Assignment No - 05 Date : / /20

Aim - calculate the message digest of a text using the MD5 algorithm in Java

theory.

1] The MD5 hashing algorithm is a one-way cryptographic fun^n that accepts a message of any length as input and returns as output

2] A fixed-length diagest value to be used for authenticating the original message. The MD5 hash fun^n was originally designed for use a secure cryptographic hash algorithm for authentically digital signatures. MD5 is used for storing securing password in database server MD5 generated message diagest of 128 bits

3]- MD5 is the third message -diagest algorithm Rivest created MD2, MD4, and MD5 have similar structures but MD2 was optimized for 8-bit machines in comparison with the two later algorithms which are designed for 32-bit machines.

4] The MD5 algorithm is an extension of MD4 which the critical review found to be fast but potentially in secure.

5] In comparison MD5 is not quite as fast as the MD4 algorithm but offered much more assurance of data security.

6] The MD5 message-digest hasing algorithm processes data in 512-bit strings broken down into 16 words composed of 32 bits each. the output from MD5 is a 128-bit message digest value.

7] The digest size is always 128 bits and thanks to hashing function guidelines a minor change in the input string generate a drastically different digest.

8] This is essential to prevent similar has generation as much as possible also known as a hash collision.

9] The MD5 hash funⁿ was originally designed for use as a secure cryptographic hash algorithm for authenticating digital singatures.

10] MD5 is a cryptographic has algorithm used to generate a 128-bit digest from a string of any length It represents the digest as 32-digit hexadesimal numbers.

Advantages of MD5 Algorithm

1] It's easier to compare and store smaller hashes using MD5 Algorithm that it is to store a large variable - length text

2] By using MD5 passwords are stored in 128 bit format.

3] A message digest can easily be created from an original message using MD5.

4] A relatively low memory footprint is necessary to integrate multiple services into the same frame work without a CPU overhead

5] Disadvantages of MD5

① when compared to other algorithm like the SHA algorithm MD5 is comparatively slow

② It is possible to construct the same hash funⁿ for two distinct inputs using MD5.

③ MD5 is less secure when compared to the SHA algorithm.

Algorithm -

Step 1 - Create a message digest object.

Step 2 - pass Data to the Created message digest object.

Step 3 - Generate the message digest.

Conclusion -

We learned how to implement MD5 Algorithm.

C