**CSS Experiment 05: Implement and design a Hashing Algorithm**

**Learning Objective:** Implement and design a Hashing Algorithm.

**Tools: PyCharm**

**Theory:**

Introduction:

MD4 (Message Digest 4) is a hashing algorithm developed by Ronald Rivest in 1990. It is a one-way hash function that produces a fixed-length output (128-bit) from an arbitrary-length input message. The MD4 algorithm was widely used for various security applications, such as digital signatures, password storage, and message authentication. However, due to several vulnerabilities found in MD4, it is no longer considered secure and has been deprecated in favour of more secure hashing algorithms, such as SHA-2 and SHA-3.

Algorithm Description:

The MD4 algorithm takes an input message of any length and produces a 128-bit hash value. The input message is first padded to a multiple of 512 bits, following a specific padding scheme. The padding consists of a single 1 bit followed by a sequence of zeros, such that the length of the padded message is congruent to 448 modulo 512. Then, the length of the original message (in bits) is appended to the padded message as a 64-bit representation.

The MD4 algorithm operates on the padded message in 512-bit blocks. For each block, it uses a set of fixed initialization constants and a set of four round functions to update the intermediate hash value. Each round function takes as input the current hash value and a set of four 32-bit words derived from the input block. The round functions involve bit-wise logical operations, such as bitwise AND, OR, XOR, and left rotation.

The MD4 algorithm performs 3 rounds of operations on each block, with each round applying 16 operations. At the end of the last block, the final hash value is obtained by concatenating the 4 32-bit words of the intermediate hash value.

Vulnerabilities:

MD4 has several vulnerabilities that make it insecure for modern security applications. One of the most significant vulnerabilities is the collision attack, which allows an attacker to find two different messages that produce the same hash value. The first collision attack on MD4 was published in 2004, and since then, several more attacks have been discovered.

The collision attacks on MD4 exploit the weakness in the round functions and the message padding scheme. By manipulating the input message in a specific way, an attacker can create two different messages that produce the same hash value. This can be used to create fraudulent certificates, forge digital signatures, or bypass password authentication systems.

Code:

Output:

Conclusion:

In summary, MD4 is a widely-used hashing algorithm that has been deprecated due to its security vulnerabilities. The MD4 algorithm operates on 512-bit blocks and uses a set of fixed initialization constants and four round functions to update the intermediate hash value. MD4 is vulnerable to collision attacks, which allow an attacker to find two different messages that produce the same hash value. Therefore, it is no longer considered secure for modern security applications, and more secure hashing algorithms, such as SHA-2 and SHA-3, should be used instead.

**Code:**

**Output:**

**Conclusion:** After performing the experiment I was able to implement Transposition Cipher.

For Faculty Use

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Correction Parameters** | **Formative Assessment [40%]** | **Timely completion of Practical [ 40%]** | **Attendance / Learning Attitude [20%]** | **Total** |
| **Marks Obtained** |  |  |  |  |