LECTURE 16

Cryptography → Basically deals with encryption and decryption

~~Q Why is cryptography important~~?

Q Places where cryptography is used)

Ans → In key exchange protocol → If the key exchange is flawed btwn sender and receiver that means there is a problem with the encryption and decryption and the whole cryptographic System is in trouble.

→ In Message Integrity → when we hash the message [we use cryptographic algorithms to do the Hashing], used in Computing MAC [which is a hashed-key]

BUT THE CORE OF THE CRYPTOGRAPHIC SYSTEM IS ENCRYPTION AND DECRYPTION

→ Cryptography is also used in random number generation

Eg of random no generation by a computer

Cloudfare generates random numbers using LAVA LAMPS, these lava lamps keep changing at regular intervals, there are cameras which look at these lights (the lights keep changing randomly), by taking snapshots of these changing lights they generated numbers at the time the light kept changing

DIFFERENT TYPES OF ENCRYPTION

* Substitution Based system

Eg there is a word henry we will substitute the letter 'h' with 'x' and so on, Nowaday modern cipher systems do not purely run on substitution

* Transposition Based system

Eg: The letters in word henry wi simply be rearranged henry - ynreh

Modern ciphere use both substitution and transposition → eg → AES (mix of substitution and transposition)

Ceaser Cipher was 100% substitution

Rare fence cipher was 100% transposition

* (1 key system) of keys / Private key system / Secret key system / symmetric system

→ The key which we use to encrypt is the same key using which we decrypt

AES is an eg of this scheme.

* (2-keysystem) / Public key system / Assymetric key system

→ 1 key is used to encrypt and a different key is used to decrypt [i.e a key used for encryption can't be used for decryption]

Eg: RSA-~~key~~ system

BUT FOR USING TWO DIFFERENT KEYS FOR ENCRYPTION AND DECRYPTION

IT IS IMPORTANT THAT THESE KEYS BE MATHEMATICALLY CONNECTED

→ This mathematical connection is done by TRAPDOOR MECHANISM

→ In a trapdoor you can enter it easily but coming out of it is difficult that same logic is used by ~~trapdoor~~. public key encryption system [where one thing [i.e encryption] is made easier but the decryption is tough]

→ ANOTHER EG OF TRAPDOOR IS EXPONENTIATION VS FACTORIZATION WHERE $a^{b|c|}$ is easier to compute than breaking a large no into its factors

* 3 BLOCK CIPHER Encryption

→ we encrypt the message by chopping it into blocks and encrypting each Block, and then after that we connect the encrypted blocks together

Eg: AES

→ Stream Cipher

we encrypt Bit by Bit or Byte by byte.

eg: SALSA 20

Q WHAT ARE THE DIFFERENT TYPES OF CRYPTOGRAPHIC ATTACK?

① Cryptoanalysis → We analyse the cipher text and try to guess what was the original message [Eg:- you might have plain text - cipher text pairs which are encrypted using the same scheme on trying to attack the system we are trying to capture the ciphertext but we also have some plain text - cipher text pairs which are captured earlier this gives us more time to analyze and do the attack because now we are given the chance to see the message and its value after encryption] so the basic aim of this attack is to infer the key, because once we have the key we can compromise on a lot of message

DISADVANTAGE OF CRYPTOANALYSIS

→ It only guarantees that we can only read one particular message using the key, it does not guarantee that we will be able to read the next message

Types of cryptoanalysis attack

→ Statical analysis on bits

→ Try solving things using mathematical eqn

→ Information leaks on side channels

~~side channels attack~~

Q WHAT IS A SIDE CHANNEL AND HOW A CRYPTOGRAPHIC ATTACK TAKES PLACE THROUGH IT?

For eg when we are running an encryption in our laptop, the power consumption varies depending on whether a '1 bit' is going through a certain process or a '0 bit' is going through a certain process. So a Hacker can just look at the power consumption statistics and based on that carry out the attack

→ This is called a side-channel attack as the Hacker is not looking into the encryption dynamics itself, but they are only looking at the power consumption

* BROTE - FORCE ATTACK

Basically try out all the possibilities, that is if you want to figure out a particular encryption, you try using one key, then try using the next key and so on until you figure out the encryption.

Q HOW TO COUNTER BROTE FORCE?

Ans We Have to make sure that someone → trying to defeat this system makes the system such that a large no of attempts will be needed to defeat it. This is also called as keyspace [i.e super large space, someone trying out every key will take forever to brute force through it]

→ Slowing down generation; Some algorithms a

deliberately designed to slow down certain operations
For eg: someone logging into the system its ok if it takes them 1sec to type a password and for this password to get hashed and compared with the hashed passwords in the database but this gives the attacker a lot of time to access the password database [i.e it will just take him a 10th of a second to do the attack], so the attack will be 10 times faster

THERE ARE TWO TYPES OF SECURITY NOTIONS FOR CRYPTOGRAPHICSECURITY

* Unconditionally secure : A scheme is unconditionally secure if no matter how much time an attacker has, or no matter how much computation resources, the attacker has, He still can't break these resources
Eg: Onetimepad is the only unconditionally secure scheme in existence today

Areas where one time pad can be used:
where you are creating your own personal application that transmit messages

But onetimepad has a disadvantage that it can't be used always as it has very long keys, thus this makes it unfeasible

4 Computationally secure

A person can break the scheme, but it will take a very long time

Advantage

For eg: the info that is of value to me now won't be of use to me 50 years down the line

SO THE IDEA BEHIND THIS SCHEME I THAT THE AMOUNT OF TIME IT W TAKE ME TO BREAK THE MESSAGE, W EXCEED THE USEFUL TIME OF THE ME

/ AMOUNT OF RESOURCES NEEDED IS GREATER THAN THE VALUE O THE MESSAGE

~~Somost security~~ schemes are COMPUTATIONALLY SECURE TODAY

MODOALAR ARITHEMATIC IS THE BASE ~~OF~~ ALL ENCRYPTION ALGORITHMS TODAY

CAESER CIPHER

→ Basically a letter is substitued by another letter ~~[illegible]~~ [which is at a distance of 3 steps from it]

~~[illegible]~~

→ DISADVANTAGE

→ It is very easy to brute force

→ IT IS NOT NECESSARY YOU HAVE TO MOVE BY 3 STEPS ONLY, YOU CAN MOVE IT BY 4 steps or 5 steps etc.

Another version of ceaser cipher is-

Monoalphebetic cipher

Here a ~~random~~ letter is substitued by a random permutation [ie letter A can be substituted by any letter through ~~[illegible]~~ 26]

~~[illegible]~~