Rebecca Dias
19/8/2022
TE CMPNA2

CSS

IA-T 1

Q3) b) Message authentication

① Message Authentication is a mechanism or service used to verify the integrity of a message.

② It assures that data received are exactly as sent (i.e no modification, Insertion, deletion or replay)

③ In many cases, there is a requirement that the authentication mechanism Assures that the purported identity of the sender is valid.

HMAC

① HMAC stands for HASH message Authentication code

② It is a specific technique for calculating a message authentication code (MAC) involving a combination of cryptographic hash functions and a secret key eryptography.

③ Design objectives

a) To use, without modifications, available hash functions

b) To allow for easy replaceability of the embedded hash function in case faster

c) or more secure hash function are found or required

d) To preserve the original performance of the hash function without incurring

Rebecca Pias
182027/19
TECMPNA2

CSS

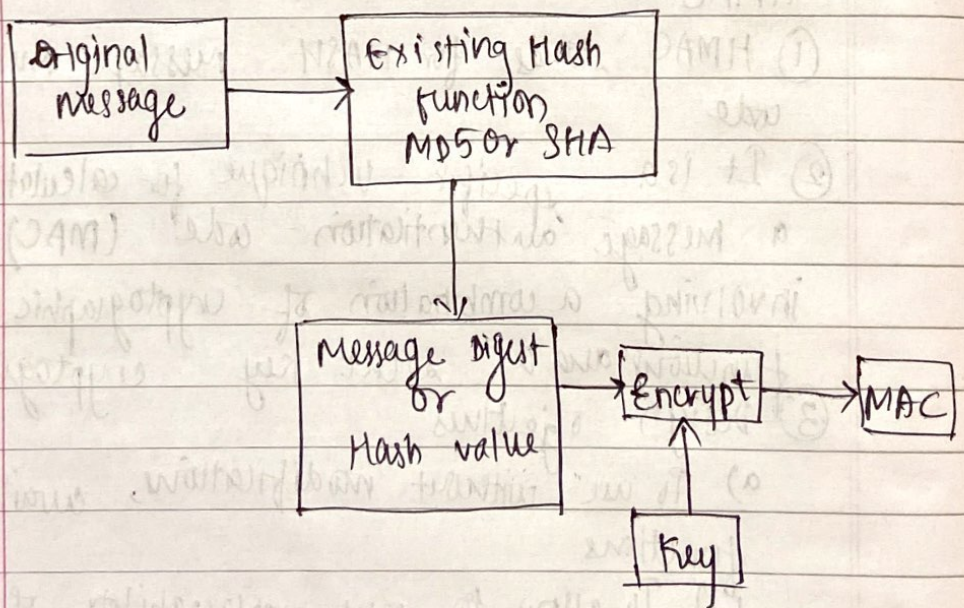
significant degradation

e) To use and handle keys in a simple way

f) To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions about the embedded hash function.

HMAC can be expressed as

$$HMAC(K, M) = H[(K^+ \oplus opad) || H[(K^+ \oplus ipad) || M]]$$



Rebecca Dias
182027/19
TE CMPN A2

CSS