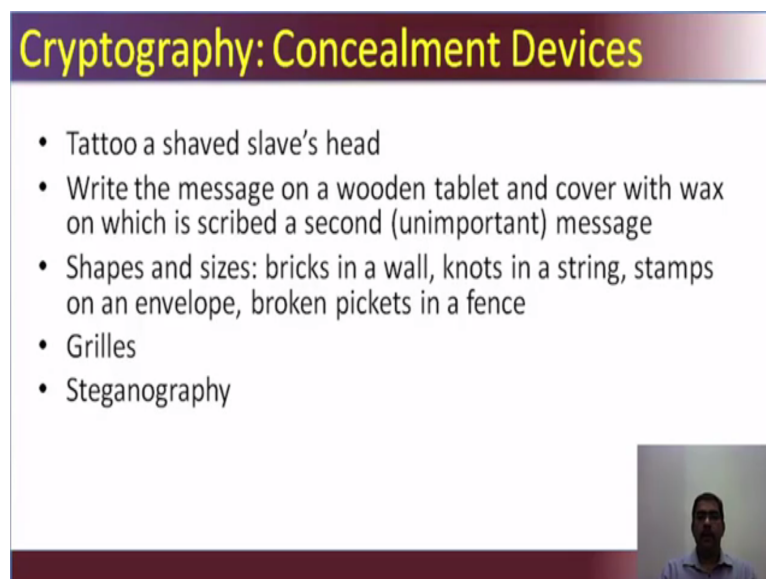


Cryptography: Protecting Communications and Stored Data

- Cryptology: The study of secret writing
 - Cryptography; making codes
 - Cryptanalysis: breaking codes
- Three methods of protecting information
 - Concealment devices
 - Transposition: scrambling the order of symbols
 - Substitution: algorithmic replacement of symbols

We will start with cryptography, which is protecting communicating and store data. What is cryptology? Cryptology is the study of secret writing, cryptography is making the codes, crypt-analysis is the breaking the codes. And there are three methods of protecting information concealment devices, transposition, and substitution. You can also say cryptography is the art of converting a legible text to something that is not legible, or not readable. But that is what basically cryptography is, let us move on and see the in the forth coming slides.

(Refer Slide Time: 01:26)



Cryptography: Concealment Devices

- Tattoo a shaved slave's head
- Write the message on a wooden tablet and cover with wax on which is scribed a second (unimportant) message
- Shapes and sizes: bricks in a wall, knots in a string, stamps on an envelope, broken pickets in a fence
- Grilles
- Steganography

In cryptography let us look at concealment devices, tattoo a shaved slave's head or write a message on a wooden tablet and cover with wax on which is scribed as second unimportant

message. Shapes and sizes like, bricks in the wall knots in a string stamps on a envelope broken pickets in a fence, then grilles and also steganography.

Now, in ancient Rome they used to tattoo a shaved slave's head, and send the slave to a place where the message was required. So by the time the slaves reached that place, you know their hair would have grown back, so on the way nobody used to suspect that they are carriers of some message. For once they reached the destination their heads were shaved again, thereby revealing what was in their head or transcribed in their head. That was the method of encryption, then again in Rome the messages were written on a wooden tablet, they were coated with a thick layer of wax. And then unimportant message was written on top of it.

So, even if the tablet was intercepted only the wax message used to be displayed, behind the wax messages once the wax is melted away, then the original content was revealed. Then shapes and sizes, sharing the code with the receiver saying that the third brick from the left, fourth brick from the bottom top right so on and so forth. Similarly, knots in a string, two knots signifies something, three signifies something, seven signifies something. Stamps on a envelope, number of stamps determine what the message or how the message has to be read. Broken pickets in a fence, then grilles and steganography, we will look at in the coming slides.

(Refer Slide Time: 03:45)

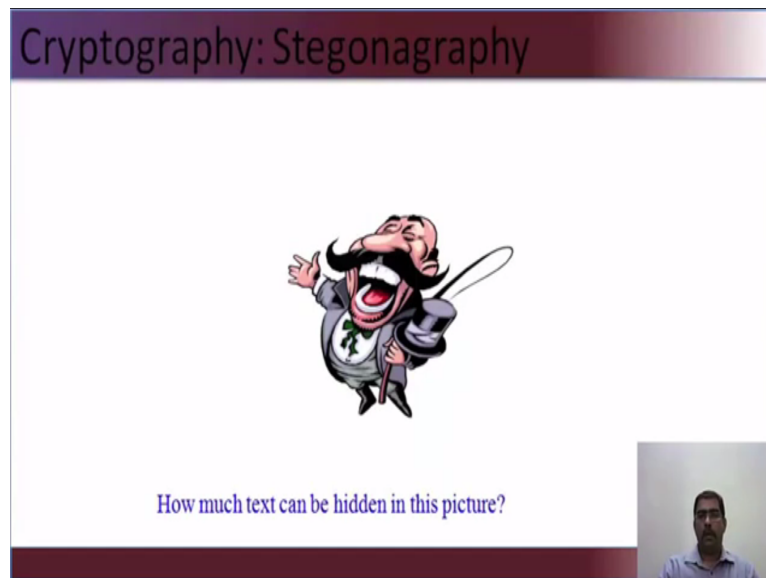
Cryptography: Grilles

Attacking the newest type of crossword puzzle requires a new approach to word structure, at least if puzzles are to be solved without staying up until dawn working with dictionaries.

This is a simple example of grilles or grilles, attack at dawn is the message it is written in such a way that only the sender and receiver, know where the letters or words have to be

read. So here if you see attach at dawn can be read by both the sender and the receiver, for any other person reading this, it just means as simple sentence or a paragraph.

(Refer Slide Time: 04:23)



Then comes steganography, how much text can be hidden in this picture? So a lot of text can be hidden in pictures there are methods of doing that, there are binders available for doing that binder softwares. So, lot of text can be hidden within a picture and then transmitted, so the receiver will know where the text is or how to retrieve that because it is pre shared. So, it is possible to insert text or put messages into a picture and transfer.

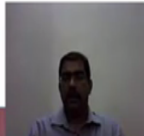
What you have to understand here is even when you downloading messages from the internet, you have to make sure there is nothing within the picture. Nowadays the high resolution images are very high in size or big in size. So, it is difficult to know what is there within the picture, whether it is a genuine picture or not, but a unusually large size of image you should be very wary enough.

(Refer Slide Time: 05:59)

Cryptography: Transposition

A T C A D W
\\//\\//\\//\\//
T A K T A N

AAAA
TCTW
TKDN



Let us see what is transposition cipher, the same message attack at dawn. If the position is changed, the position of the letters is changed, if you see the right hand side of the screen 4 A's T C T W T K D N, but there is a method of reading this. Again in a predefined manner, you read top down from the first row onwards first column onwards A T T A C K A T D A W N. So, you get attack at dawn this is basically a small example of how a transposition works.


(Refer Slide Time: 06:04)

Cryptography: Substitution - Caesar's Cipher

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

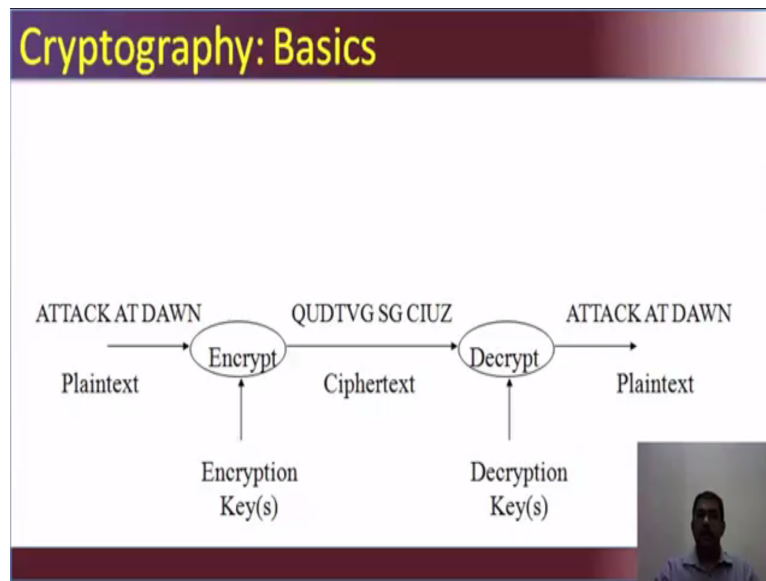
Plaintext: NOW IS THE TIME FOR ALL GOOD PEOPLE TO COME
TO THE

Ciphertext: KLT FP QEB QFJB CLO XII DLLA MBLMIBQLZLJB QL
QEB



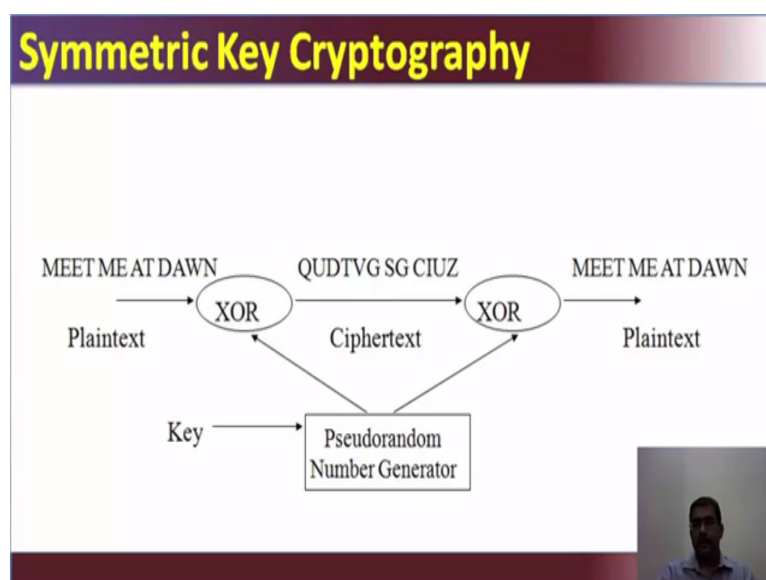
Then there is something called the Caesar's cipher, if you see the plain text. Now is the time for all good people to come to the. that is the plain text, now using Caesar's cipher if you see the two rows on top A is substituted by X, B with Y and so on. For now is K LT so if you say now is K L T, F P means is S, so it is decoded this way to decrypt.

(Refer Slide Time: 06:37)



A simple representation of how cryptography works, attack at dawn as a plain text, it is put through a encryption algorithm or a encryption key is punched into attack at dawn. You get a resulting cipher text, at the receiving end the message or the cipher text is decrypted with a decryption key or again the algorithm that is used for encrypting. Then you will get a resulting plain text that is attack at dawn. So, here in this case the keys are shared, so the message or the keys that are used encryption is used for decryption.

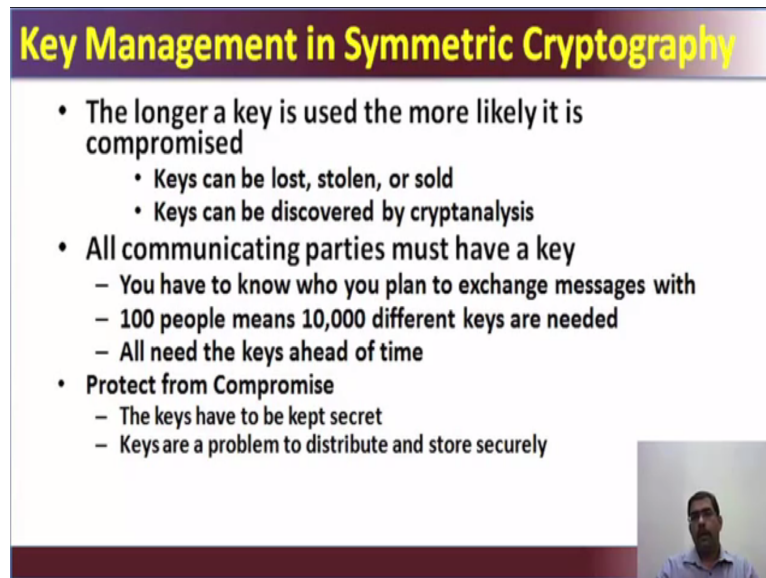
(Refer Slide Time: 07:23)



That is the fundamental concept of symmetric key cryptography. Now meet me at dawn is the plain text it is passed through a pseudo number generator, or a algorithm you get the resulting cipher text. Now with the same algorithm you decrypt the message, and you get meet me at


dawn as the plain text. So, symmetric key uses both or uses a single key for both encryption and decryption. So, the sender as well as receivers should have both the or both should have same key.

(Refer Slide Time: 08:01)



Key Management in Symmetric Cryptography

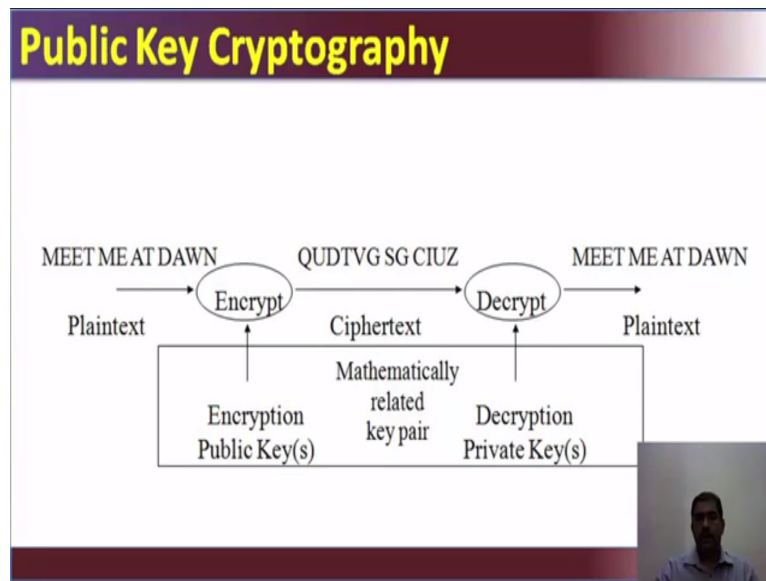
- **The longer a key is used the more likely it is compromised**
 - Keys can be lost, stolen, or sold
 - Keys can be discovered by cryptanalysis
- **All communicating parties must have a key**
 - You have to know who you plan to exchange messages with
 - 100 people means 10,000 different keys are needed
 - All need the keys ahead of time
- **Protect from Compromise**
 - The keys have to be kept secret
 - Keys are a problem to distribute and store securely



But there are key management issues in symmetric cryptography. What is it? The longer the key is used the more likely it is compromised, what it basically means is the longer time that you use a key, the more likely that it could be compromised. That means keys can be lost it can be stolen or it can be sold, keys can be discovered by crypt analysis. So the downfall of symmetric key crypto system is or cryptography is the longer a key is used the more likely that it could be compromised.

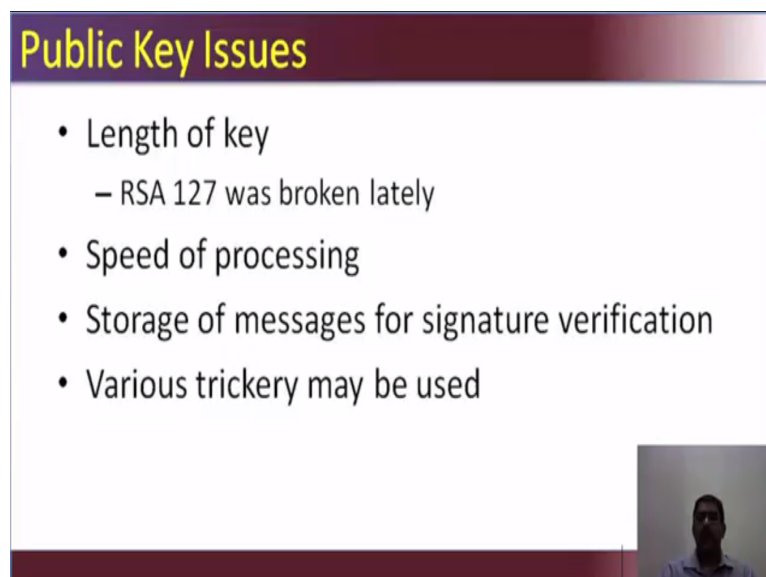
Then all communicating parties that is both the sender and the receivers, should have the key. You have to know who you trying to exchange the message with, so if you are in sync with or if you are sending a message with hundred people, means you need ten thousand different keys. All need the key ahead of time meaning, you have to send the key much before they received a message, otherwise they cannot decrypt a message. Then you have to protect the keys from compromise, the keys have to be kept secret, keys are a problem to distribute and store securely. How will you send a keys, how will you transmit the keys that is a problem. What if there is a man in the middle attack and somebody tries to get the keys, that is an issue. So, these are some of the issues of key management in symmetric cryptography.

(Refer Slide Time: 09:31)



To overcome this issue of key management of public key cryptography, come into work public key cryptography is also called asymmetric cryptography. So, there are two symmetric and asymmetric cryptography, or symmetric and public key cryptography. Now, the same message when you are using the public key, the meet me at dawn you message the plain text is encrypted using a public key. So, you get a cypher text, it is send to the receiver, it is decrypted using a private key. So, you get a resultant plain text what you have to note here is the encryption or the public key and the private key are a mathematically related key pair. That means you encrypted the public key for that the receiver can be encrypt with his or her private key.

(Refer Slide Time: 10:30)



But there are issues with public key also, the length of the key is a factor RSA 127 was broken sometime back. Then it requires a lot of processing power, so the speed of processing is an issue. Storage of message for signature verification is an issue.