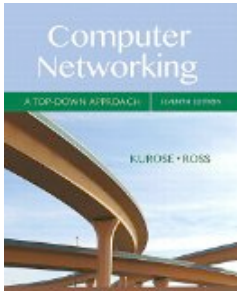
COMP 375: Lecture 40

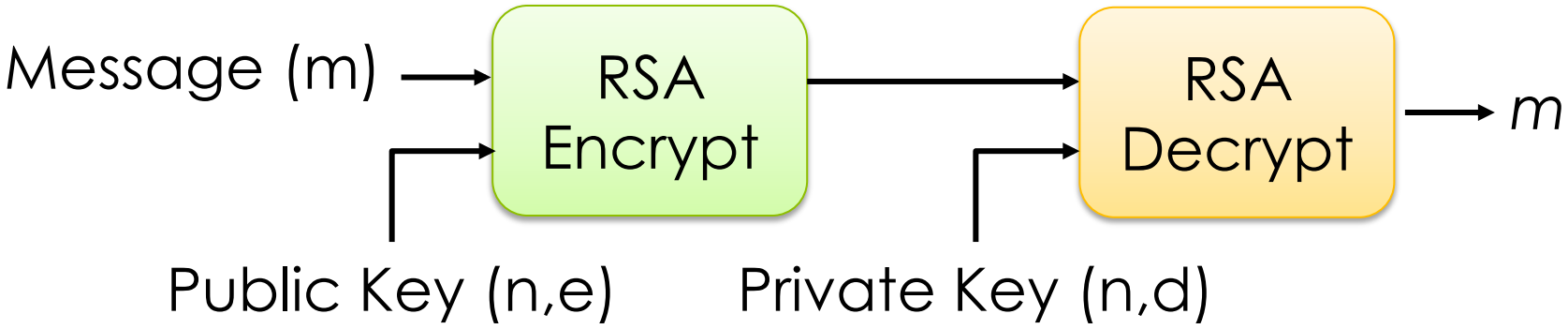


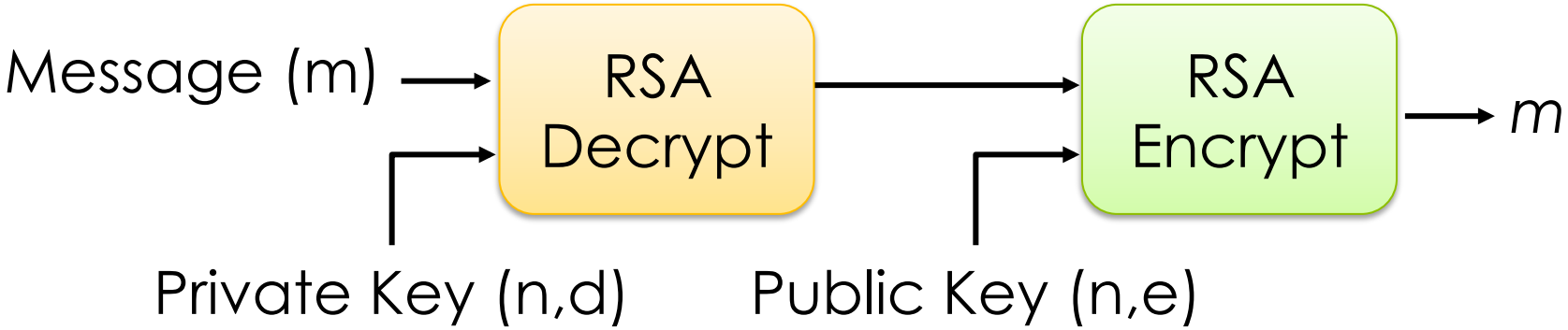
- **News & Notes:**
  - ACM Club Meeting tomorrow
  - Project 5 demos due by Monday at 5PM
  - Final Exam: Friday, May 18
- **Reading (Fri, Dec. 11)**
  - None

Section 8.2.2

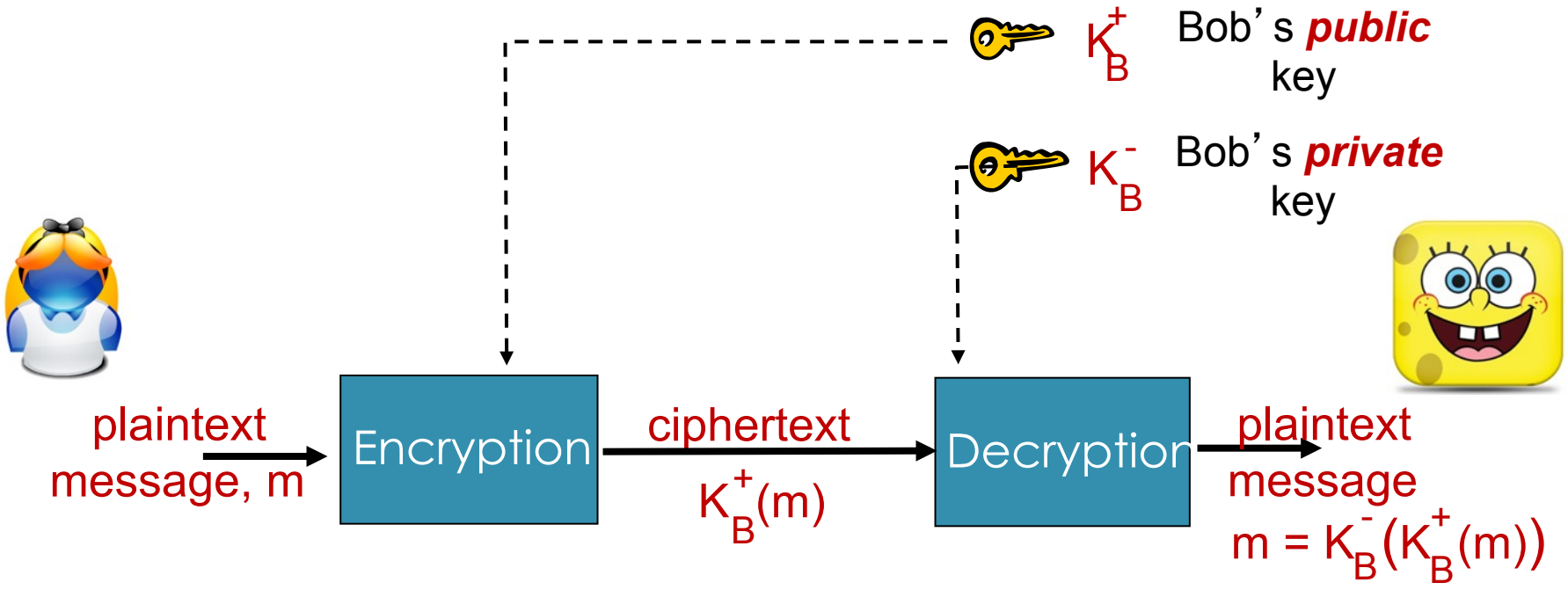
PUBLIC KEY ENCRYPTION

RSA has the important property that it doesn't matter if you "encrypt" or "decrypt" first.

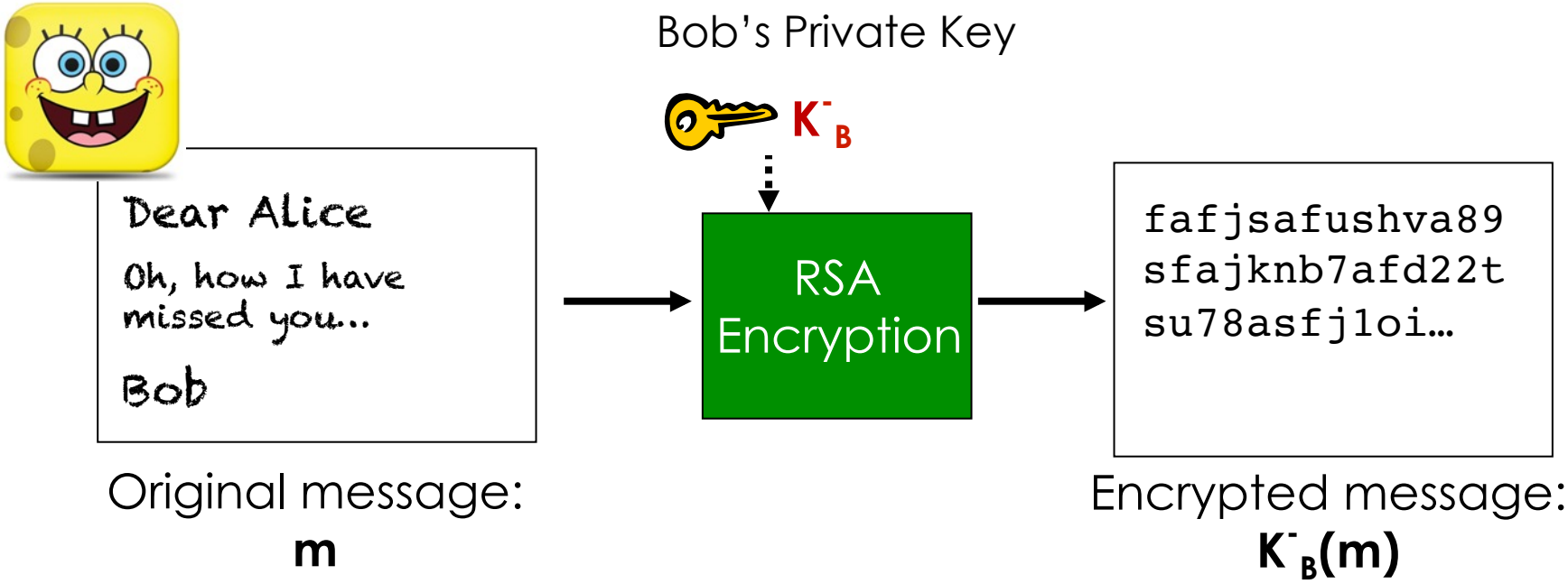




Like symmetric key crypto, public key crypto enables confidentiality.

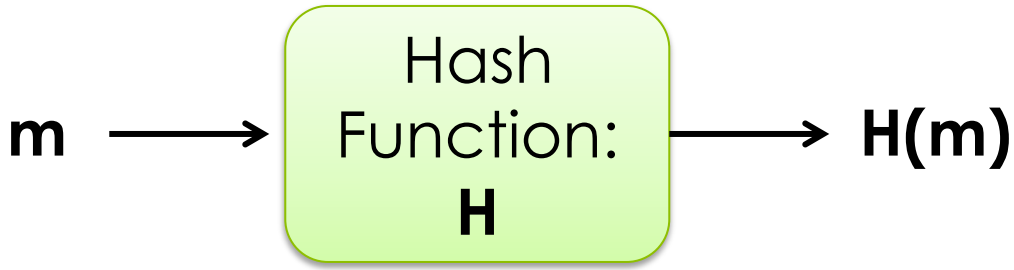


Which security features does the following setup provide to us?



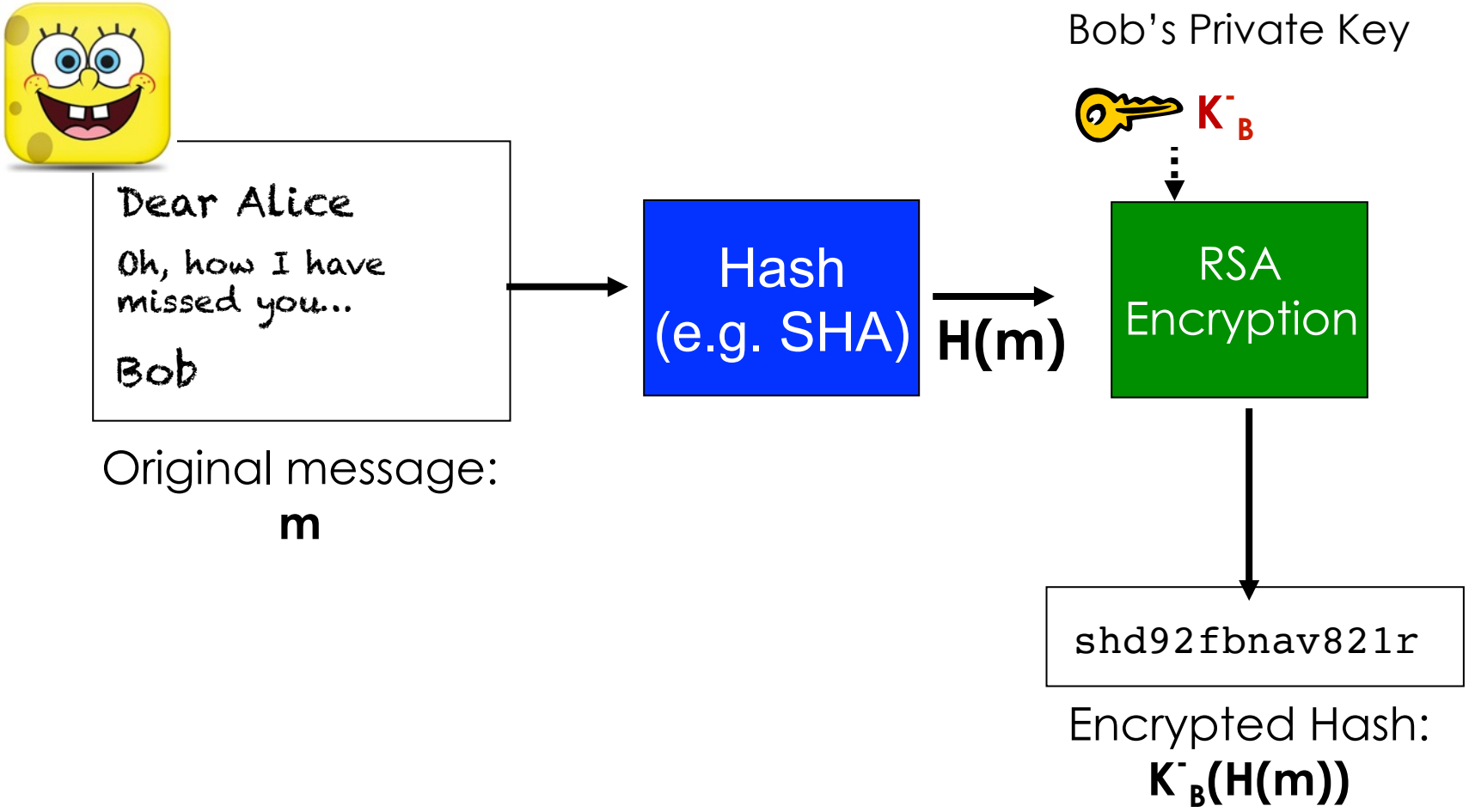
A.	Confidentiality ✗
B.	Digital Signature
C.	Both A and B
D.	Neither A nor B

Cryptographic hashes are fast functions that can complement encryption.

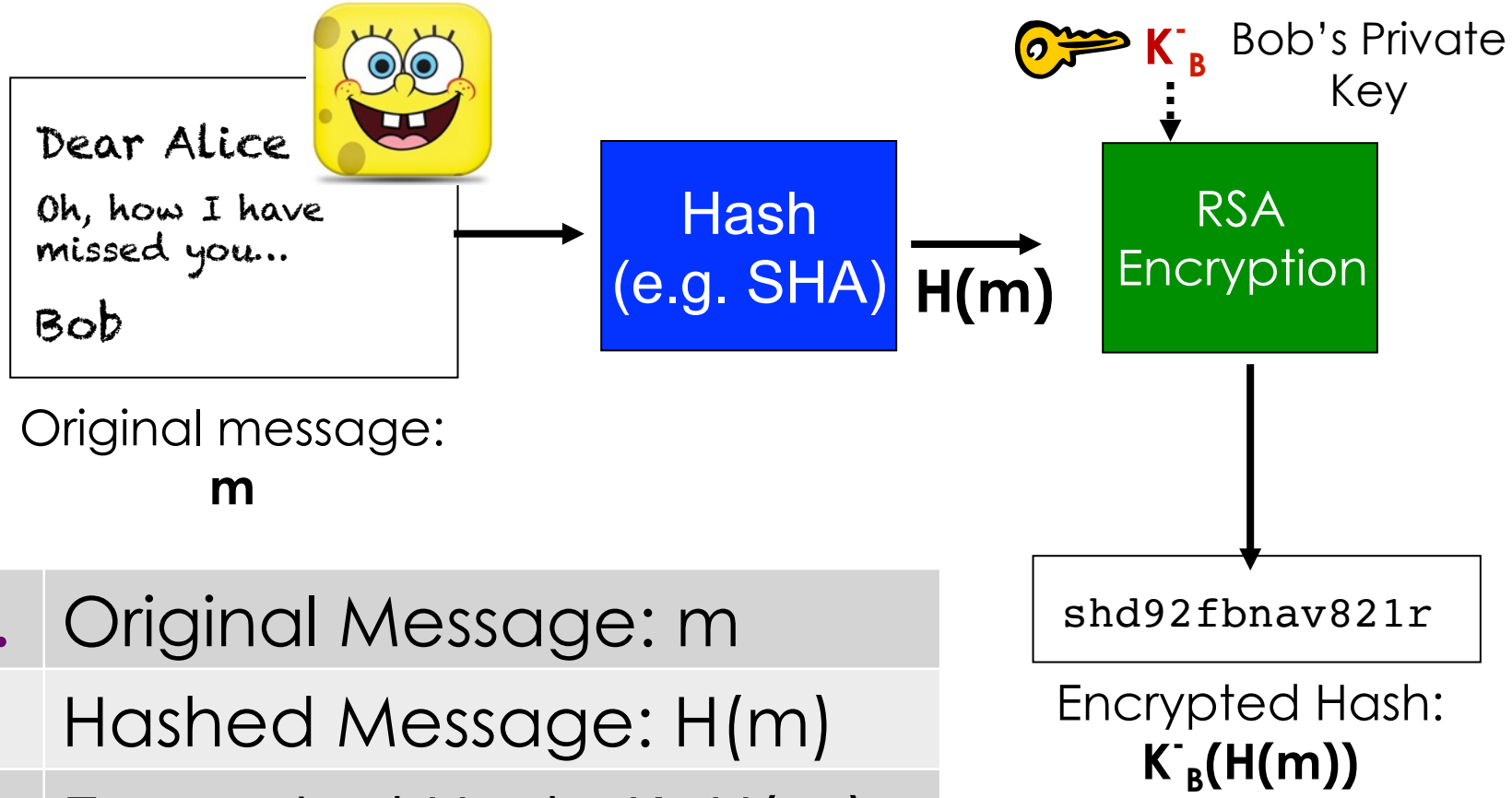


What are the important properties of a cryptographic hash function?

By hashing first, we reduce the amount of data we need to encrypt.



Which are required in order to both **view** the message **and verify** it's **integrity**?

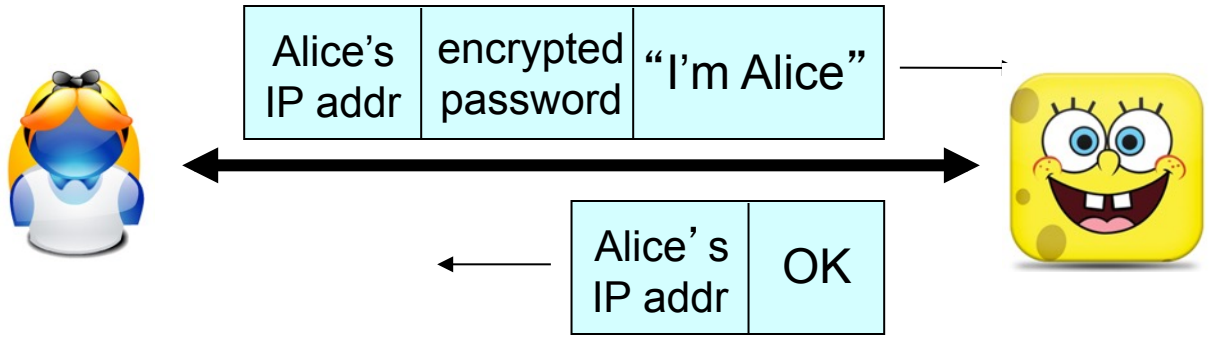


A.	Original Message: m
B.	Hashed Message: H(m)
C.	Encrypted Hash: $K^-_B H(m)$
D.	Two of the above
E.	All of the above.

Section 8.4

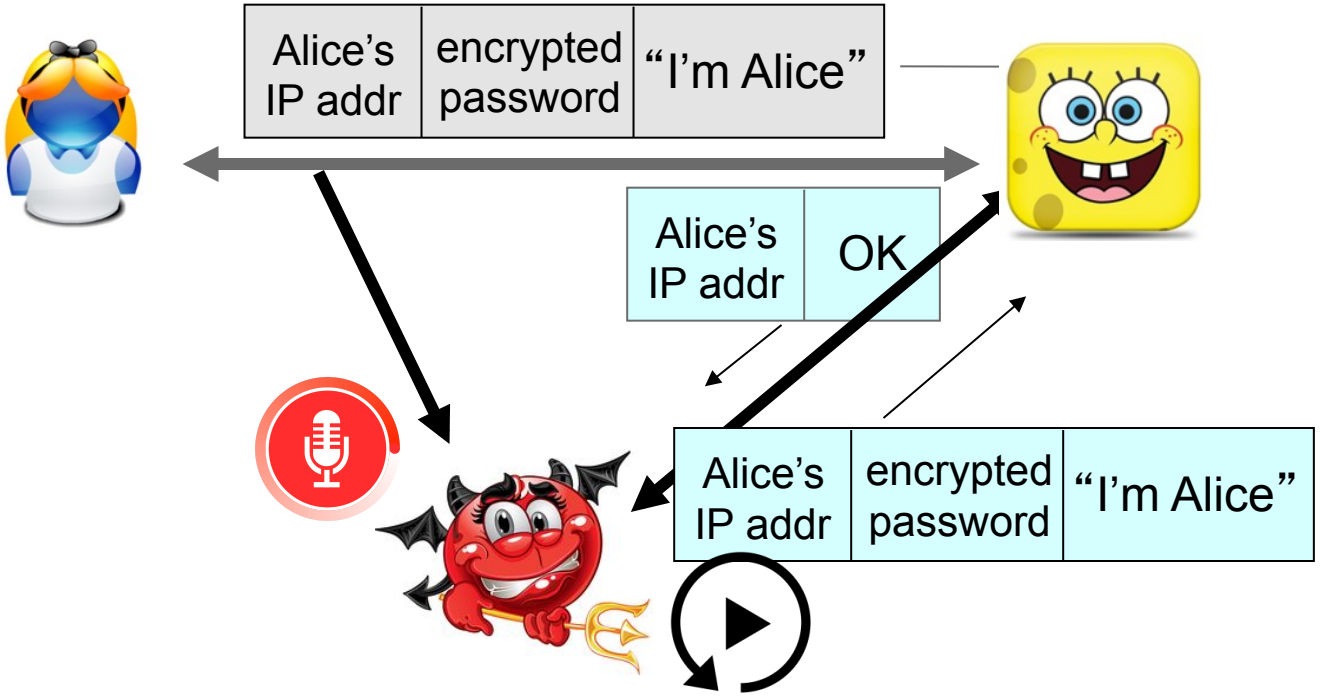
AUTHENTICATION

Authentication using only an encrypted password isn't secure.

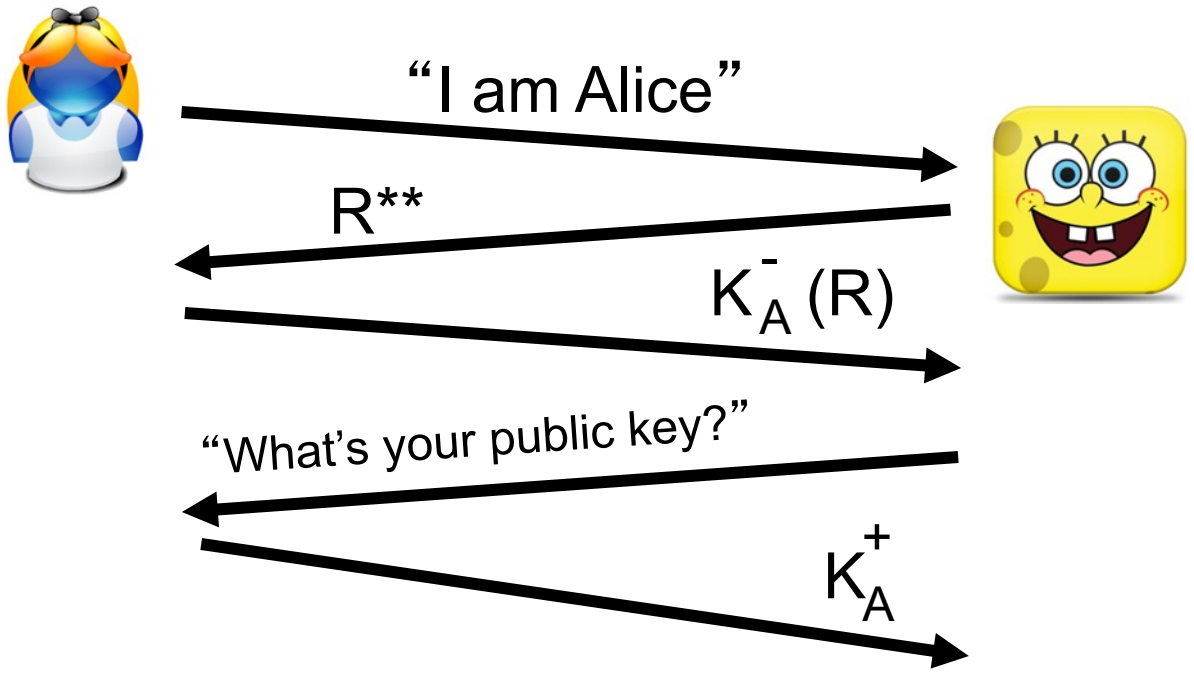


How might the little devil successfully authenticate as Alice?

If the same message is sent every time, **replay attacks** become possible.

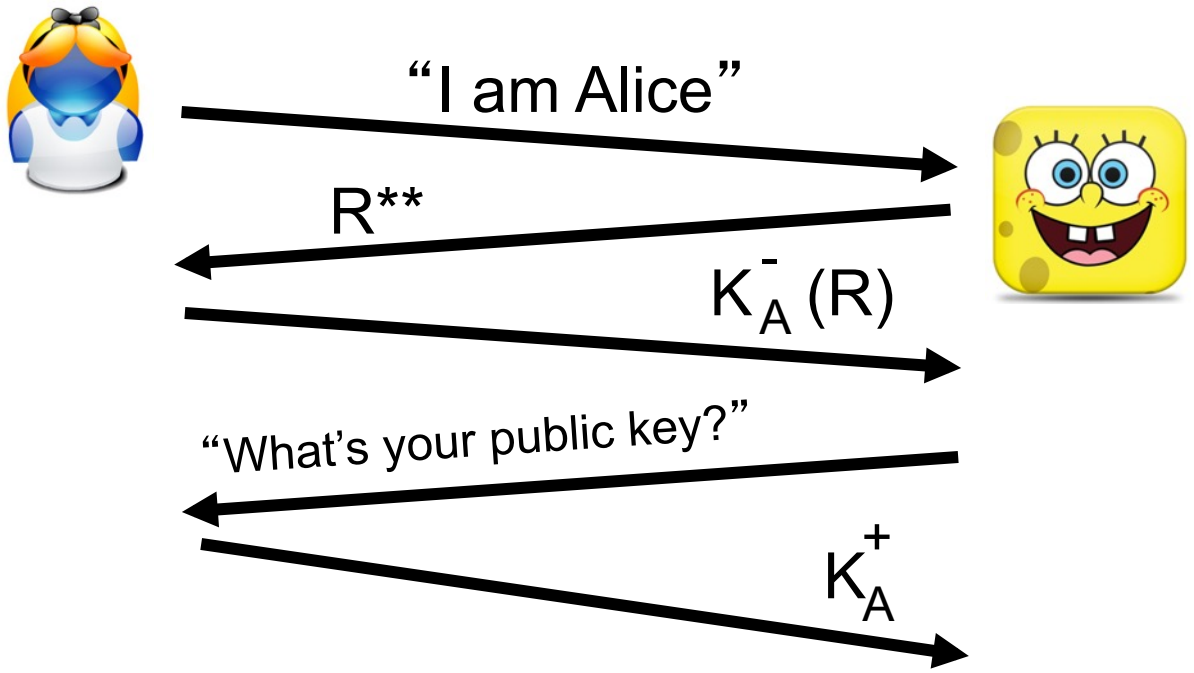


We can use a **nonce** to introduce more randomness and thwart replays.



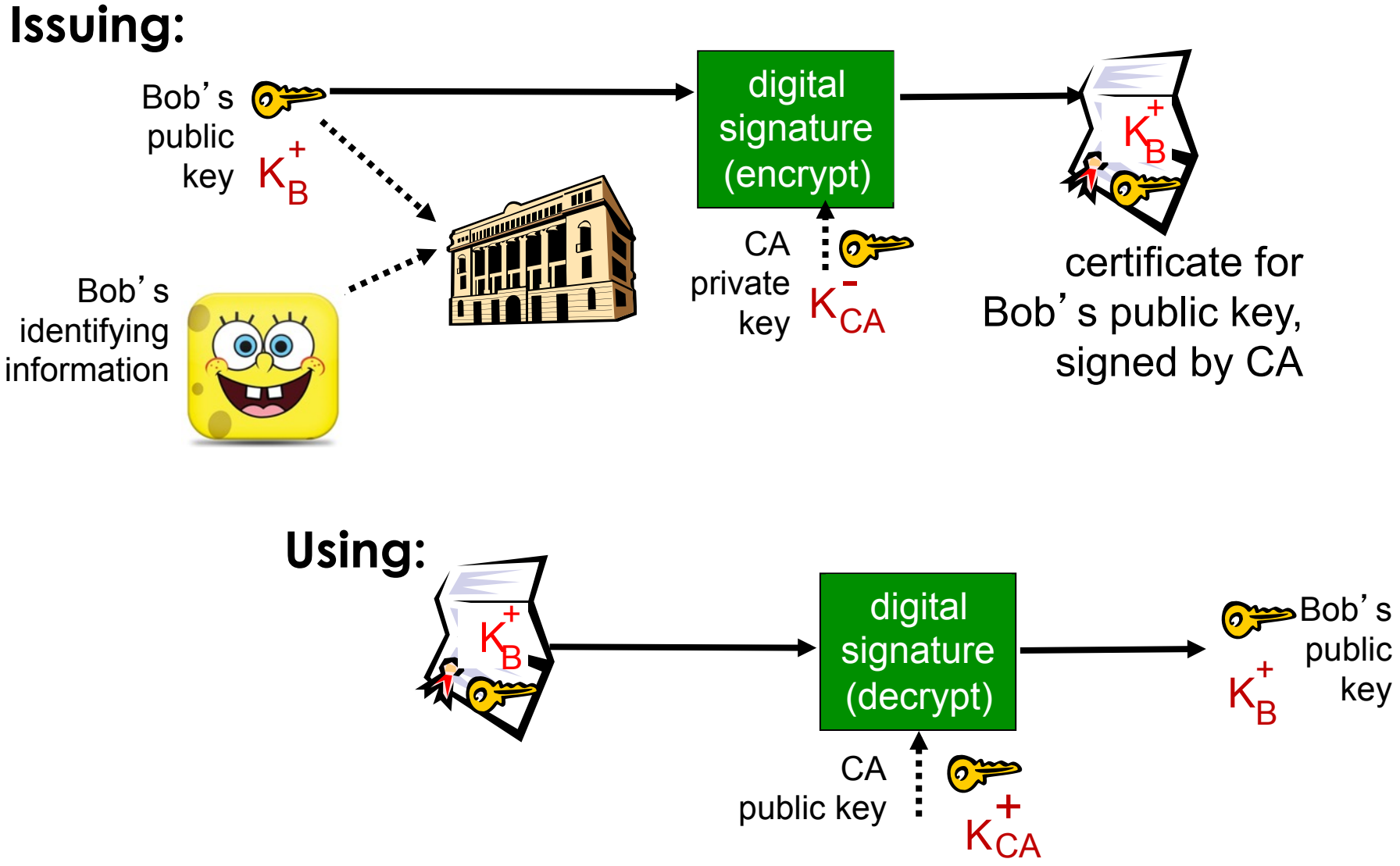
***R is a nonce (i.e. "one time value").*

Does this guarantee that Bob is actually talking to Alice?



A.	Yes
B.	No

A **certificate authority** can bind a public key to a person/organization.



Which layer in our network stack should we handle security?

A.	Application Layer
B.	Transport Layer
C.	Network Layer
D.	Link Layer
E.	All of the above