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

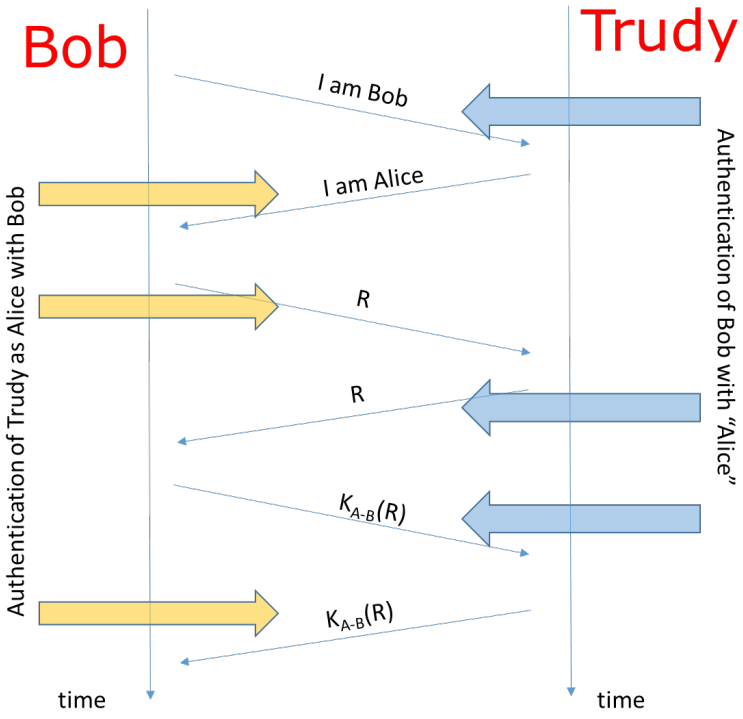
No. One of the three properties of the hash is that, given a hash x, it is computationally infeasible to find a message m with H(m) = x.

R16

It defends against replay attack. If you intercepted the message I used to open my car, you cannot use it because next message will 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. There are no more security tools that Alice could use, thus Bob cannot verify that Alice created a message
b) Yes, Alice can encrypt a message with Bob's public key, and only Bob will be able to decrypt it.

P23

The text says that Bob's key is unique to him, which implies that nobody else should know it. Think for example about a private key, or a symmetric key. For the proposed MAC to work, Alice would need to receive the key in advance to verify the MAC, but this is not compatible with the key being unique to Bob.