Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 08
Lecture: 23

Which is cyber security technologies, so we are seeing that as part of cyber security management, you can actually choose to defend or make your defense stronger or invest in mitigation mechanisms. So what are those mechanisms, what are those technologies that exist in cyber security to provide you better security or reduce your cyber risk and well, feel more safe with the new safeguards? So that is the discussion today. So this, let me put an disclaimer, this is an overview, so each of these cyber security technologies are topics, distinct topics in the field of engineering and technologies. So I am not getting into the details, particularly the detail of design but from a managerial perspective for awareness, for having a decent awareness of what do cyber security technologies do and where are they used and probably some functional aspect as to how they work, for example, Cryptography, how does it work ? So that is the sort of plan for this session. Well, I encourage you to watch some movies related to cyber security, I know you watch a lot of science fiction, well I am just presenting two of them which I have watched and it was you know, these are not recent movies when you have so many cyber security incidents. In particular 1984 is a book, of course written by George Orwell in 1949.

So he wrote the book in 1949 predicting what would be a potential scenario in 1984 and it is a classic, of course. George Orwell is someone who is highly respected, especially in political philosophy, I would say he has a book Animal Farm, I recommend that book for you to understand what is politics. And his book 1984 is about surveillance, so how surveillance or surveillance technologies would become a very powerful tool for governments to enter into the private space of individuals and then, you know the government would decide what citizen would do, you know that kind of a situation is what is depicted in 1984. It does not mean that that is the world we live in but we also understand potential abuse of surveillance technologies by agencies who have power.

So it is a power asymmetry essentially, that plays out here, you know you are vulnerable you do not have much say in what government should do and should not do. So the other is, Minority Report of course, you like Tom Cruise, I am sure so Steven Spielberg, famous movie which was released in 2002, Minority Report. So you can see the retinal detection for access to systems. So that is a important topic in the movie. So access control is a mechanism for ensuring cyber security.

So this concept we have already discussed, access control and we know the CIA triangle, coming back to the fundamental aspect of security - confidentiality, integrity and availability are the objectives of cyber security and a mechanism for ensuring confidentiality, integrity and availability would involve four steps. This also we have discussed or covered in one of the sessions - identification, authentication, authorization and accountability. Now in this session, we are going to see how technology can be used for this access control mechanism. We have discussed what access control do but briefly we will try to see how access control technology serve to effect the function of CIA or how access control is enabled by technology. So identification, we have discussed this already, it is about getting your ID okay, each one who wants to access a system or a cyber asset or a cyber service should have a ID.

So creating ID is the first step, we have seen this already and now there are different types of IDs. So the ID card is the classical one. An identifier is something that uniquely identifies a user. You know in British era or for governance in particular, you need to identify citizens and you did not have all the current technologies. In those days, during the colonial days but they used to identify individuals.

When I was in school, there was no ID card but I was identified uniquely, do you know how you were, what was the system in schools and colleges to identify people ? Not biometrics. Not even your photograph. There will be certain unique marks in your body, okay a black mole on the right cheek. So I recall that being recorded every time when they talk about my ID. So permanent body marks, seeming that these marks are permanent and the particular spot where that mark exist in your body may be very unique to you.

So but you can see it is it, whether it is very unique or not, you can always question but that those were the methods or rudimentary methods that existed for identification. But today you have advanced techniques and the second step is, of course authentication. Once you have the ID and that ID is stored somewhere, okay when you present yourself for a service, then whatever you present is compared with what is stored, okay so that comparison is known as authentication, whether you are the person whom you claim to be, okay. You say I am X, I need to verify that you are X, so authentication is the process of establishing you are whom you claim to be and how is the authentication done? There are different methods, some of the methods are shown here. It could be using something you know.

Password is a method for authentication. Password is something that is unique, only you know, okay and it is stored and you have stored your password and then you give your password because only you know this and it is compared. Passphrase is, I think getting some importance today because password can be sort of cracked. So passphrase is a longer

expression, it is a phrase, not a word. Okay, so that is another method.

Password I think, was developed in MIT many decades ago, passphrase is under discussion today and you also know the one-time password today, okay. We live in the era of multi-factor authentication. I think one of the groups referred to multi-factor authentication, okay authentication can be done using one factor like the password or passphrase. Authentication can also be done using multiple factors. For example, you log in, if you, if you today log in to say, State Bank of India for accessing your bank account, I first say what is my username.

That is my ID, that is what I claim to be, okay that is the first step. You say who you are, okay we want to verify who you are. Give your password, okay. I give my password. They compare my password with what is stored, that is first factor authentication.

The first factor is the password, okay. Then are you a man or an animal, okay? So you have the CAPTCHA code. So that actually as a second step, ensures that you are a human being, not a script. Then you are allowed entry into the next level. In the next level, there is a OTP, OTP actually goes to a different device, okay.

So password is in your mind, it is stored somewhere, okay. In the multi-factor authentication, the second factor comes from a different device, okay. You have to read that from something you own, okay something which is yours, okay and that is your phone. You know in India, of course because of our tele density touching close to 100%, that has become a mechanism for multi-factor authentication. So the one time password is the second factor, I would say, the second factor in authentication.

So there are three factor authentication and so on which Apple uses. So basically to be very very very sure that it is you and not anybody else, okay. So it increases the level of access control, when you have multi-factor authentication. So the other methods are, you know you have smart cards, you have fingerprints, retina and iris scans, okay. These are properties of the eyes which are unique to an individual.

For example, the blood veins or the vessels in your retina, the patterns are very unique to each individual, just like your fingerprints or the iris scans which is actually the pattern around your pupil, pupil of the eye. So these are actually parts of your body which are unique to you, okay and that, when it is captured using camera and stored becomes a ID, becomes an ID of you. That is your identity, okay so which can be used for authentication and the fourth type of authentication could be using what you produce- your voice, your signature etc. You know that is something that you produce. So you can see the different methods of authentication using different types of IDs or a combination of them, which

is called multi-factor authentication and this can be biometric.

That is a part of your body or it can be, you know non biometric. So both can be used in combination. Now since biometric devices are widely used in cybersecurity, particularly for access control. From a technology point of view, one must be aware of certain limitations of biometrics. So this graph depicts the limitations while using biometric devices.

In India, I have read the cases of implementing e-governance services particularly for rations, okay, so one of the challenges India faces while deploying digital technologies is the problem of digital inclusion. So in urban settings, we are all privileged to be very aware and updated about technology and we use technology. You can go to a retail store and use any payment methods today which you want. You can use a UPI, you can use a credit card or a debit card, you can pay in cash but if you go to a rural area in a, farmer does not have a credit card and may not be even aware. So they are excluded from the benefits of digital technology.

So what the government in several states try to do is to make it easy for them and include them also into the benefits of digital technology. So they developed fingerprint based authentication for providing ration. So in Krishna district of Andhra Pradesh, where I actually met the IAS officer who was implementing this project, it came for a competition, a national level competition and I was one of the judges and they made a good presentation on how the system was implemented. So a farmer could actually come to the ration shop and may not be having a wallet or cash but still can get her or his ration by just showing the fingerprints. So the fingerprint biometrics is already taken from these users and stored in the system and the, there is a Adhar and Adhar linked bank account.

So the bank account is also linked to the ration system, the distribution system. So when you actually want a ration, say 2 kg of rice and then you show that I want the payment to be done from my bank account directly. So you authenticate, do that, so then you show your fingerprint with that the payment will be completed. So this is like acting as your credit card. So in credit card you swipe, Hey, take my fingerprint, it is very good thinking but they face problems while implementing this solution because the ridges, the ridges in the finger, they get worn out, especially if you are doing manual labour.

So the system was not able to sense it and that was a technology challenge they faced in implementing this solution. Then they came out with not just one fingerprint but make a combination, do a combination of all the five fingers, so that the probability of identification or correct identification improves and with that the system was implemented. So that is the case study. So what I am actually suggesting is in using

biometrics, there is the false positives and false negatives and you know that there is a trade-off between false positive and false negative. It is like controlling the entry into a system.

Suppose you know, many of you entered for an MBA program into DOMS through CAT score. CAT score is an important score for admission. Suppose the Institute decides or the department decides, we are going to make it very strict, we do not want bad students here at any cost, we only want good students. So 99.99 is the CAT score for entry into DOMS.

You see what happens, you are actually trying to ensure that the students who enter are really good. So you are trying to prevent, what do you call false positives. There should not be any bad students. So that is your major concern. There should not be any false positive.

So then what happens? CAT of course is a questionable, it is a, at the end of the day it is a measurement and there can be measurement error. You know somebody who could not do well on that day for the CAT examination but is actually a really good student, because the score is you know, not exactly matching. What about someone who has 99.8 ? That student may be better than somebody with 99.

9. These are all you know, you know not very actual measures of someone's aptitude for management and therefore it results in false negatives. False positives is strictly controlled but then it actually increases. False positive goes down, false negative goes up. Suppose you relax it, okay.

So this is not good. So you actually relax it, you say 80% is fine for admission, okay. Basically your false negatives will now go down. You will not have students rejected. You are actually, control the rejection. It is like type 1 and type 2, you know in hypothesis testing.

So the false negatives goes down but the false positives go up, so you can see that trade-off. That is what is compared here, FAR and FRR. They stand for false acceptance rate and false rejection rate. When you increase FAR, your FRR actually is low; when FRR goes up, FAR goes down. So the optimal point is known as Crossover Error Rate, CER.

CER is the optimal point and that is what is specified. A CER is typically specified in biometric devices and one should be able to check what is that CER and is it a desirable CER ? Is it sufficiently low, is something needs to be checked and it has an implication for FAR or false positive and false negative and of course, you think through the problem in hand and decide whether this is an acceptable biometric device or not. So that is a brief

about evaluating biometrics and the property of biometrics, in terms of acceptance and rejection and the trade-off between the two and the concept of crossover error rate, which is the optimal point. The widely used biometrics today are the fingerprints, the retina, blood vessel pattern and iris. Iris is the random patterns of freckles, pits, striations, vasculature and coronas.

These are different attributes of iris. The iris has multiple attributes, this is a, combination of this becomes unique to an individual, okay. Watch the movie which I suggested, you will see the use and abuse of these biometrics. Well, we move from access control to firewalls, okay. So we are broadly discussing what are the technologies for cybersecurity from a protection point of view, for protection mechanism. So one is you know, you strictly control access, who can access the system, okay and make it really impossible for unauthorized users to access the system.

So biometrics actually increases that protection and other, which are widely, the other system which is widely used and which today, all of us are aware is the firewalls, basically to prevent unauthorized access to your data center or your servers, okay. So it is about, like building a fire, a wall which is burning around the classroom and you know, the enemy cannot actually enter in here, that is the metaphor here. But essentially what a firewall does is it provides access based on identity. For example, if someone from a particular IP address is trying to access a database server, okay. The firewall can decide whether that person can access the database server or not.

So the rules is built into or configured in the firewall, who can, which IP address cannot access a given system and if someone uses that IP address and try to access, the access will not be granted. So that is what a firewall does. It actually specifies who cannot, who can access or who cannot access, okay and who can access is all other than who cannot access configured in the firewall typically and there is also the concept of and this particular diagram illustrates what a DMZ, DMZ means. So in this particular diagram you can see there is a terminology known as trusted network. What is a trusted network? And then there is untrusted network, here.

A trusted network in firewall literature or in cybersecurity literature means your network, okay. That is your network, your internal assets, cyber assets, okay. This is internal or this is your data center. Typically you take it as your data center, okay consisting of different servers and applications that is running services for your organization, okay.

That is the trusted network. What is the untrusted network ? Any network that is external to the organization is untrusted, okay. Because it is external, you do not know, okay. So always go by you know, we do not trust it unless we know. So this is external. Now since

the external world is varied and you know there could be good and bad and ugly in the external world, you need to have some mechanisms in place to provide access to your trusted network and one method of that is to avoid direct access, okay.

You do not want any external agent to directly access your trusted network, to directly get into your trusted network. Suppose they want certain resource, certain data from your trusted network, that is not directly provided. A copy of your resource is available in a dematerialized, demilitarized zone, okay. Sorry it is not dematerialized - demilitarized, okay. I am sorry for the mispronunciation, demilitarized zone, DMZ.

So the DMZ is a replica of the trusted network. So the external agent is given access to the DMZ, not to the trusted network. So it actually builds a sort of proxy, okay. It is a proxy system that is a mediator between the external world or external systems and your trusted network, okay. So you are aware of proxy servers which we also use in our data center, essentially to insulate your trusted network from the external world.

That is what a proxy server do and this is another mechanism. Firewall is, of course an application where you configure who cannot access your system using firewall rules, okay. So it prevents access, okay. Now the third category of technologies used for protection, okay to ensure confidentiality, integrity and availability of your cyber resources is cryptography and cryptography is a technology basically to ensure that data or information is not accessed, is not used, not accessed okay. Here the access control is not, the access is not controlled, someone despite all the firewalls or all the biometric systems and all that you have put in place, somebody can still gain access to your system when data is moving from source to destination, okay. There is a flow of data, data in transmission, while data is being transmitted someone who is not supposed to access, okay the imposter or the evil, okay can still gain access.

Assume that somebody gains access, how can you still prevent that information is not leaked to that person? That technology is known as cryptography, okay. So in cryptography you do not control access .In cryptography you assume that somebody has access but still, well you made all the efforts but you do not understand what you got, okay. So that kind of a strategy is used in cryptography. So essentially in this, there is a person Bob and I would call Alice, who is his girlfriend possibly.

So Bob sends a secret message or confidential message, he want, he does not want anybody else to receive that message, right. Only Alice, probably Valentine's Day message. So but somebody is very curious. There is someone who is very jealous there, right. Yeah in this setting, there is a jealous guy, okay so who wants to actually see what, what Bob is sending to Alice and that is a problem.

That is something that should not happen, okay. So in cryptography, what you use, do is you encrypt. You encrypt the message or there is a message and there is an encrypted version of that message which, the encrypted version is not something that is legible or not something that can be understood, okay because it is different, you cannot see the message in it. You can only see some characters there but it does not make any sense to someone who accesses it, okay that is krypt, kryptos. Actually I think it is creek, means hidden writing, okay. So encryption is the process of hiding the information by encrypting it.

So cryptography there, of course evolved over several years in the world of cybersecurity and of course during the World War there was, you know the Germans used cryptography and it was broken by the British scientists, you know, you can. You have popular movies on that today. But this is something that is actually employed in the, in cybersecurity. All of us uses Whatsapp right, and we all feel confident to use Whatsapp to send a message. Bob to send a message to Alice because as soon as you start texting, there is a message from Whatsapp to you saying that all Whatsapp messages are end to end encrypted, end to end has a meaning, okay.

End to end means from the sender to the receiver. There is no one in between, it is encrypted, not even Whatsapp can read your message. That is what end to end. So there is no any, there is no other system as of now. We do not know what government will do in future. That is where the problem of power of technology or a symmetry of power of technology actually comes but as of now there are those messaging applications which provide end to end encryption.

So basically, there is a plain text or message, that is the original message and it is sent as a bit stream over a communication channel and the bit are grouped into blocks. It could be blocks of 8 bits or 16 bits and so on and each block is what gets encrypted. The blocks are encrypted and we will see some of the mechanisms or methods for encryption as we go. Cipher is the transformation of the individual components, the characters, bytes or bits of the plain text into an encrypted component so and the cipher text or cryptogram is that unintelligible encrypted message or encoded message.

To decipher means to decrypt. So you have an encrypted message but for someone at the other end, Whatsapp encrypts your message. When you send "Hi" and send it to someone, Whatsapp encrypts it but at the receiving end, the receiver should be able to read it as Hi, not as a, not as something else, not as an encrypted message. So it has to be deciphered or therefore there has to be decryption and you will see that decryption always involves use of a key. Key is the key to encryption, some of it is locked and someone should be

able to unlock it and you know decipher the message. So key is a very important concept in encryption and what I am discussing here or trying to present to you must be known to many of you.

because these are sort of common, this is common information that is available in any textbook on cybersecurity or information security. So there are two types of, broadly there are two types of encryption methods, the symmetric key encryption and the asymmetric key encryption. Symmetric key encryption and Asymmetric key encryption. So there are two ways to manage the key, you see that there is a key, a message is encrypted, so it is encrypted using a key. It is like locking your message and you put your message into a locker and hand it over to the recipient, it goes as something that is locked.

So the recipient should have a key to unlock it and then you see the message. So that is concept here. So now you can see symmetric key, in symmetric key encryption there is only one key, there is only one key, the key that you use to encrypt and the key that you use to decrypt, it is the same. The same key is used for encryption and the same key is used for reading. Now obviously you can see the trade-off, the plus side is, that makes it simple.

You have only one key to manage, there is no multiple key. But how do you manage that ? If Bob wants to send his message to Alice, he encrypted it but how will you inform Alice who is in some other place that this is the key I have used? The key has to be passed to the recipient. But if you assume that the network is unsecure, anybody can access the network, access cannot be completely controlled, that is assumption in encryption and if you send your key to the same unsecure network, the key can also be accessed and that makes the whole arrangement little, you know vulnerable and therefore key management is a challenge. You can see the key again passes through the same network and therefore that is a limitation of symmetric key encryption. And that is overcome in the asymmetric key encryption which is depicted in this diagram. In asymmetric key encryption, the asymmetry is in the key, the key that is used for encryption is different from the key that is used for decryption or for reading.

There are two keys here and typically known as public key and private key. There is a private key and public key. How do I illustrate this ? Here is Alice and what Alice does is, what Alice want Bob to often send messages to her. So Alice actually generates two keys. One is, Alice gives a key to Bob which is her public key, okay When you send your messages use this key to lock. When Bob uses Alice's public key, when Bob uses Alice's public key to lock the message or to encrypt the message, the message is encrypted and it goes to Alice.

Alice does not use the public key to open it. Public key cannot be used to open a encrypted message. You need another key which again resides with Alice. Alice has two keys, one is private key, other is public key. So Alice can use her private key to open that message. See here the advantage is the public key may go to the sender over the, you know unsecure network, that key is used for encryption, but public key cannot be used for decryption.

You cannot read the message using public key. The private key resides or stays with Alice and that makes the system secure, okay because you use two keys, public key for encryption, private key for decryption and that method is known as asymmetric key encryption. So it is like Alice has a master key you know, in when you travel by airplanes, you are supposed to lock your suitcases with a particular lock which can be opened by TSA, right. The TSA I get it is marked TSA so the master key is with the airport authorities, they can actually if they want open that, so it is like Alice has the master key. So in one sense and the public key can be used only for locking, not for unlocking that is the approach. It is not exactly the same, what I am giving as an example but it is a sort of two different type of keys that is used for encryption and decryption and on a lighter note, you can see Alice has distributed her public key, not only to Bob but to many others, okay.

So now we come to the third aspect of key management, which is the digital signature and certificates which are commonly used in in networks when messages are passed from one node to the other, for one sender to receivers. You often come across this term digital signature and digital certificates, okay. So what is the digital signature? Sometimes you see that, you know your system, your browser wants you, you know, this is not a secure site or this does not have a updated certificate. So this also pertain to the domain of encryption but here the asymmetric process is reversed. You see that in previous example, the sender has the public key and the recipient has the private key.

When you change that, the sender sends a message with his or her private key and the public key is used to open. That is the method used in digital signature and digital certificate. The purpose here is basically to prevent non, to ensure non repudiation, something called non repudiation. This is an important concept, especially in blockchains as well.

Somebody should not refuse that I send the message. There are certain contexts where this particular role is very important. Non repudiation is very important, okay. Suppose in a look at banks, suppose you sign a cheque, okay and give to someone for getting it monetized from a bank branch, you signed it. That person files a case saying that it is a signed document, it is a signed cheque and the, you refuse to accept that you signed it, that is repudiation.

So in banking systems, you know, this is something that blockchains ensure. You cannot refuse, if you have actually signed something. So non repudiation in business transactions is an important requirement, non repudiation. Indian government implemented certain e-governance projects very successfully, e-governance projects like the passport seva is one example and also another project that is implemented by the government is for mandatory filings by companies. Companies need to file certain documents like the annual reports.

All listed companies or all registered companies need to file that with the government. Now this if it is done manually, it is very inefficient. So Government of India decided to automate the system. So TCS was the IT company which developed the system for automatic filing of mandatory reports and then there was this problem of non repudiation. Suppose your company X and you are filing your mandatory documents to government and how can the government ensure that it is you who sent it and tomorrow you should not be denying that you sent it, and suppose you want to correct it or manipulate it etc, there should not be any provision once you send it.

It is you who send it and you cannot refuse, non repudiation. So that was actually done through another project of digital signature where each company was given a key to sign the document before it is sent to the government. So that digital signature project was actually implemented by many IT companies. Basically one of my students did a project on this with Satyam computers those days and Satyam was distributing the private keys through a dongle which actually they obtained from the government. So this third party or the IT vendor acted as a key manager for the government.

So the key implementation was done by the third party. Essentially the purpose you can see here is more than security of the information, along with the security of the information that is passed, the non repudiation. Someone should not refuse ownership of the document that is filed also was important. So that is a different context and you can see the other context, where the digital certificates are important. When you actually type the address of a particular site, you want to visit, say IIT Madras. The browser needs to ensure that you are actually accessing IIT Madras and not something else and all genuine, you know the organizations would try to have a digital certificate to, for your browser to verify that it is IIT Madras.

So they verify IIT Madras's digital certificate. So you can imagine that digital certificates are like signatures, signed by the company, managed by a third party. So your browser will access your digital set, the digital certificate of the site you are trying to access with that resource and verify. Well you are fine, there is a certificate stored somewhere which authenticates that site, that is known as digital certificate. So I will quickly take you through some of the common methods or some of the broad techniques for encryption

and then close this session, may be in another, less than 10 minutes, so that we have time to discuss the article.

Encryption technically in a generic sense have, can be implemented by three methods. Substitution, Transposition and XOR. This is technical. Some of you may be familiar with what is an XOR gate in digital circuits, Exclusive OR .

That is one type. Transposition is another type. Substitution cipher is a third type. Substitution, transposition and XOR are three methods used in encryption. This is described in your textbook as well. And talking about substitution, there can be mono alphabetic substitution, there can be poly alphabetic substitution. To illustrate that, the encryption methods, particularly using substitution is very old and it was used by Caesar in his communications with his commander and that is widely cited, when we talk about encryption.

If Caesar has to send a very secret message to a command, commander, you know there is no other channel. There is no digital channel. Those days you have to send a message to through someone, through a messenger. So the messenger should not be able to read that So Caesar would not write the message in, in a Latin or in a language that is commonly in circulation.

Then he would change it to something else. He will encrypt the message. So can you read what was said, What is Caesar communicating to his commander ? This is the message that Caesar would send to his commander. If it is written in English, well you have one minute, say when your letter is A instead of A, you will say B,C,D, instead of A, you will make it D. So you advance it by a number and that is known as Caesar's cipher. Meet me after the toga party, that is what that, that encrypted message actually communicates.

Now you can see the formula for that, right. It is p plus k and k is the number that you add. So here what is the value of k? m m n o p, so you add 3. So and then substitute your character with character after three positions, that is why it is called substitution. You substitute each character with a character in the alphabetical series based on a constant number, which is k. It is p plus k, of course you have a situation when the alphabetical series ends, then it actually routes back to the first number or the beginning.

So that is the, that is the use of mod 26, meaning it actually goes back to the first position. So this is Mono Alphabetic Substitution, in the sense it is the same rule that applies for all alphabets. The same rule that applies to all alphabets. You can have Poly Alphabetic Substitution, where for each alphabet, there can be a different rule. Then, so the key here is, well the key here is k, right.

Here there is a key for encryption which is k, once that key is known, Caesar is gone, right. If you, if the messenger knows the key, then he or she can read the message. This is Poly Alphabetic Substitution where for each character, there is a different substitution method. When it is A, which letter is to be substituted is determined by a key, there can be a key.

So here is a problem for you. Use IITM as the key, DOMS need to be encrypted, using poly alphabetic substitution. So what you do is as I said, for each letter there is a different rule, There is a different rule. So I go to D, D is to be encrypted. So where do I, what do I use? I yeah, so D becomes L. So instead of going through each of this I will, sorry you use the key to determine the substitutes.

That is known as a poly alphabetic substitution. Read your textbook more. They have more examples. Transposition is, you know that bit streams are transmitted in blocks, here it is blocks of 8, 8 bits and again substitution is by transposition. For each bit in the block, there is a different rule. So it is block wise transposition and each bit having a different rule for encryption. So that is known as transposition and therefore when you apply this particular rule or particular key to each block, the plain text gets transformed into the cipher text.

For each position you have to apply the rule or the key, the key is nothing but the rule for changing the positions. This is known as transposition. ' Exclusive OR' some of you may know the truth table of Exclusive OR, if you have learned, this in engineering.

Otherwise do not worry. Exclusive OR is represented like this. You have two inputs, X1 and X2 and this is your Y, whatever. So the X1 X2 Y. Y is the output. When both the values are the same, the output will be 0.

When they are different, the output becomes 1. When it is 1 0 again 1. When it becomes 1 1 again 0, that is Exclusive OR. Now you can see, how the encryption is done using Exclusive OR. A message blocks are this, for each bit you apply a key. So you can see that when it is 1 and 1 it becomes 0; 0 and 0 it is 0, 1 1 0, whenever there is a difference it becomes 1.

So that is the Exclusive OR. in encryption. So I am just outlining three broad techniques. It does not mean that encryption is so simple as what I am describing but to give you basic principles of encryption and maybe I would summarize this particular topic and some of the encryption standards in the next class and with that summary I will, so I will recall

today's discussion and summarize and close this in the next class. So I will close it here and we will listen to the presentation on active defense today.