coding temple

Module 5 Project

Title: Analyze and Compare Cryptographic Algorithms using CyberChef

Objective

To understand the workings of different cryptographic algorithms, analyze their strengths and weaknesses, and gain practical experience using CyberChef.

Scenario:

In this project, students will use CyberChef, an online tool for encryption and decryption tasks, to explore different cryptographic algorithms. They will encrypt and decrypt text using symmetric, asymmetric, and hashing algorithms, then analyze and compare their effectiveness.

Your Role:

1. Choose Algorithms: Select one algorithm from each category – symmetric (like AES or DES), asymmetric (like RSA), and a hash function (like SHA256 or MD5).
2. Get Familiar with CyberChef: Navigate to CyberChef's website (https://gchq.github.io/CyberChef/). Familiarize yourself with the interface and different operations provided by CyberChef. You can find different cryptographic operations under the 'Encryption and Encoding' category.

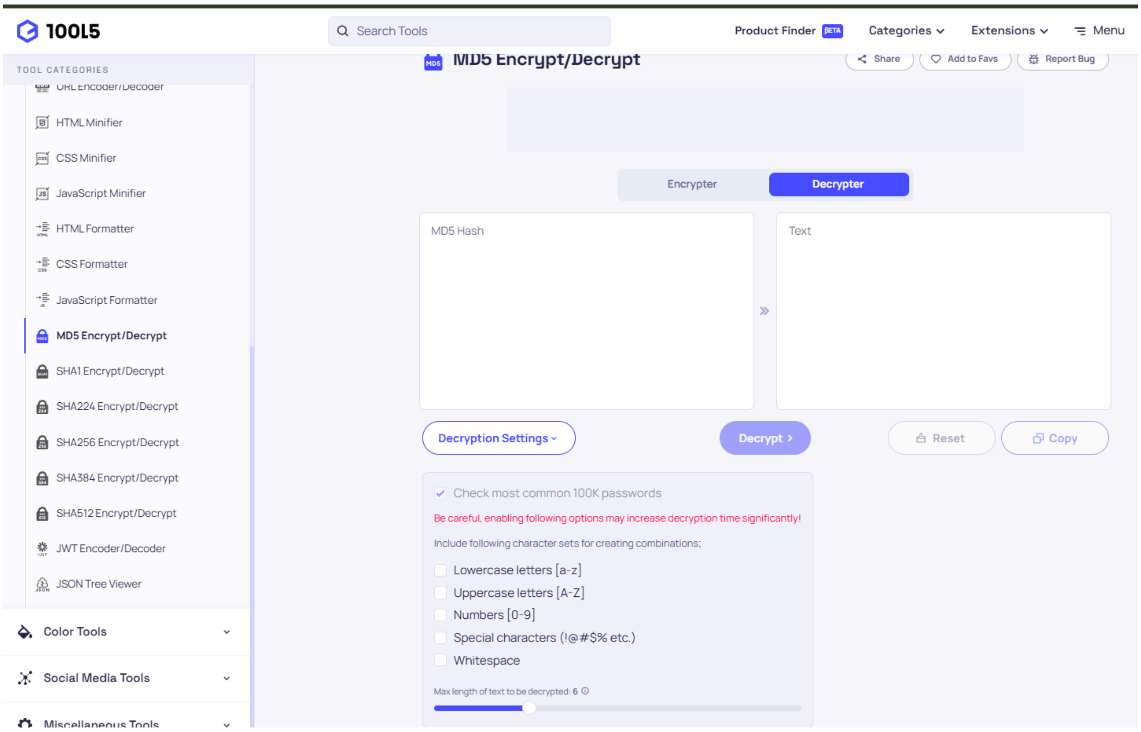
3. Encrypt and Decrypt: Write a piece of text (plaintext). Use your chosen symmetric and asymmetric encryption algorithms to encrypt this text in CyberChef. Decrypt the ciphertext back to plaintext and ensure it matches your original text.
4. Hashing: Use your chosen hashing algorithm to create a hash of your plaintext. Understand that hashing is a one-way function, i.e., you cannot retrieve the original data from the hash.
5. Analyze and Compare: Analyze the strength and weaknesses of each algorithm based on factors such as key length, speed, security, and ease of use. Record your observations.
6. Report: Prepare a report detailing the steps you took in this project, including the algorithms you used, the process of encryption, decryption, and hashing, and your analysis of each algorithm.

BONUS

Use this link below to solve these hashes:

https://10015.io/tools/md5-encrypt-decrypt

Hint: Search for the hashing algorithm in the search bar and try to decrypt it using the Decrypter. You can also use Decrypter settings to fine-tune the decryption process



☑ Check most common 100K passwords

Be careful, enabling following options may increase decryption time significantly!

Include following character sets for creating combinations:

☐ Lowercase letters [a-z]
☐ Uppercase letters [A-Z]
☐ Numbers [0-9]
☐ Special characters (!@#$% etc.)
☐ Whitespace

Max length of text to be decrypted: 6

Sample Hashes to Attempts:

MD5 hash: 801338b11e9d13070dc726cbc67ab160

This is a standard MD5 hash that produces 32 bytes long hash.

Hint: rumor has it that this is a 5-character password of alphabets, digits, and the common punctuations

SHA256 hash:

5f22db794e7a7c5219980eb2a492f577804179e30be20c3db28623ed63f19c90

This is a standard SHA256 hash that produces 64 bytes long hash.

Hint: rumor has it that this is a 7 character password, composed of lowercase letters (a-z), uppercase letters (A-Z), and digits (0-9).

bcrypt hash:

$2b$12$O64GAcboleHTqpDeCMwQJe7IwT.6AE1ycBJZGKQGt5EZJv1MoVCt

*This is a standard bcrypt hash (note that bcrypt hashes include a salt, so there are many possible outputs).

Hint: rumor has it that this is a commonly used password.

Submission:

THIS WRITEUP SHOULD DEMONSTRATE THAT YOU HAVE A SOLID UNDERSTANDING OF SYMMETRIC, ASYMMETRIC, and HASHING. You will need to be very comfortable with these topics for your final presentation and for your career!

Upload the completed report in pdf format in Google Classroom.