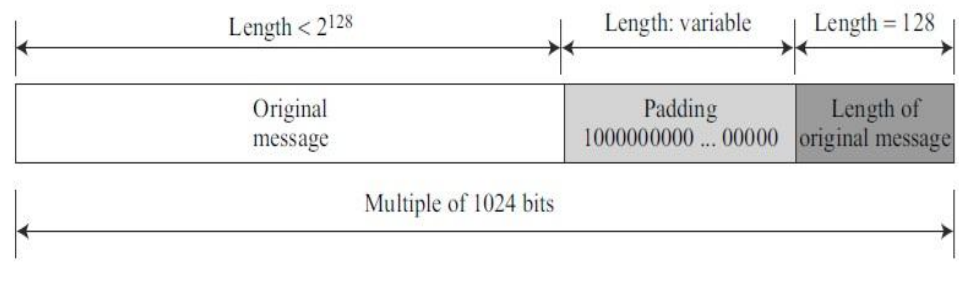


Tutorial – XIII (Hash Algorithm)

1. If hash function has an output length of 80 bits, we need to check 2^{80} messages for finding second pre-image. Prove that attacker needs only about 2^{40} messages due to the birthday attack. Show the necessary steps to illustrate birthday attack.
2. How much time is required to find the second pre-image for a hash function with a 64-bit digest? Assume that an attacker can perform 2^{20} (one million) tests per second.
3. SHA-512 creates a digest of 512 bits from a multiple-block message. Each block is 1024 bits in length. The length of the padding field can be calculated as follows. Let $|M|$ be the length of the original message and $|P|$ be the length of the padding field.

$$(|M| + |P| + 128) = 0 \bmod 1024 \quad \rightarrow \quad |P| = (-|M| - 128) \bmod 1024$$



- (i) What is the number of padding bits if the length of the original message is 2590 bits?
- (ii) Do we need padding if the length of the original message is already a multiple of 1024 bits?

Note:

- SHA-512 insists that the length of the original message be less than 2^{128} bits. This means that if the length of a message is equal to or greater than 2^{128} it will not be processed by SHA-512. This is not usually a problem because 2^{128} bits is probably larger than the total storage capacity of any system.
- The length field defines the length of the original message before adding the length field or the padding.
- Before the message digest can be created, SHA-512 requires the addition of a 128-bit unsigned-integer length field to the message that defines the length of the message in bits.