CRYPTOGRAPHY

BY ELEMENTAL X

UNDERSTANDING ENCRYPTION

WELL, THIS TOPIC IS ABOUT CRYPTOGRAPHY RIGHT? BUT WAIT WHAT'S "ENCRYPTION"?. IN SIMPLE WORDS "ENCRYPTION" IS THE BASIC APPLICATION OF CRYPTOGRAPHY, TURNING A DATA INTO UNREADABLE FORM IN ORDER TO ENSURE ITS CONFIDENTIALITY .

WHY CRYPTOGRAPHY?

Everyone loves privacy isn't it ? in this cyber world there are hundreds of chat applications , and millions of people using them producing tons of data in form of personal messages , files , pictures and what not . keeping all this in mind cryptography plays a keen role in safeguarding data and network security.

LET'S GET TO SOME FUNDAMENTALS OF CRYPTOGRAPHY :-

Plaintext

Key

Ciphertext

Symmetric Encryption

Asymmetric Encryption

PLAINTEXT

Plaintext can be referred as the words present in human readable form and which needs to be secured from hackers or any unwanted third party .

Example :-

Imagine you are “X” , you and “A” are very good friends you guys share your secrets as you both sit at the same bench in the class . But one you had to sit with “Y” and your friend “A” with “Z” , and now you need to share the secret “Party at seven” without letting your new bench partners knowing it . So here “ Party at 6” is the plaintext.

KEY

During the process of hiding messages or encryption a secret value is being used known as “Key” . This value changes the original human readable plaintext into Ciphertext. The term “Ciphertext” will be discussed at the next slide .

Example :-

Do you remember the example at the previous slide ? X has to send the message “party at 7” now he thought of a different idea to send the message to A without Y & Z being able to read that. He decided to encipher the plaintext with an increment of one. So for now he has a key = 1.

CIPHERTEXT

Ciphertext can be defined as the unreadable or encrypted form of text which has been enciphered using a secret value i.e. the key.

Example :-

Let's continue with the previous example where X had enciphered a message "party at seven" for A with the value of key 1 . So let's look at the enciphered message now "qbsuz bu tfwfo" as one can notice every alphabet has been incremented by one , so X passes the cipher text "qbsuz bu tfwfo" to A with a key "1" and as soon A receives the ciphertext he deciphers it using the key "1" and the process finally gets executed .

SYMMETRIC ENCRYPTION

Hope the previous examples were crystal clear , moving onto our next step , hands on symmetric encryption . Let's break this huge term into more simple words .

Symmetric encryption can be defined as the process of enciphering and deciphering data with a one single key . The sender and the receiver must share the private(secret) key in order to make this process a successful one .The secret key can be any specific letter or number as per the encoder.

Some examples of symmetric encryption are Classical Ciphers such as the Caesar Cipher & Vigenere Cipher. Let's simplify the term "Classical Cipher" at the further slides.

ASYMMETRIC ENCRYPTION

Asymmetric encryption can be defined as the kind of encryption where 2 keys are used i.e. one to encrypt the plaintext and other to decrypt.

“Public key” is the one referred as the key used to encrypt the plaintext.

“Private key” is the one referred as the key used to decrypt the ciphertext .

THE CAESAR CIPHER

A symmetric encryption based on simple substitution classical cipher which uses one single key to encrypt and decrypt the message .

Named after popular Roman Dictator Julius Caesar .

Working :- Each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

Example :- Let's assume you are one of the senior most military personnel at Caesar's court and a war has been waged by the enemy and you want to convey the message "defend the wall of east" to your soldiers without the enemy being notified . So now you take a key = 1 . Using it you increment every alphabet with the key and previous plaintext is now in a secured form i.e. (efgfoe uif fbtu xbmm pg uif dbtumf") and seems gibberish to the enemy . So you successfully encrypted the message.

THE CAESAR CIPHER

Mathematical Description :-

i) First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2, ... , 'z'=25. We can now represent the Caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k) \pmod{26}$$

ii) Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption function is :

$$e(x) = (x - k) \pmod{26}$$

THE VIGENERE CIPHER

Defination & Working :- A polyalphabetic substitution cipher quite similar to the Caesar cipher except the letters aren't shifted but rather by values defined by a key , a collection of letters that represent numbers based based on their position in the alphabet.

Example :-

Let's move with the previous example but in this situation we will be using Vigenere Cipher , so we need to secure the plaintext "defend the wall of east" using the key 'durk' the plaintext are shifted using the values {3,20,18,11} because D is three letters after A, U is 20 , R is 18, K is 11 , and this format of 3,20,18,11 shifts and repeats untill the entire plaintext is encrypted. The plaintext [defend the wall of east] would encrypt to [gywoqxkrhyrcwqrvoiwdkytkvnco].

UPCOMING..

Hope the topics were crystal clear to you .

In the upcoming series we will look into the topics:-

1. Why are Classical Substitution ciphers weak?
2. How do ciphers work ?
3. Attack models
4. Asymmetric Encryption .

Please mail your queries , questions at :- *community@sec.army*

We look forward to help you and enrich the community.

SECARMY

COMMUNITY

THANK YOU .

https://community.sec.army