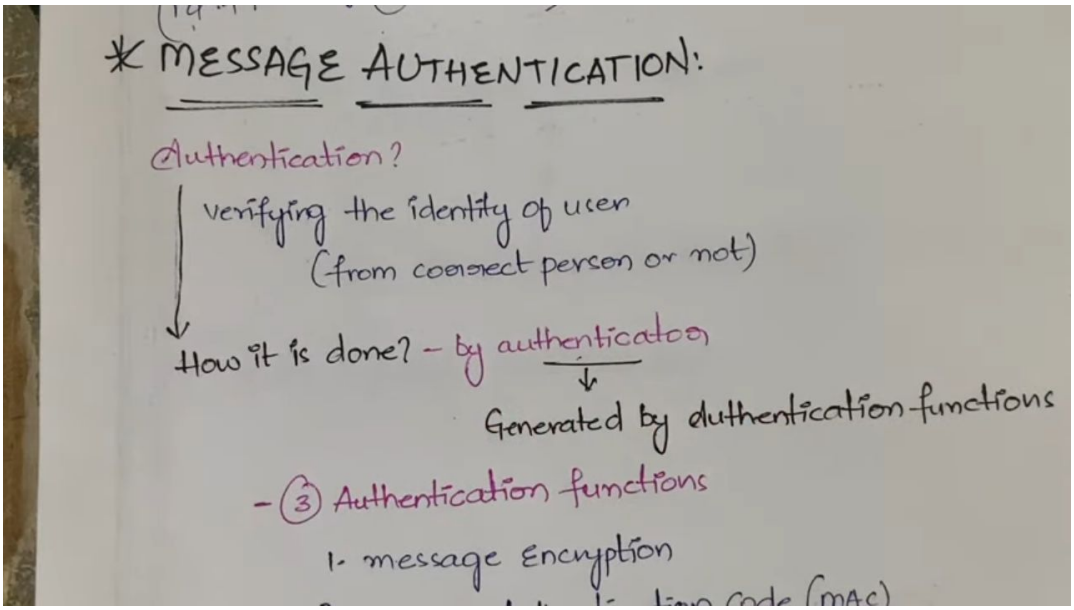
View, add and edit your notes in the app

#33 Message Authentication & Authentication Functions in Cryptography |CNS

Generated on December 19, 2023

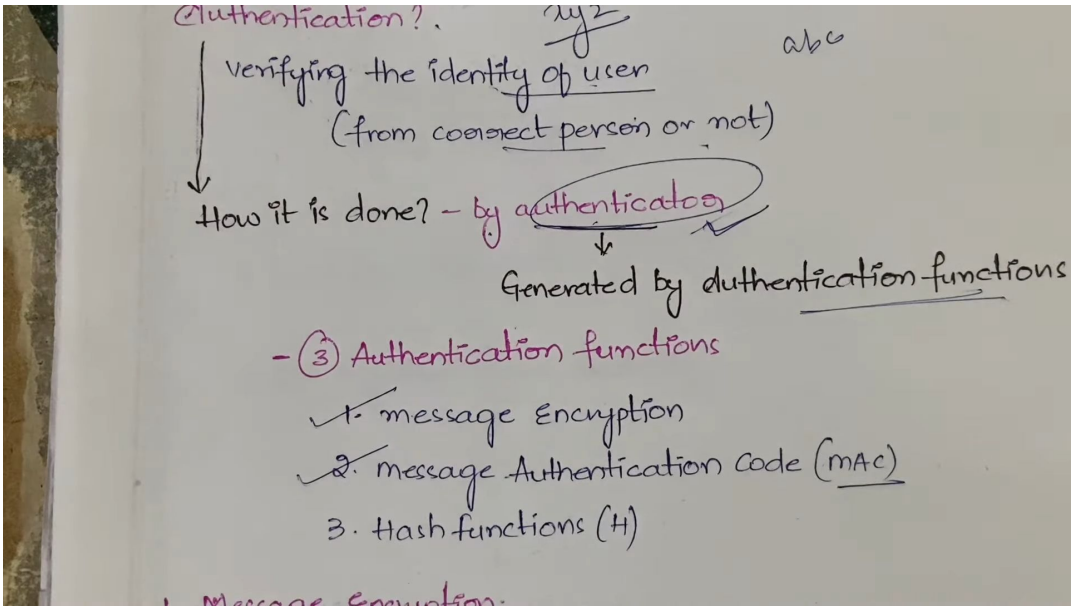
Summary

Notes	Screenshots	Bookmarks
0	5	0

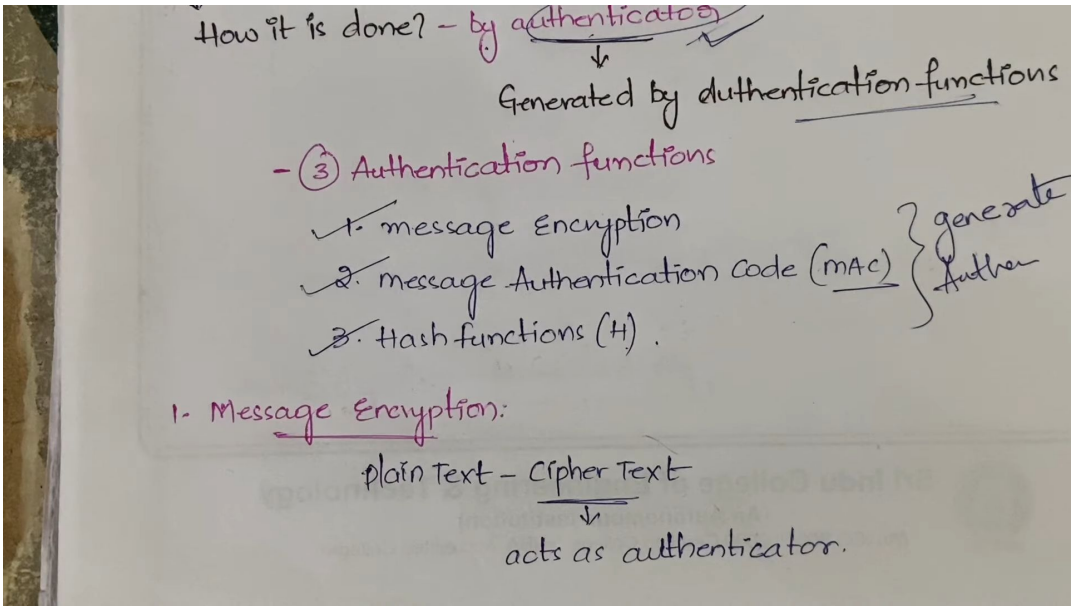


Researchers have discovered a new species of bird in the Amazon rainforest, known as the reter.

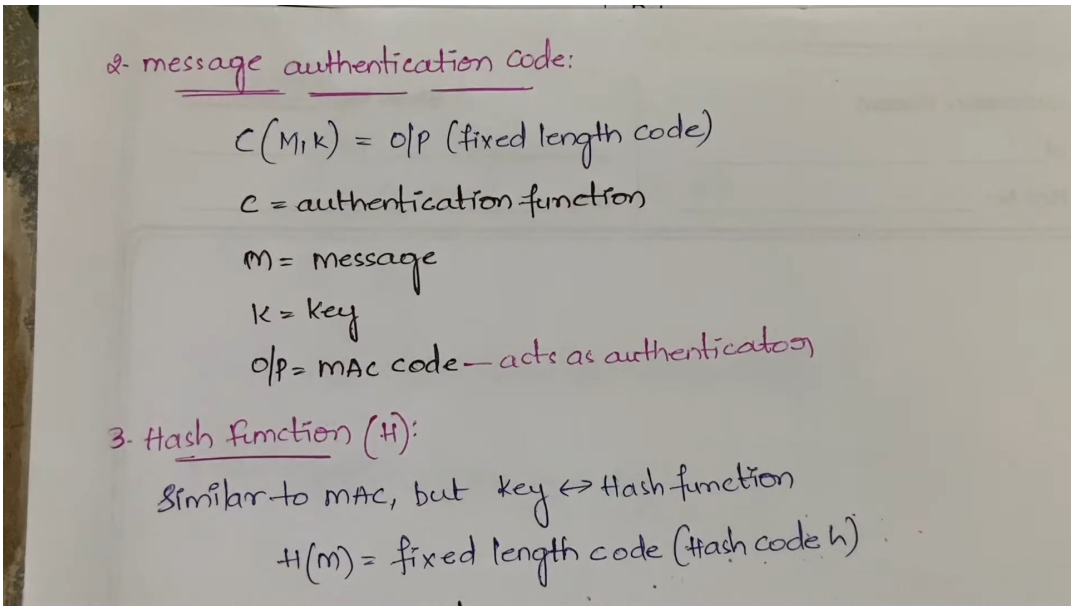
0:10


Authentication?
xyz
abc
verifying the identity of user
(from correct person or not)
How it is done? - by authenticator
Generated by authentication functions
- (3) Authentication functions
1. message Encryption
2. message Authentication code (MAC)
3. Hash functions (H)

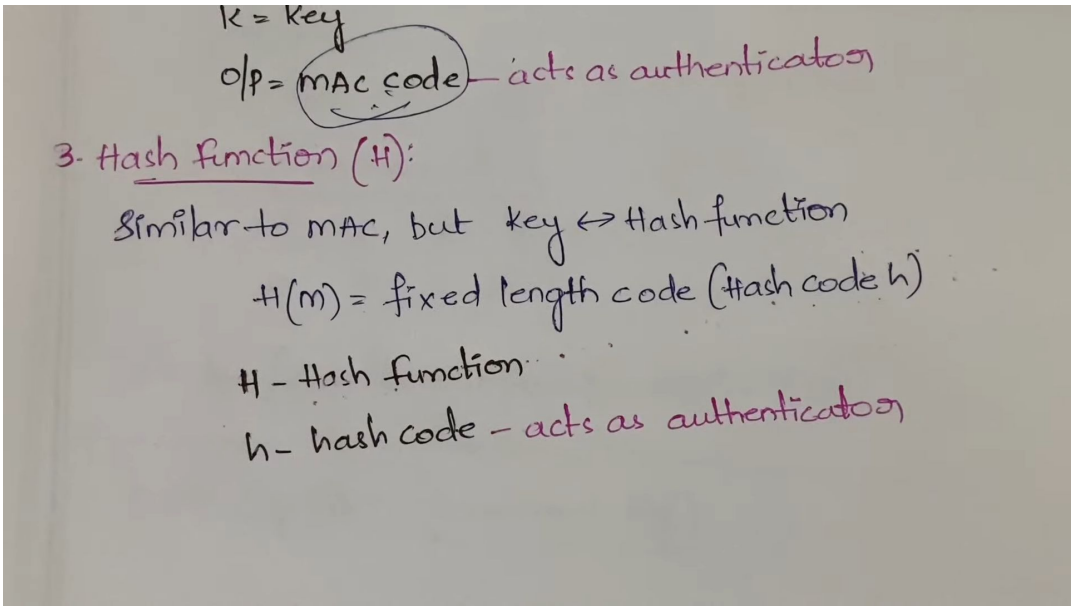
2:44


How it is done? - by authenticator
Generated by authentication functions
- (3) Authentication functions
1. message Encryption
2. message Authentication code (MAC)
3. Hash functions (H).
generate
Authen
1. Message Encryption:
plain Text - Cipher Text
acts as authenticator.

3:12


2. message authentication code:
C(M, K) = o/p (fixed length code)
C = authentication function
M = message
K = key
o/p = MAC code — acts as authenticator
3. Hash function (H):
Similar to MAC, but key ↔ Hash function
H(M) = fixed length code (Hash code h)

▷ 3:59


K = key
o/p = MAC code — acts as authenticator
3. Hash function (H):
Similar to MAC, but key ↔ Hash function
H(M) = fixed length code (Hash code h)
H - Hash function
h - hash code - acts as authenticator

▷ 4:48