confidentiality → read msg

Intigrity → check the alteration and modification in msg.

PAGE NO.:
DATE

* Message Integrity & Authentication

1) Message Integrity
   - Message Digest 5 (MD5)
   - Secure Hash Algorithm (SHA)
2) Message Authentication
3) Digital signature.

① → * Message Integrity :-

① Encryption and decryption provides security, or confidentiality but not Integrity.

A ⟶ B

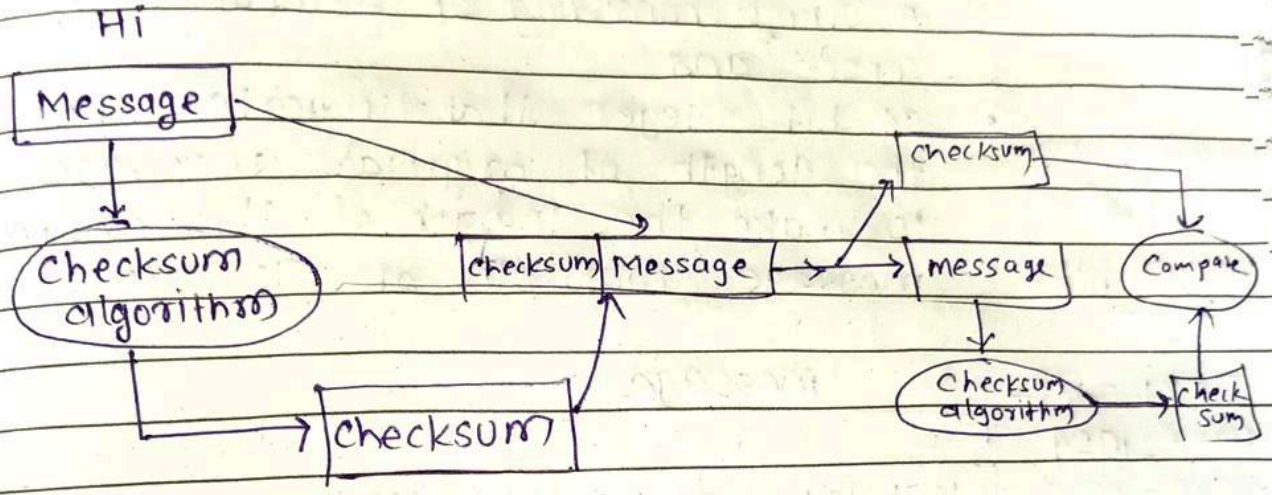
② The integrity algorithms enable the receiver to check whether the message send by the sender has been altered in any manner during its transit.

③ In these algorithms, a cryptographic integrity Checksum is calculated and attached to the message by the sender.

④ The receiver recalculates the checksum at its end compares it with received Checksum. if they are same message is intact.

Example of checksum algorithms are :

① message Digest 5 (MD5)
② Secure Hash Algorithm (SHA)



Hi
0589 → msg is not altered

Hello → message
0598 → altered.

Message Digest 5 :- (MD5)

① There are a no. of popular message digest algorithm known as MD_n for various values of n.

② MD5 is the most popular and is fifth in a series of message digests design by Ronald Rivest

This algorithm operates on message 512 bits at a time.
Message not multiple of 512 bits are padded with :

① A string consisting of 1 followed by zeroes and

② 64-bit integer that indicates the the length of original message, to make the length of the composite message multiples of 512 bits.

original message | padding

1000 bits

512 x 1 = 512
512 x 2 = 1024
512 x 3 = 1536

1536
− 64
1472

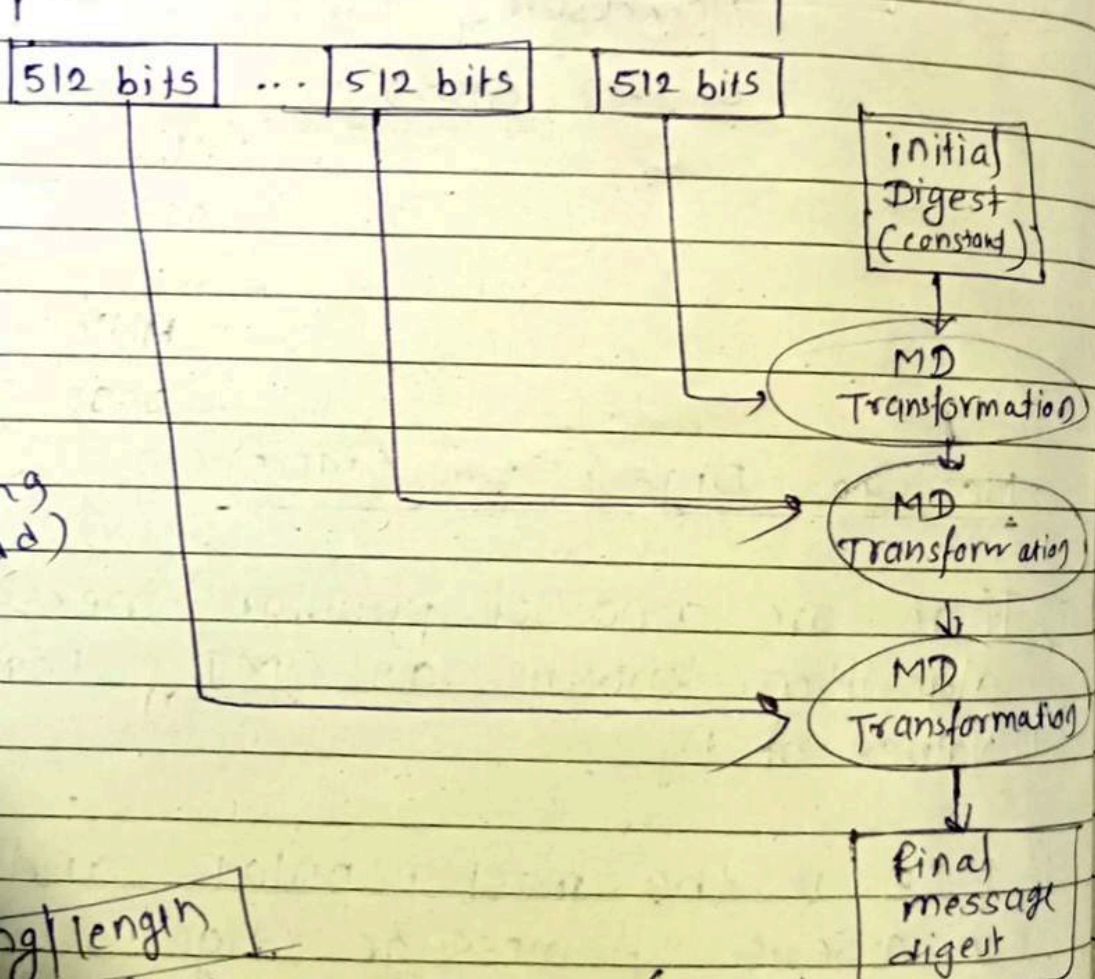
1000 (padding add)
+ 472
1472

64 bit less than exact multiple of 512

original msg | padding | length

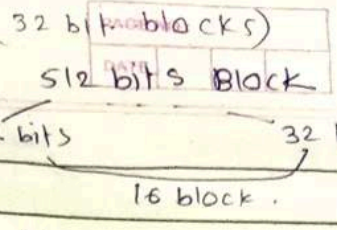
(ii) append original length bet. padding (modulo 64)
1000 | Length mod 2^{64}

(iii) divide it in 512 bit blocks.



Message Digest 5 (MD5)

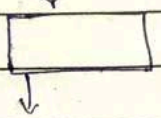
process Blocks
→ copy four chaining variables into corresponding variables.
{A = a, B = b, C = c, D = d}
→ divide 512 bit block into 16 (32 bit blocks)
→ four rounds



MD5 Algorithm

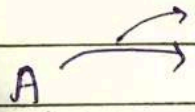
1. cryptographic hash function algorithm
2. by Ronald Rivest in 1992
3. a series of message digest
4. Digest size — 128 bit.
5. block size - 512 bit
6. No. of Rounds — 4

i/p → 1024



128 bit

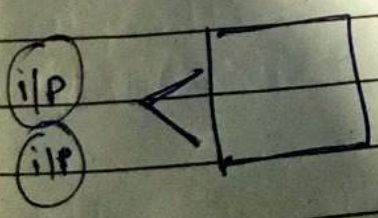
purpose → integrity check



Applications / Uses of MD5

1. Secure passwords of users Hello → 1a954
2. in 128 bit format
3. to verify data integrity
4. used for file authentication

Weakness / Disadvantage



→ digest.
same.

even a small change in msg will result in a diff. hash value