CRYPTOGRAPHY 0X02

BY ELEMENTAL X

LET'S GET TO SOME OF THE NEW TOPICS :-

1. How do ciphers work?
2. WHY ARE CLASSICAL SUBSTITUTION ciphers WEAK ?
3. FURTHER ATTACK MODELS
4. ASYMMETRIC ENCRYPTION .

HOW DO CIPHERS WORK ?

Well you want to dive deep down the topic ‘cryptography’ isn’t it ? So let’s get familiar with the working of cipher a bit better way .As we are pretty familiar with the previous examples on Caesar Cipher and Vigenere cipher we can absolutely abstract out a basic idea regarding the working of these ciphers.

So, let’s understand the concepts individually :-

i) The Permutation

ii) The Mode of Operation

PERMUTATION

As , we had already encountered the topics 'Caesar' & 'Vigenere' Cipher these ciphers are kind of classical substitution ciphers as we can remember was mostly was in shift of alphabets , although the set of symbols can vary .

BUT WAIT? A cipher's substitution can't be any random substitution ! It must be a permutation which is proper rearrangement of letters 'A' to 'Z' such that each letter has a unique inverse .

Example :- Let's assume a substitution that transforms the letter {'P','Q', 'R','S'} respectively to {'R', 'P', 'S', 'Q'} is a permutation because each letter maps onto another single letter . But a substitution cipher that transforms {'P', 'Q', 'R', 'S'} to {'S' , 'P', 'P' , R'} is not a permutation , because both Q & R both map towards 'P' . With a permutation each letter has exactly one reverse .

BUT WAIT? Aren't we using encryption to turn our data into the most secure one ? But every permutation is not quite secure . Well let's see what are the criteria that make a cipher's permutation secure enough !

PERMUTATION

Well the three criteria which can be kept in mind and discussed are as follows :-

1. The permutation should be determined by the key :- As to keep the permutation secret as long as the key is secret. In the Vigenère cipher, if you don't know the key, you don't know which of the 26 permutations was used; hence, you can't easily decrypt.

2. Different keys should result in different permutations :- It becomes easier to decrypt without the key: if different keys result in identical permutations, that means there are fewer distinct keys than distinct permutations, and therefore fewer possibilities to try when decrypting without the key. In the Vigenère cipher, each letter from the key determines a substitution; there are 26 distinct letters, and as many distinct permutations.

PERMUTATION

3. The permutation should look random :- There should be no pattern in the ciphertext after performing a permutation, because patterns make a permutation predictable for an attacker, and therefore less secure. For example, the Vigenère cipher's substitution is pretty predictable: if you determine that A encrypts to 'F', you could conclude that the shift value is 5 and you would also know that 'B' encrypts to 'G', that 'C' encrypts to 'H', and so on. However, with a randomly chosen permutation, knowing that 'A' encrypts to F would only tell you that B does not encrypt to F.

MODE OF OPERATION

Hope the concept of permutation was crystal clear to you . So moving to our next key topic known as Mode Of Operation .

Basically mode of operation can be taken as the process where a cipher mitigates the exposure of duplicate letters in the plaintext by using different permutations for duplicate letters . The mode of the Vigenere cipher partially addresses this : if the key is ‘X’ letters long then X different permutations will be used for every X consecutive letters . But wait ? However this still can result in the patterns in the ciphertext because the Xth letter of the message uses the same permutation . That’s why frequency analysis works to break the Vigenere cipher , as we will see in the upcoming example .

MODE OF OPERATION

Well, examples are always helpful to grasp new concepts , so let's take an example . So assuming that we have a secure permutation that transforms {A to X}, {B to M} , and {N to L} and using "BANANA" as plaintext we get the ciphertext as "MXLXLX" where each occurrence of 'A' is replaced by an X . Using the same permutation for all the letters in a plaintext thus reveals any duplicate letters in a plaintext . By analyzing those duplicates one might surely not learn the entire message . In this example you don't need the key to guess that the plaintext has the same letter at the three 'X' positions and other at the two L positions . So simply if you know that the message is a fruit's name you can very easily determine its BANANA rather than CHERRY or another six-letter fruit.

SUMMARY ON WORKING OF CIPHER

So finally we grasped the key concepts of how does a cipher really works .Basically to build a safe form of cipher which is after all our primary goal we need to combine a secure permutations with a secure mode . Ideally this combination prevents attackers from learning anything about a message other than its length .

WHY ARE CLASSICAL CIPHERS INSECURE?

Well we had encountered the use of Classical Ciphers at the previous slides .But are those fully "Secure" , because making the data is our primary goal . Let's study we should one shift from Classical Cipher to Asymmetric Encryption . We will have a glimpse of Asymmetric Encryption in out further slides .

Let's get to the point "WHY ARE CLASSICAL CIPHERS INSECURE?". These ciphers are doomed to be insecure because they lack the computational power of a computer and are easily broken by simple computer programs . Let's study them deeply what makes them insecure in the further slides .

WHY ARE CLASSICAL CIPHERS INSECURE?

Mathematical Description :-

Remember that a cipher’s permutation should look random in order to be secure . After all the best way to look random is to “be” random i.e. to select every permutation randomly from the set of all permutations .

And there are many permutations to choose from. In the case of the 26-letter English alphabet, there are approximately 2 88 permutations:
26! = 403291461126605635584000000 ≈ 2 88
Here, the exclamation point (!) is the factorial symbol, defined as follows:

$$n! = n \times (n - 1) \times (n - 2) \times . . . \times 3 \times 2$$

WHY ARE CLASSICAL CIPHERS INSECURE?

(To see why we end up with this number, count the permutations as
lists of reordered letters: there are 26 choices for the first possible letter,
Then 25 possibilities for the second, 24 for the third, and so on.) This
number is huge: it's of the same order of magnitude as the number of
atoms in the human body. But classical ciphers can only use a small
fraction of those permutations—namely, those that need only simple
operations (such as shifts) and that have a short description (like a short
algorithm or a small look-up table). The problem is that a secure
permutation can't accommodate both of these limitations.
You can get secure permutations using simple operations by picking a random permutation,
representing it as a table of 25 letters (enough to
represent a permutation of 26 letters, with the 26th one missing), and
applying it by looking up letters in this table. But then you wouldn't have a short description .
For example it would take 250 letters used in the Vigenere Cipher .

CASE STUDY : ONE-TIME PAD

Essentially classical ciphers cannot be secure unless it comes with a huge key , but encrypting with a huge key is useless & impractical. However the one time pad is among an exception which guarantees extreme level of secrecy although the attacker has unlimited computing power , it’s impossible to learn anything about the plaintext except for its length . In the upcoming slides we will read this exceptional Classical Cipher .

FURTHER ATTACK MODELS

Let's get a brief idea on attack models of cryptography . Basically an attack model is a set of assumptions about how attackers might interact with a cipher and what they can and can't do . The goals of an attack model are as follows:-

>To set requirements for cryptographers who design ciphers , so that they know what attackers and what kinds of attacks to protect against .
>To give guidelines to users about whether a cipher will be safe to use in their environment .
>To provide clues for cryptanalysts who attempt to break ciphers , so they know whether a given attack is valid . An attack is only valid if it's doable in the model considered .
We will discuss the detailed list of attack models like "Kerchkhoff's Principle" , Black-Models Models , Gray-Box Models and all .

ASYMMETRIC ENCRYPTION

So , in the previous slides we already had an brief idea of symmetric encryptions , attack models , how does ciphers works and lot more . So let's get an introductory level idea of what "Asymmetric encryption" is ? .So basically in a asymmetric encryption there are 2 keys : one to encrypt (KNOWN AS PUBLIC KEY) and other to decrypt (KNOWN AS PRIVATE KEY) .
Working :-
The public key can be computed from the private key , but obviously the private key can't be computed from the public key .

So, Basically symmetric and asymmetric encryption are two main types of encryption , and they are usually combined to build secure communication systems .
In the upcoming slides we will be present with more real life examples of Asymmetric Encryption and more encryption techniques .

UPCOMING ...

1. KNOWING ATTACK MODELS A BETTER WAY & SECURITY GOALS .
2. A BETTER INTERACTION WITH SOME MORE TYPES OF ASYMMETRIC ENCRYPTION TECHNIQUES .
3. HOW CAN THINGS GO WRONG ?
4.BLOCK CIPHERS
5.STREAM CIPHERS .

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