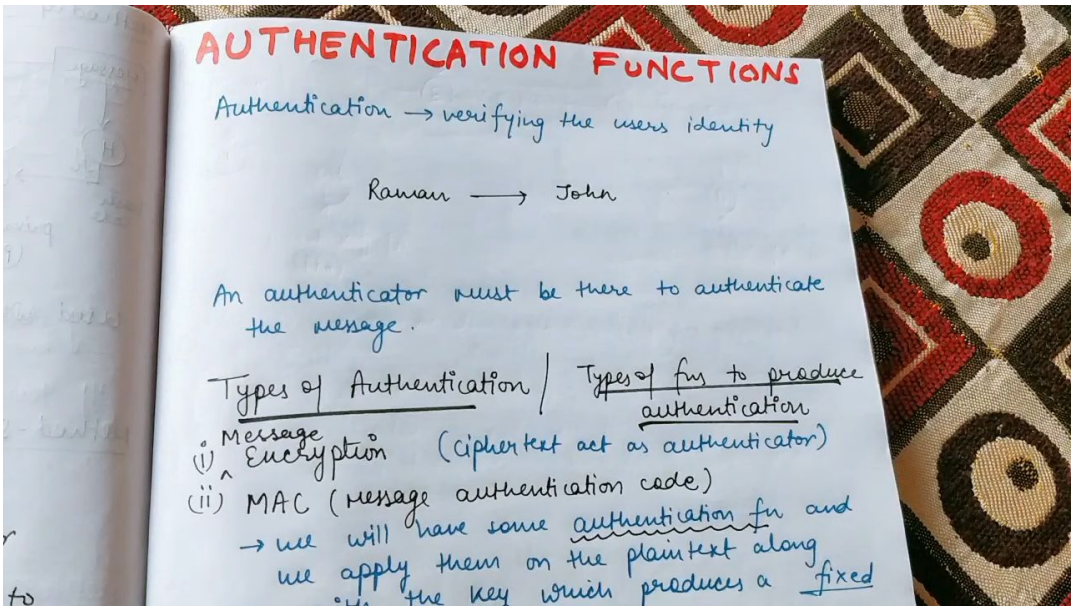
View, add and edit your notes in the app

Authentication functions and 3 ways to produce authentication | Message authentication

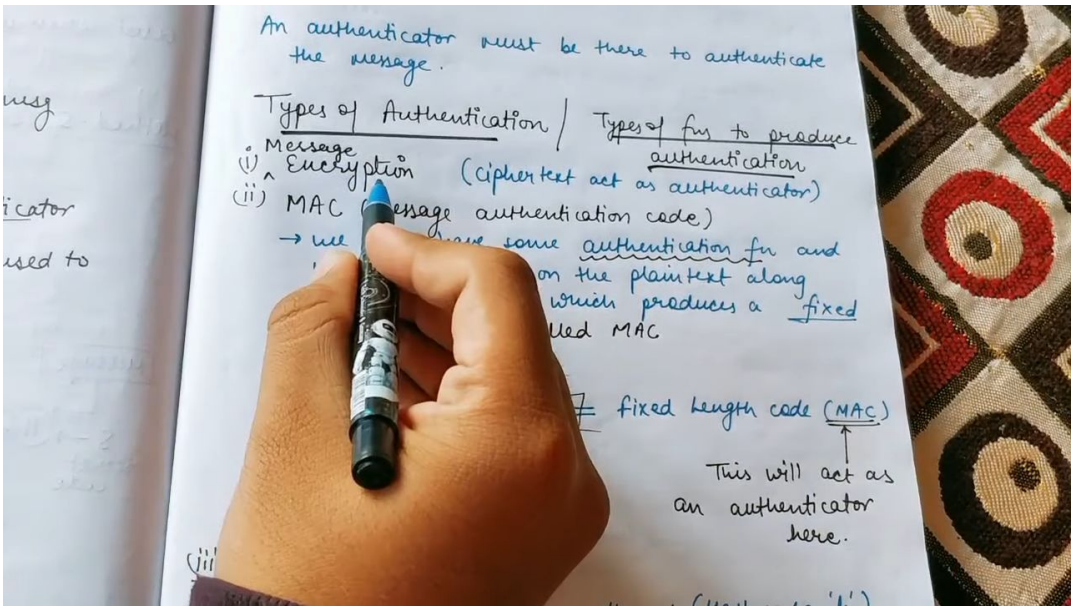
Generated on December 19, 2023

Summary

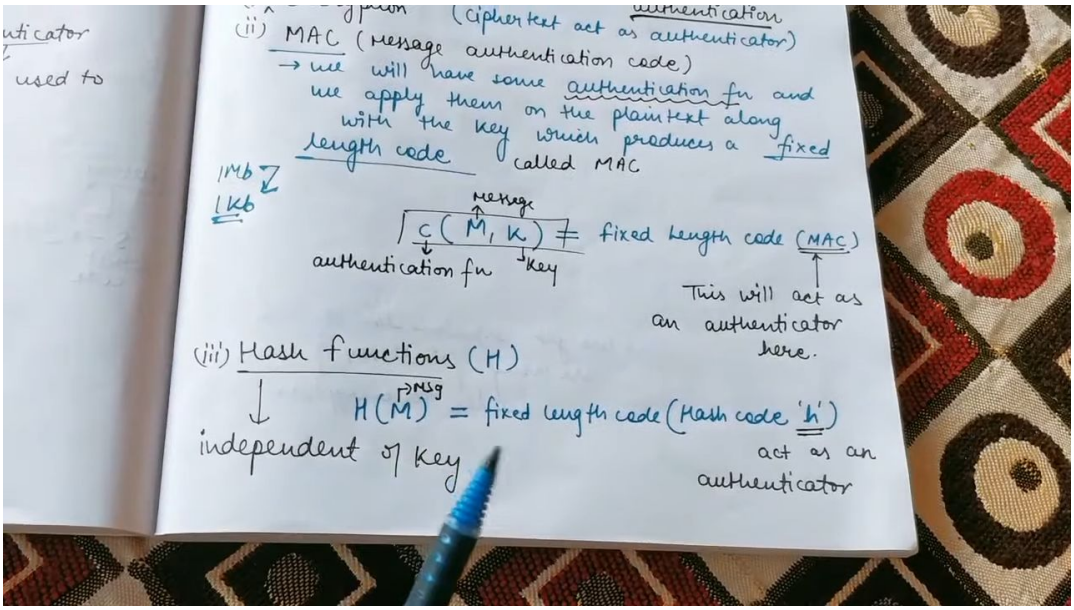
Notes	Screenshots	Bookmarks
0	7	0



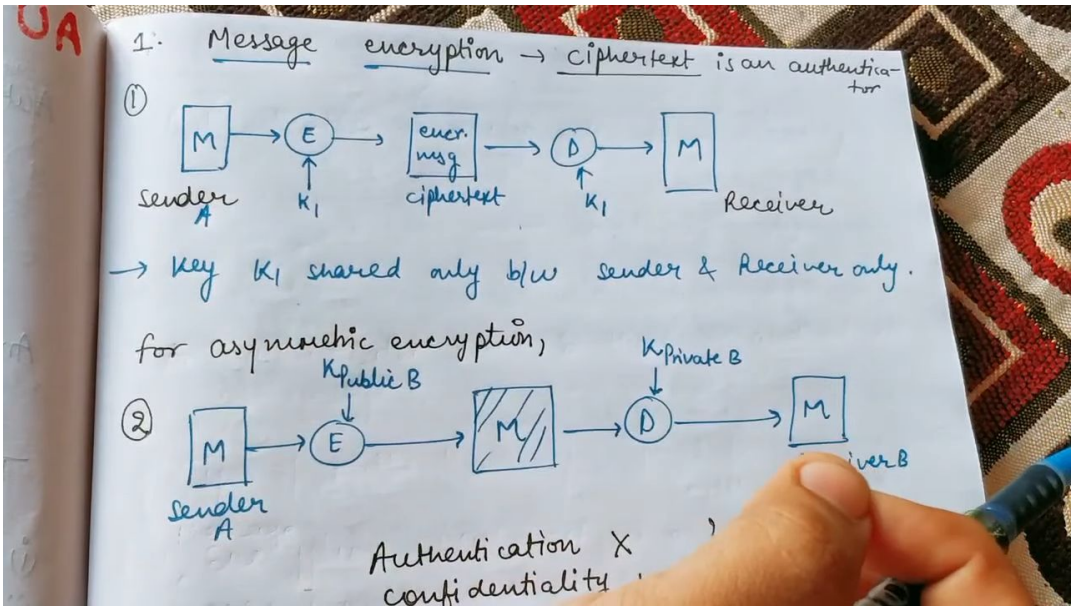
0:16


An authenticator must be there to authenticate the message.
Types of Authentication / Types of fns to produce authentication
(i) Message Encryption (ciphertext act as authenticator)
(ii) MAC (Message authentication code)
→ we will have some authentication fn and we apply them on the plaintext along with the key which produces a fixed length code called MAC
≠ fixed length code (MAC)
This will act as an authenticator here.
(iii)

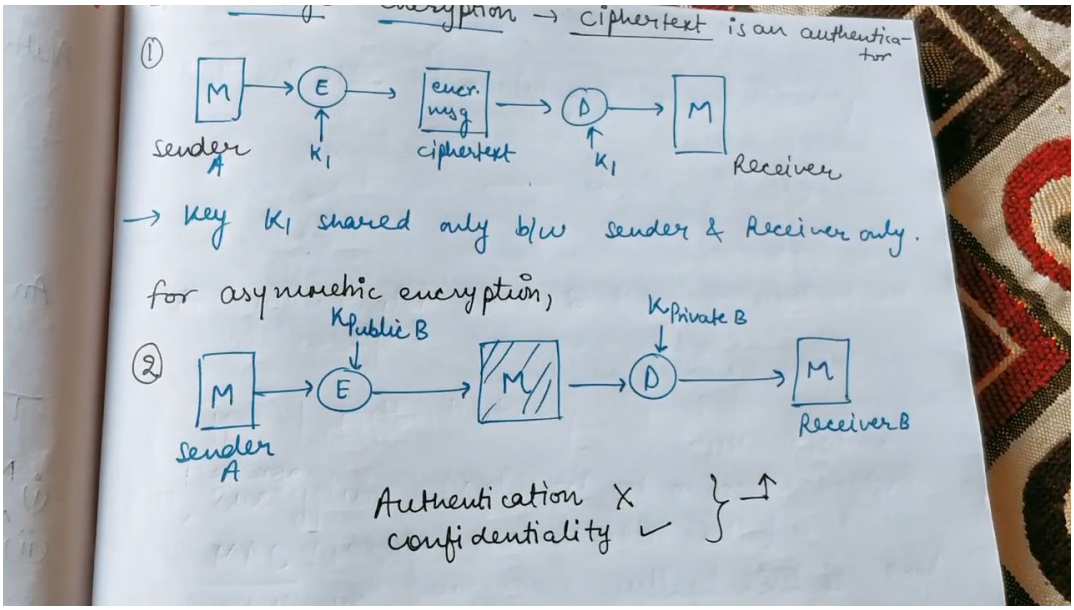
1:35


(ii) MAC (Message authentication code)
→ we will have some authentication fn and we apply them on the plaintext along with the key which produces a fixed length code called MAC
1MB
1KB
Message
C(M, K) ≠ fixed length code (MAC)
authentication fn
Key
This will act as an authenticator here.
(iii) Hash functions (H)
H(M^Msg) = fixed length code (Hash code 'h')
independent of key
act as an authenticator

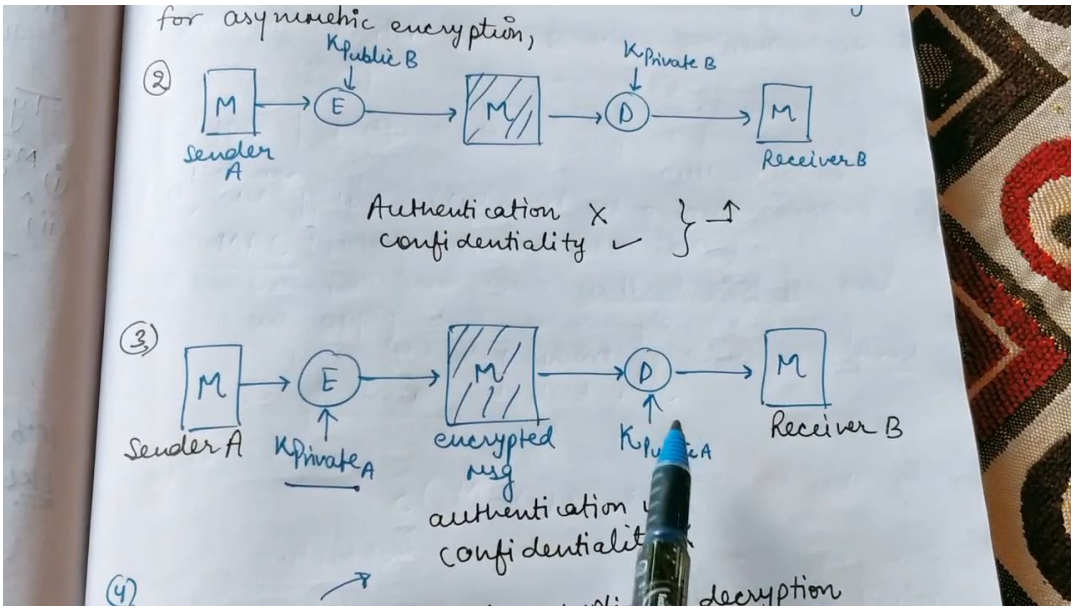
3:23


1. Message encryption → ciphertext is an authentication
(1)
M
E
K1
sender A
encr. msg
ciphertext
D
K1
M
Receiver
→ key K1 shared only b/w sender & Receiver only.
for asymmetric encryption,
(2)
K public B
K private B
M
E
D
M
Sender A
Receiver B
Authentication X
confidentiality

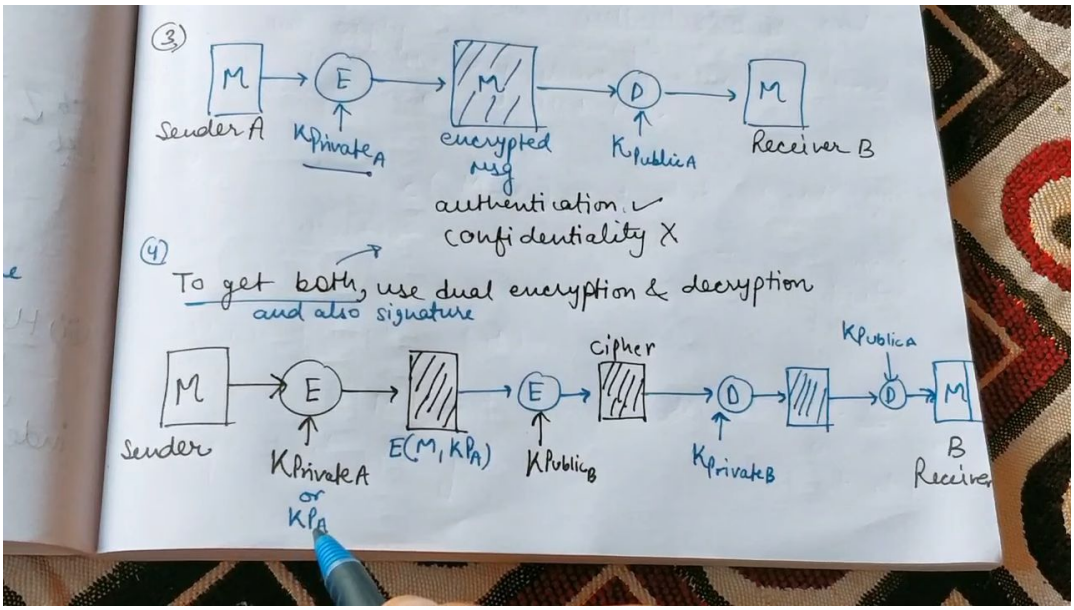
▷ 5:23


(1)
M
E
K1
sender A
encr. msg
ciphertext
D
K1
M
Receiver
→ key K1 shared only b/w sender & Receiver only.
for asymmetric encryption,
(2)
K public B
K private B
M
E
D
M
Sender A
Receiver B
Authentication X
confidentiality ✓

▷ 7:56


for asymmetric encryption,
② M E M D M
Sender A
K Public B
K Private B
Receiver B
Authentication ✗
Confidentiality ✓
③ M E M D M
Sender A
K Private A
encrypted msg
Receiver B
authentication ✓
confidentialit
④
decryption

8:54


③ M E M D M
Sender A
K Private A
encrypted msg
K Public A
Receiver B
authentication ✓
Confidentiality ✗
④ To get both, use dual encryption & decryption
and also signature
M E E D D M
cipher
K Public A
Sender
K Private A
or
K P A
E(M, K P A)
K Public B
K Private B
B
Receiver

9:52