Cryptography

Created	@November 7, 2022 7:53 PM
Tags	

Goal of the exercise:

Go through the standard and necessary problem solving steps so that we could hash and decrypt cypher text. Executing a brute force attack.

Steps:

What are we looking for?

How are we going to search the necessary data?

How to confirm if data “makes sense”?

What do we need?

Symmetric or asymmetric?

Do we use algorithm analysis or brute force?

Faster ways of doing the brute force attack?

What do we know of the characteristics if any of the key that is used?

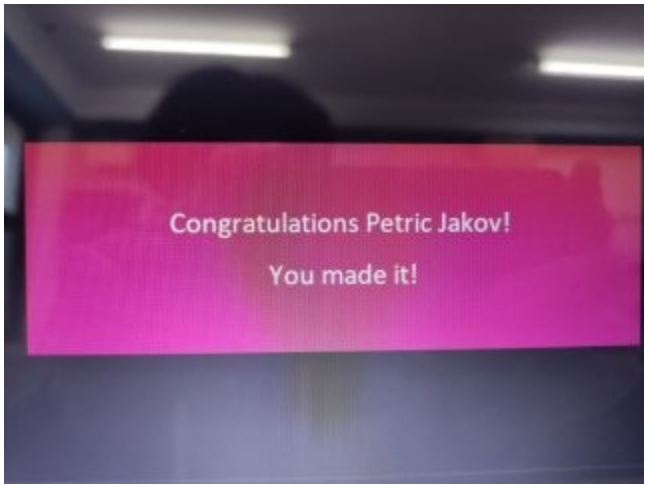
What is the entropy?

Do we know in what format the plaintext is stored in?

Implementation:

First, since we know that the file is in the PNG format, we look up the specification standard for PNG so that we can orient ourselves to what we are looking for in the decrypted text. As it would not be necessary to decrypt the whole text and check, we know by the specification that PNG has a header that appears at the front if the file is read as in binary. Having read the specification standard, we determine how many bites

we should take and decrypt and see if the searched for tag has appears in those selected few bites. After we confirm the “sense” of the plain text, we store it in a file so that we can see ourselves if we hit the mark. It takes a long time without parallel processing.



Takeaway:

Most important to properly divide the complex problem into a number of easily solvable sub-problems and combine them for the intended effect.