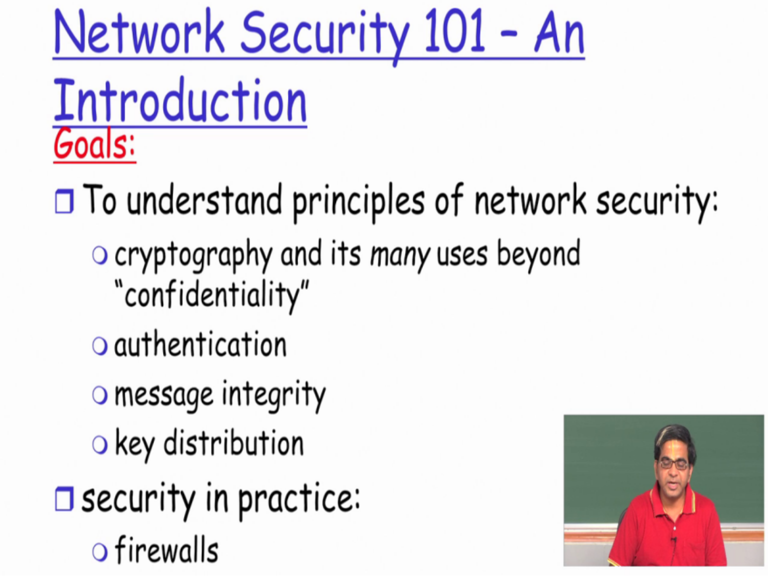
Information Security 3
Sri M J Shankar Raman,
Consultant Department of Computer Science and Engineering,
Indian Institute of Technology Madras
Module 51
Network Security: An Introduction

(Refer Slide Time: 00:17)



Network Security 101 - An Introduction

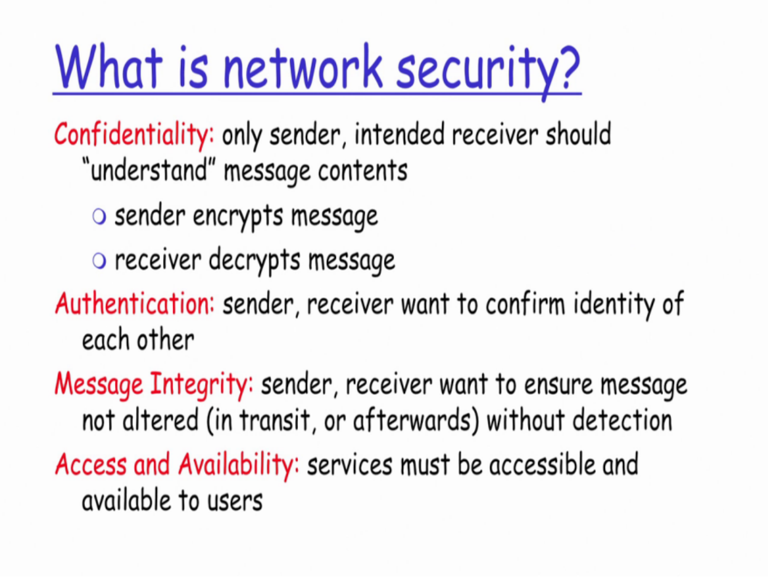
Goals:

- To understand principles of network security:
  - cryptography and its *many* uses beyond "confidentiality"
  - authentication
  - message integrity
  - key distribution
- security in practice:
  - firewalls

Over the next set of modules in this course we will actually be trying to talk about the basic principles of network security wherein we will introduce the concepts of cryptography and the associated security principles like confidentiality, authentication, message integrity and the kind of keys that is actually used for securing the communication as well as how those keys are distributed.

So later on we will also see some of the products that are typically deployed from the point of view of network security to get a feel of how these different principles of network security are actually implemented in these kind of products and software tools.

(Refer Slide Time: 01:01)



What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and Availability: services must be accessible and available to users

So if I have to introduce about network security we need to look at the different types of principles on which the which is actually provided by security, so the first and which is actually provided by security, so the first and foremost is basically what we are referring to here as confidentiality right.

So we all would have actually heard about confidential documents or confidential messages in our normal speaking parlance but when it comes to network security what we actually try to mean here is that the sender and the intended receiver only should understand the message contents right,

So essentially the the keyword here is understand and also the word only right, so what we essentially mean here is that if some unknown or unauthorized person tries to take look at the contents of what is getting communicated between two different parties then that person even if he is able to look at the message should not be able to understand what exactly was the intended message right.

So how is it typically done is the sender encrypts the message and receiver decrypts the message so by this way even if an unauthorized third party tries to basically look at the message in the middle when it is getting transferred on the wire, they will not be able to sort of get back the original message without knowing something what is called as a key and this key is basically like a key to our houses without which we will not be able to open it likewise without the presence of the key nobody will be able to sort of get back the original message that the sender originally wanted to communicate.

So the next principle is basically what is referred to as a authentication, now what we mean by authentication here is that it would be required that the sender and the receiver would want to sort of confirm their identity to other party, so the sender would need to confirm who is he really to the receiver and there will be situations where the receiver also would be required to be confirming to the sender on who is that particular system is trying to act as right.

So essentially authentication is basically ensuring that the other party to whom this communication is being setup or data is getting transferred is really the person who is actually it is intended to be right, so by this way I just ensure that I don't by mistake transfer the content across to some other person who is not the really the intended recipient of this particular message.

The next part is basically what is refer to as message integrity so with the message integrity we basically ensure that the message does not get altered right, so the alteration could either happen by any chance or it could also happen specifically done by any mischievous person right and similarly this alteration of the message could happen when the message is actually in transit over the wire from the sender to the receiver or it could even happen afterwards when the when the message is received and stored in a particular location, right?

So what we mean here by message integrity principle is that whenever the sender and the receiver wants to ensure that there has been no modification or corruption of the message and it has been received and it is being seen as it was at the time of transmission then the message integrity part of the principle helps us to ensure and any kind of modifications getting detected which any kind of modifications that is actually happened as part of it getting transmitted or when it is getting stored after receiving the data right.

So this is just to ensure that again spurious hacker has not intersected the message modified the contents and reintroduced it all the way to be sent to the receiver without the receiver being aware that something like this some sort of a modification is actually been as actually happened when a message was in transit from the sender to him right, then the next two parts of it is what is refer to as access and availability.

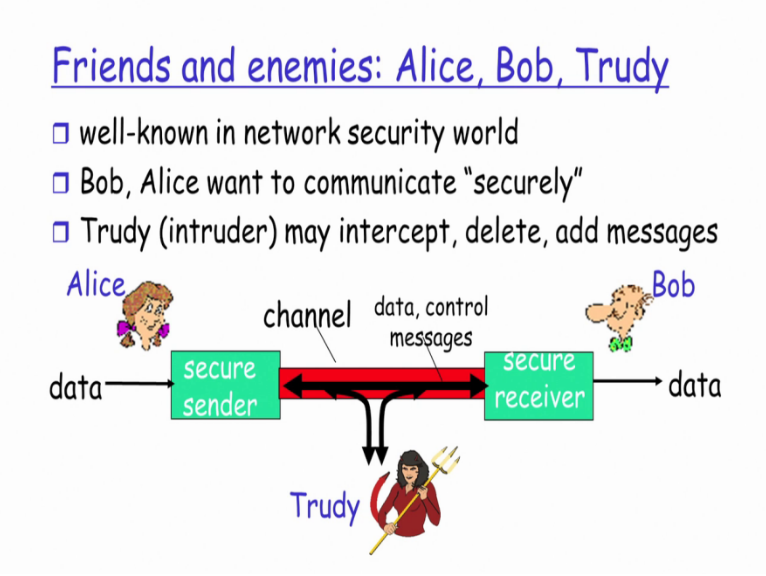
So all these services that are that are claiming to be very secure should always be accessible and also available to users, so essentially here we are talking of any kind of possible attacks like what some of us would have heard about called as a deep dos or d dos os the dos stands for denial of service and d dos stands for distributed denial of service where the hacker sitting outside your network typically would be able to attack and bring down very important server or a service running in any of the server missions in such a way that it is essentially brings down the entire organization from being able to work right.

So for example let us say that the organization is actually using a central authentication server like something like an LDAP or an active directory on windows right, now if this ads server as as some of us would know the ads server if if it is authentication server in a centralized location for the organization, this server needs to be up and running for the individual employees or the users or the organization to be able to successfully login into their network and then a sort of do their work in terms of trying to access the data or modify the data or whatever it is right,

Now if a hacker sitting outside the network wants to potentially bring down the entire network all he or she has to basically do is to ensure that this particular ads server is attacked and then brought down with which he will be able to make sure that none of the users in that particular organization or in that particular network will ever be able to do any work thereby ensuring that practically for all practical purposes the the entire organization has been brought down to its knees right.

So we will have certain mechanisms which are actually put in place to ensure that the the principles of access and availability is also provided through some specific mechanisms when we talk about network security.

(Refer Slide Time: 07:54)



Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages

So when we talk about network security you need to classify people is either a friend or an enemy right, so a friend is somebody with whom you are actually expecting to talk or who is also possibly a a authorized user who can actually communicate with you and get the data from you right,

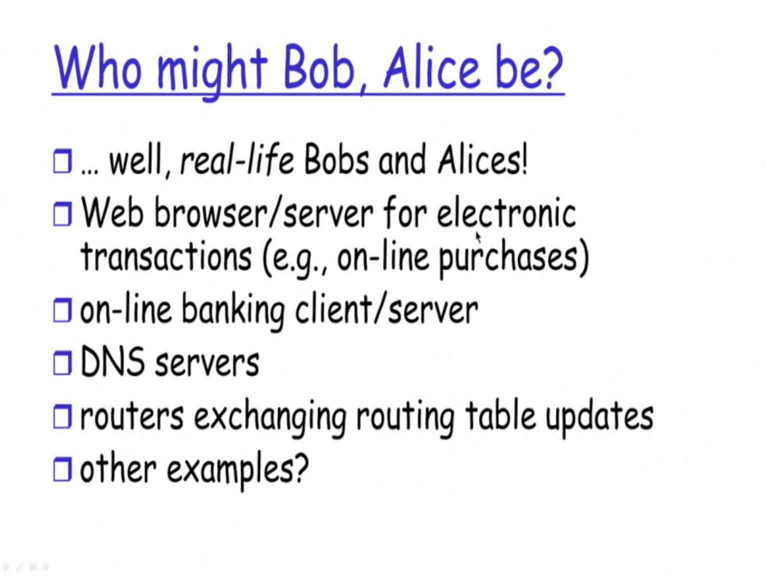
So here the word user is referred to as somebody denoting a normal system user or the user could also in some context refer to a system or a host or a node in my entire network right. So that's basically how we will have to coral it it when we hear the word user in the context of the network security domain.

so here the basic objective here is that there are two users bob and Alice who wants to talk in a very secure manner so we just defined security with authentication with confidentiality and so on in such a way that a Trudy another character if he basically tries to intercept the messages or make any kind of modifications like deleting or adding the messages then this particular character should not be able to do that right,

so here we are going to be having something called as a secure sender and a secure receiver, secure sender will basically be doing the encryption of the data and then sending it into a channel which is expected to be a secure channel and a secure receiver will be doing the decryption on the data in such a way that the the receiver basically is able to extract the original data that the sender was actually trying to send the data to right.

So here we are talking of a mechanism to make the sender secure we are talking of a mechanism to make the receiver secure and we are talking of a mechanism to have a secure channel of communication between the secure sender and the secure receiver in such a way that any kind of an intruder wanting to intercept the messages is not successful in their attempts right.

(Refer Slide Time: 09:58)



Who might Bob, Alice be?

- ... well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

So in the real world whenever people talk to you about network security who all will these Bobs and Alice’s map onto right, so it could really be a pair of a web browser, web server that is actually been doing for electronic transactions so we all right now buy a lot of things from the ecommerce portals and we all use typically a web browser to connect to our e commerce portal site for buying the things that we require.

And when we login in this manner after selecting whatever items you want to buy we also give them our confidential details like typically either our bank account details or credit card details or whatever it is and these need to go in a very secure manner and reach the intended e commerce web server alone rather than some other server or some other device or whatever it is outside, right?

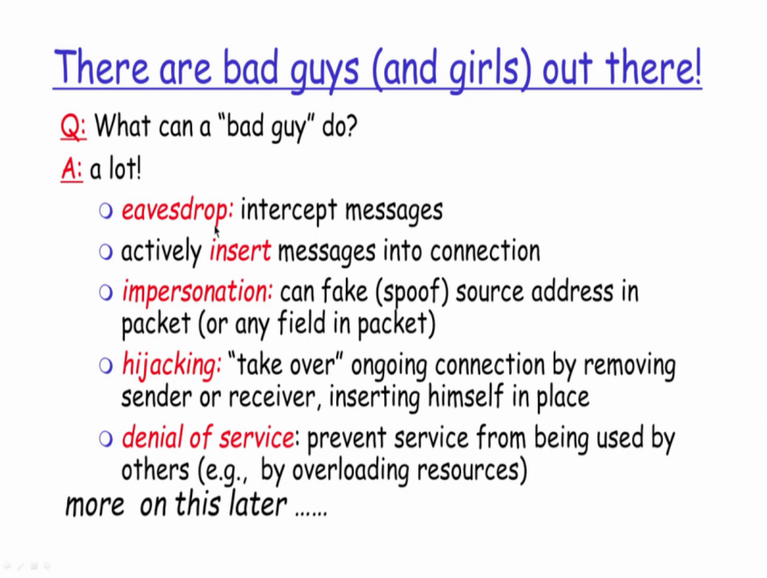
So that is something which is really mandatory and that the web browser and the web server combination here could really be the two parties that we are trying to map onto the bob and Alice of the previous slide or alternatively it also be online banking clients server so it could potentially be your web browser again which is being used for communicating to your bank servers, so if you actually have a bank account with any kind of bank, they all provide online access facilities for you right now.

So you need to talk to the server on the banking portal site in a very secure manner because all your account detail are actually going to go across over the network and these needs to be extremely secure or again it could also be a DNS server. So DNS as most of us would know stands for domain name servers which is actually a network servers that is actually used for mapping the host names to the IP addresses right,

So a DNS client is going to transparently run on your system whenever you give any kind of host name for connecting to irrespective of whatever application it is, so from your males male client on your browser right or any kind of a network in application if you try to use any kind of a host name like www.google.com DNS is a protocol that actually runs to convert that host name to the corresponding IP address so a DNS client wants to talks to the DNS server in a very secure manner otherwise it could.

It has a possibility of it creating a lot of ruckus in the network and similarly routers exchanging the routing table updates also needs to be getting done on a very secure channel and not being able to get easily updated by a spurious update from a device which could be existing or a non existing also right, likewise we could actually think of quite of few other examples also which will require two different parties in a our real life day to day activities today in the highly network world where they have to be having a very secure way of communicating.

(Refer Slide Time: 13:11)



There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

more on this later ……

So if there are bad guys out there of what all could they potentially do right, so they can actually do a lot first and foremost they can just do an eaves drops where they just simply intercept the messages and try to listen to what is actually getting communicated between two parties, what is the pattern of communication right.

So what is the pattern of respond that is actually coming for a particular type of message and all that, so here this is basically what we refer to as a very passive kind of activity which a hacker typically tries to involve with where he or she doesn't try to do any kind of modification or give any kind of signal that they are present in the network but they just simply listen and eaves drop and try to understand the kind of messages that is actually going back and forth or alternatively once they possibly try to understand what is actually happening,

They might start actively inserting the messages into the connection where they get into an active mode from being in a passive mode by just doing an eaves dropping right, so here they actually start participating very actively in the conversation but the problem here is that they are participating in the conversation either representing somebody else or without getting authenticated properly.

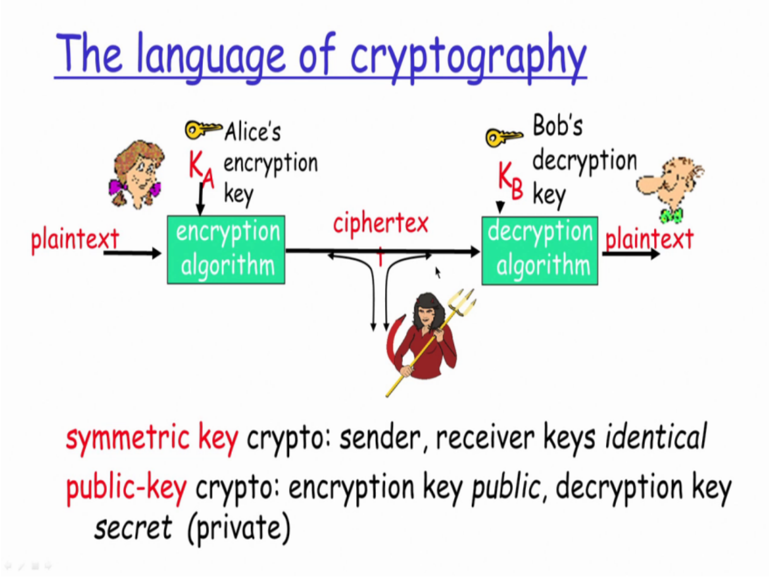
So you don’t want them to really do this because of which I basically try to see what kind of mechanisms I put in place to detect and then eject the amount of my conversation right or alternatively they could also do an impersonation, so impersonation is basically spoofing in such a way that they try to act as somebody else by just possibly modifying the source address in the packet or for that matter any field of the packet.

So by that way they try to impersonate as somebody else which is again a very serious issue for me right or as a next step they can even sort of hijack the entire conversation that is actually happening between two authenticated parties in such a way that the other guy is not even realizing that somebody else is acting as on behalf of the other party with whom he is trying to communicate with or at the most he can receive the go into such an extent that he can do a denial of servers attack so as we were just discussing right now.

I could basically have the hacker prevent his service from being used by anybody else and thereby ensuring that the entire network actually goes down from it being from a useable state to completely unusable state even though all the servers or physically up and running the network connectivity is up and running but by trying to attack one particular servers which is very very critical for the entire network to be use the hacker will ensure by doing a denial of servers attack or a distributed denial of server attack that the entire network just fall flat on its knees right.

So these are the different kinds of things that potentially a hacker could do and all these things needs to be protected against with if we have to have a network that is very secure and which can continue to function 24 X 7.

(Refer Slide Time: 16:19)



The language of cryptography

Alice's encryption key

K_A

Bob's decryption key

K_B

plaintext

encryption algorithm

ciphertex

decryption algorithm

plaintext

symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

So for doing the cryptography as we were saying we will actually have confidentiality, so what we is actually do here is that there are two types of ways by which we will be able to do confidentiality but essentially for all of them I run an encryption algorithm on a sending side and I run a decryption algorithm on the receiver side where the plane text is is is one of the inputs into my encryption algorithm along with a key that is used.

So with both these inputs the plane text is getting converted into a cipher text by the encryption algorithm and then sent on the channel and on the receiver's side the corresponding decryption algorithm will run with the key as an input so for the decryption algorithm I have two inputs, one which is the cipher text that is going inside this block and another which is the decryption key with both these inputs the decryption algorithm will be able to magically generate the original plane text that the sender wanted to send, right?

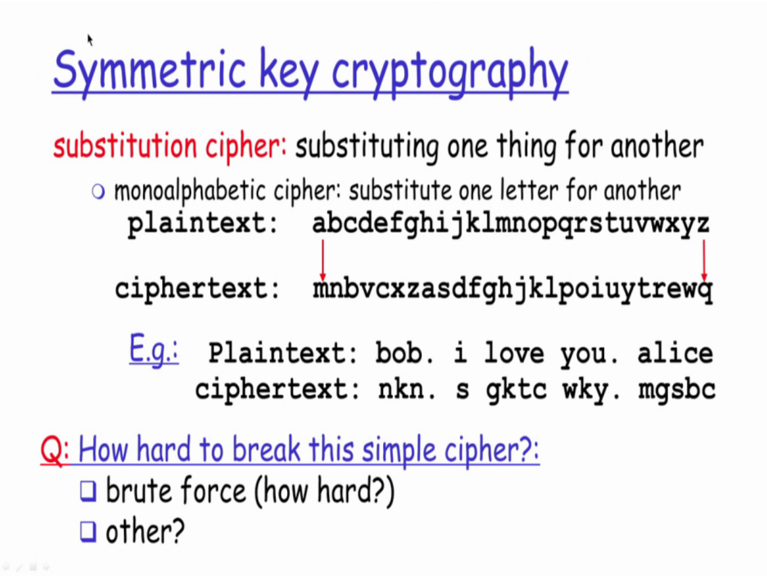
so now what is the advantage that I have here is that, the cipher text that is actually going on the cable right, if my attacker wants to basically take a look at it they will not be able to understand the original contents because it is expected that this hacker or the attacker will not have the key available with him right.

So although he will be able to read the cipher text from my network wire, they will not be able to make head or tail of that and sort of decipher that because the whole message is actually encrypted with the key and this key is not available with the hacker and because of which this whole thing becomes very secure.

Now this encryption algorithm basically here are two types one which is called as a symmetric key and another which is called as asymmetric key or a public key algorithm right, so a symmetric key algorithm I have both the sender and the receiver use the same key right so on the encryption side I will use the same key as what I am actually using for my decryption side for regenerating the message back to plain text.

Whereas in a public key cryptographic algorithm or what we called as an asymmetric cryptographic algorithm, the encryption algorithm will use the different key what is refer to as a public key and the decryption algorithm will use a different key what is refer to as a private key.

(Refer Slide Time: 18:43)



Symmetric key cryptography

substitution cipher: substituting one thing for another

○ monoalphabetic cipher: substitute one letter for another

```
 plaintext:  abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

```
E.g.:  Plaintext: bob. i love you. alice
      ciphertext: nkn. s gktc wky. mgsbc
```

Q: How hard to break this simple cipher?:

□ brute force (how hard?)

□ other?

So in a symmetric key cryptography I could just do a very simple sub substitution cipher, where I will just say that I am just going to convert every character in the input plain text to some other character based on a particular table right.

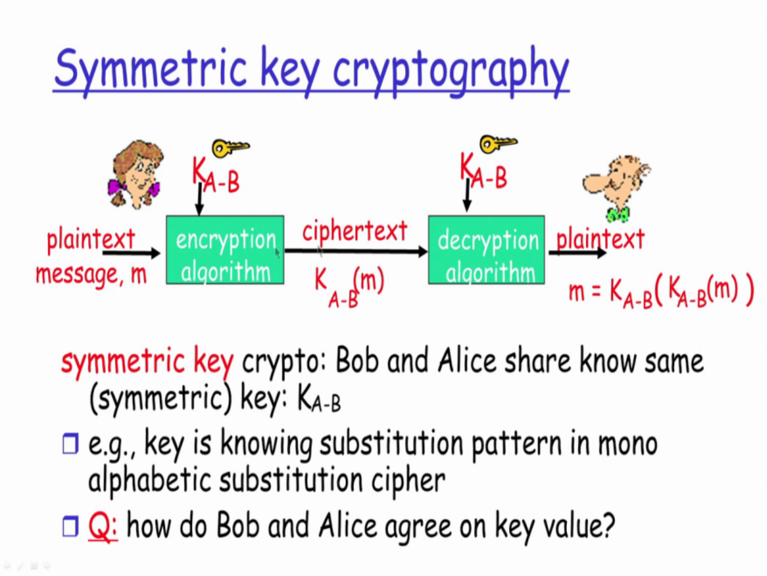
Now in this particular plain text if if I am basically doing this kind of a mapping I can say that the letter a is going to be mapped to letter m, letter b is going to be mapped to n and so on right, so when I receive the cipher text I do the corresponding mapping back into the original plain text by looking at the table indexing into the table finding the corresponding original plain text letter and then putting that as part of my plain text message and I do this for every character with which I will be able to generate the complete original message right,

So I could basically have to do a very brute force method where I just need to find out by looking at different messages what kind of mapping is been used for this substitution cipher algorithm and sometimes it could be very easy depending on in what language the text is being sent right,

Because if you for example take the language of English although you have 26 different alphabets that could be used potentially we all know from our comfortness in English language that there are only handful of characters out of those 26 characters which are very very commonly made use of right.

So the attacker in this with this information will try to ensure that the letters which has a highest amount of frequency probability out of these 26 letters, he first tries to arrive at the mapping for them and with that he will be able to quickly arrive at what are the remaining letters depending on whether there is a two letter word or three letter word in the entire cipher text message that has actually come in right. So it could be potentially easy but again it depends on what kind of language it has been made use of for the substitution cipher converting the plain text to the cipher text right.

(Refer Slide Time: 20:44)



Symmetric key cryptography

K_{A-B}

K_{A-B}

plaintext message, m

encryption algorithm

ciphertext

$K_{A-B}(m)$

decryption algorithm

plaintext

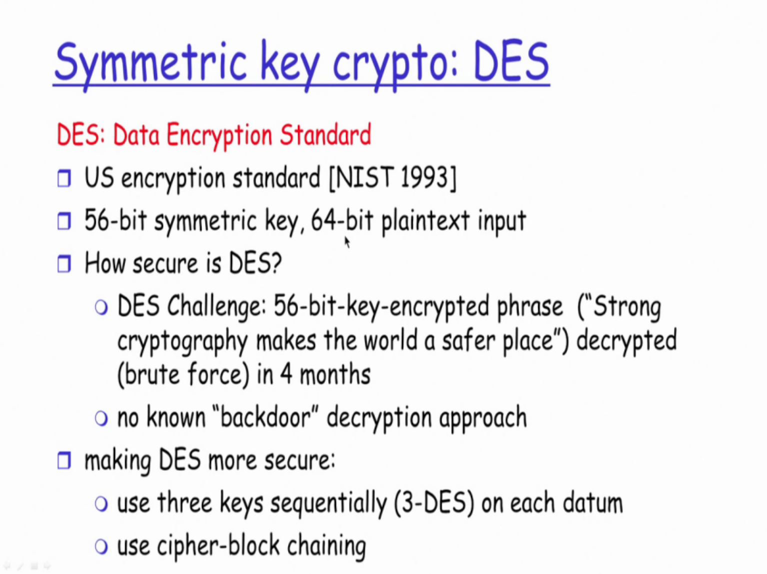
$m = K_{A-B}(K_{A-B}(m))$

symmetric key crypto: Bob and Alice share know same (symmetric) key: K_{A-B}

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- Q: how do Bob and Alice agree on key value?

So a symmetric key cryptography as we were discussing both the sender and the receiver will basically agree upon the key that is being used and the key will be the same on both sides, and the encryption side the same key will be used and at the decryption side the same key will be used to get back the original message.

(Refer Slide Time: 21:03)



Symmetric key crypto: DES

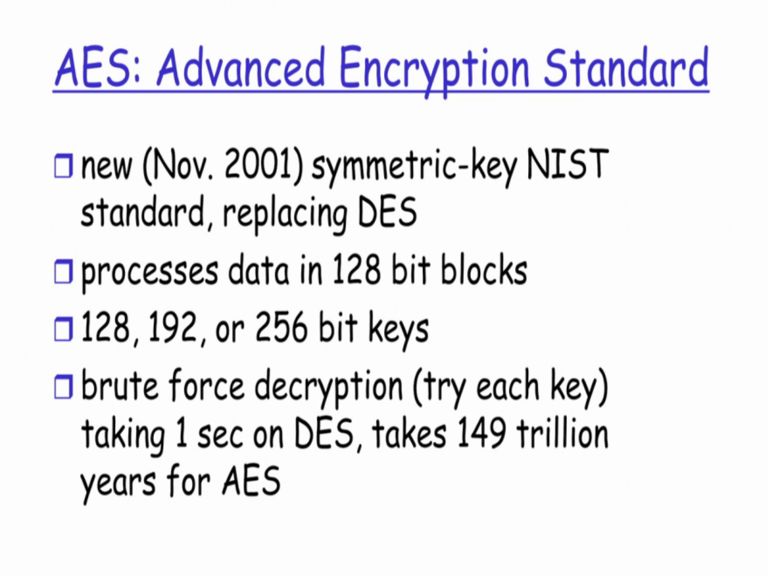
DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64-bit plaintext input
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase ("Strong cryptography makes the world a safer place") decrypted (brute force) in 4 months
  - no known "backdoor" decryption approach
- making DES more secure:
  - use three keys sequentially (3-DES) on each datum
  - use cipher-block chaining

So some of the very common symmetric key cryptographic algorithms are first one which is called as a des, now des stands for data encryption standard it actually came out around 1993 where there is a 56 bit symmetric key and on a 64 bit plain text and it basically goes through multiple iterations of the same modification that is actually done.

But for every modification or every iteration the inputs are basically different because of which with this cipher block chaining approach what is refer to as cbc it basically becomes very secure but after some point in time with the advanced power of the hardware processing capability des was not that much secure

(Refer Slide Time: 21:45)



AES: Advanced Encryption Standard

- new (Nov. 2001) symmetric-key NIST standard, replacing DES
- processes data in 128 bit blocks
- 128, 192, or 256 bit keys
- brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES

So it des was getting replaced with triple des and AES where the AES is stands for advanced encryptions standard, so it basically processes the data in 128 bit blocks and the key size here is basically much bigger so 128 or 122 or 256 big keys that is actually used right.

So because of the amount of the the computation that is done as well as the bigger size of the the key that is there it becomes computationally very very difficult for somebody to hack on to this particular protocol and trying to regenerate the plain text on the cipher text without knowing the key that is used that has been used for the original encryption.

So AES turns out to be pretty much, the most popular symmetric key cryptographic algorithm that is actually being currently used for quite of few security applications today

Thank you.