Lecture 13 (Chapter 8):

R9

Given a checksum, it is not hard to find another message with the same checksum. Thus, it is good for error correction, but bad for authentication.

R10

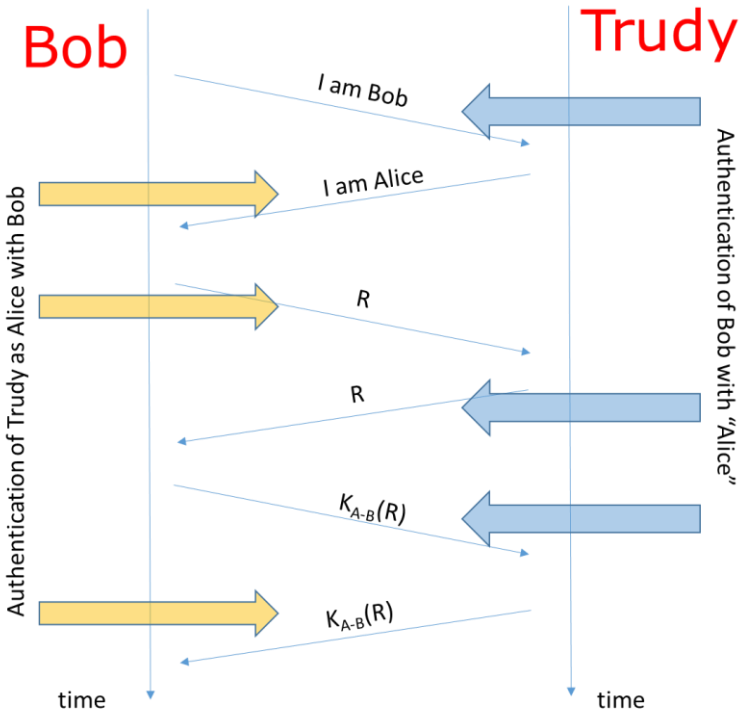
No. One of the three properties of the hash is that, given a hash x, it is computationally infeasible to find a message m with H(m) = x.

R16

It defends against replay attack. If you intercepted the message I used to open my car, you cannot use it because next message to open the car must be different, thanks to the nonce.

P15

Trudy waits for Bob to authenticate himself, to extract the encryption of the nonce, and use it to sell herself as Alice.



Thus, Trudy does not need the shared key K_{A-B}, since it can extract $K_{A-B}(R)$.

P18

a) No. The public key of Bob is widely known, thus anybody could use it, for example to share a symmetric key. Without a public-private key pair or a pre-shared secret, Bob cannot verify that Alice created the message.
b) Yes, Alice can encrypt a message with Bob's public key, and only Bob will be able to decrypt it.

P23

"The book says that the key of Bob is **unique to him**, thus it is a key that Bob will not disclose (either his private key, or a key for a symmetric encryption algorithm.)
For Alice to verify the signature, she would need to know the key of Bob, which is not possible. Thus, the proposed MAC scheme cannot be implemented."