①

MD5	SHA 1
1) Message digest 5	1) Secure Hash Algorithm
2) 128 bits message lengths	2) 160 bits message lengths
3) Faster compared to SHA1	3) Slower
4) Simple	4) Complex
5) To make out the initial message the aggressor would want 2^{128} operations	5) 2^{160} operations

(2)

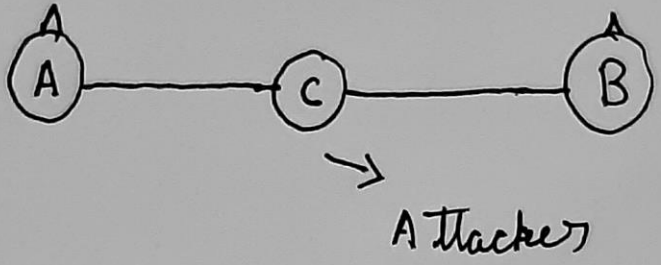
AS and TGS are the two main parts of a Key distribution center (KDC).

The AS (Authentication Service) is used the authenticate the client.

The TGS (Ticket Granting Service) provides tickets TGTs to the client systems. TGT contains the client ID, the client network address, ticket validity period and ticket granting server session key.

(3) Man in the middle is an attack where the attacker secretly relays and possibly alters the communications b/w two parties.

eg:



1) (A:) Give me your key → (C) → (B)

2) (A) ← C's key (C) B's key ← (B)

3) (A) —Encrypted message with C's key→ (C) —altered message encrypted with B's key→ (B)

B Thinks it is a message from A.

~~from~~