Anish Sachdeva
DTU/2K16/MC/13

Class Test

Date

Page No.

Cryptography & Network Security
MC-407
Class Test - III

Q. Explain MD5 Hash Function

Message Digest Algorithm (MD5) is cryptographic Hash algorithm that can be used to create 128-bit string value from an arbitrary length string.

Although there have insecurities identified with MD5, it is still widely used. MD5 is most commonly used to verify the integrity of files.

However it is also used in other security protocols and applications such as SSH, SSL and IPSec. Some applications strengthen the MD5 algorithm by adding a salt value to the plaintext or by applying the hash function multiple times.

An MD5 hash is typically expressed as a 32 bit hexadecimal number. MD5 operates on 32-bit words. Let M be the message to be hashed. The message M is padded so that its length (in bits) is equal to 448 modulo 512 that is the padded message is 64 bits less than a multiple of 512. The padding consists of a single bit, followed by enough zeroes to pad the message to the required length. Padding is always used, even if the length of M happens to equal 448 mod 512.

Class Fun

Date | Page No.

As a result, there is at least one bit of padding and at most 512 bits of padding. Then the length (in bits) of the message (before padding) is appended as a 64-bit block.

The padded message is a multiple of 512 bits and, therefore, it is also a multiple of 32 bits. Let M be the message and N the number of 32-bit words in the padded message. Due to padding, N is a multiple of 16.