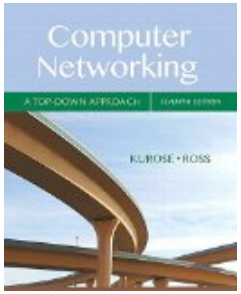
COMP 375: Lecture 41



- **News & Notes:**
  - Project 5 demos: Sign up on Piazza
  - Need volunteer to administer course evals on Monday
  - Clicker Registration in class Monday
  - Final Exam: Friday, May 18
- **Reading (Mon, Dec. 14)**
  - "Neverwhere" by Neil Gaiman

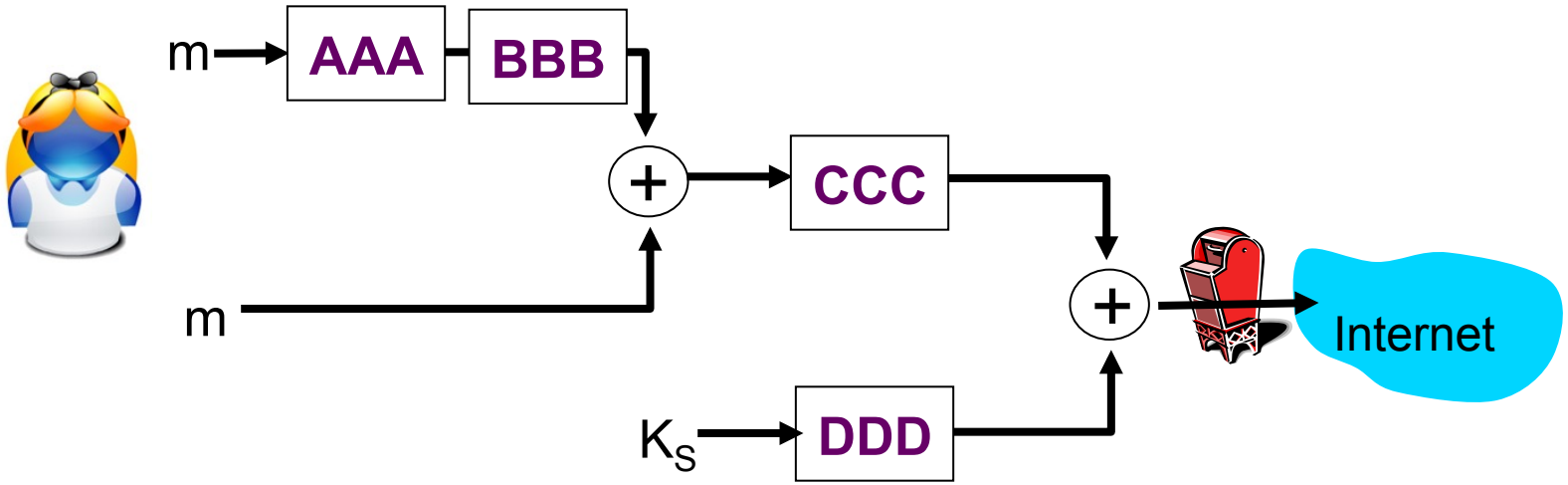
"This is America,
Don't catch you clickin' in"

- Childish Gambino

Section 8.5

APPLICATION LAYER SECURITY (EMAIL)

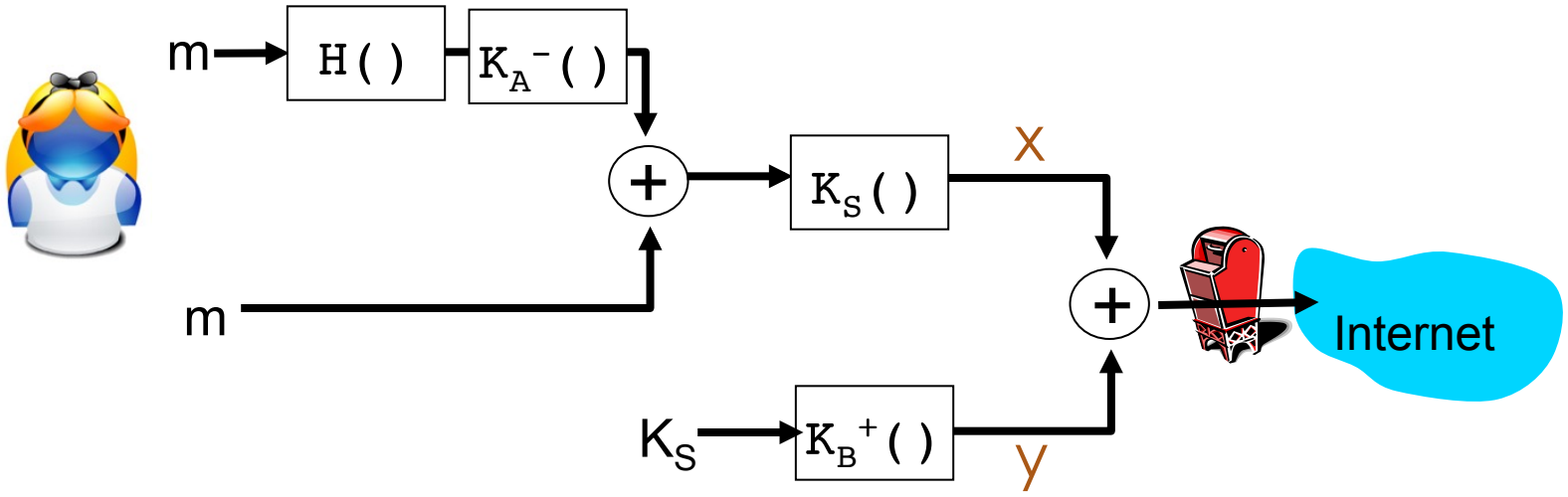
Fill in the ops so that e-mail is private, and cannot be forged/modified.

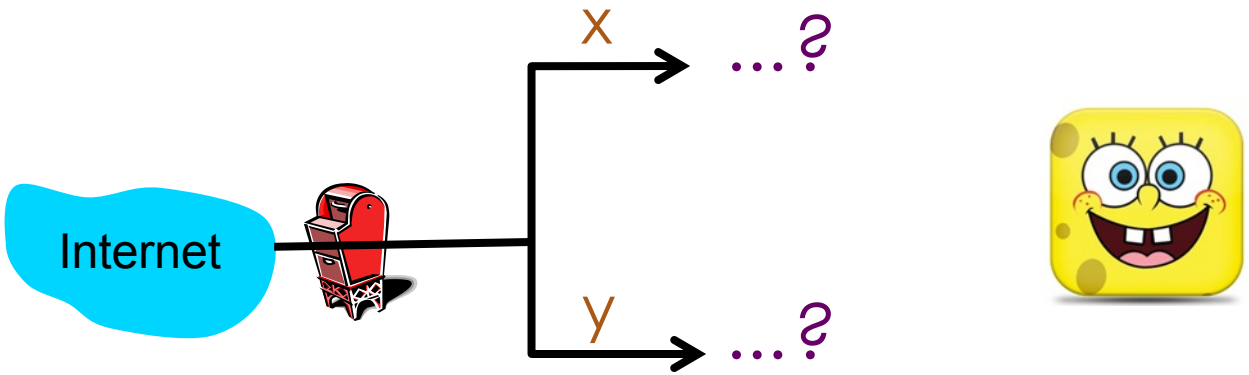


Available Ops:

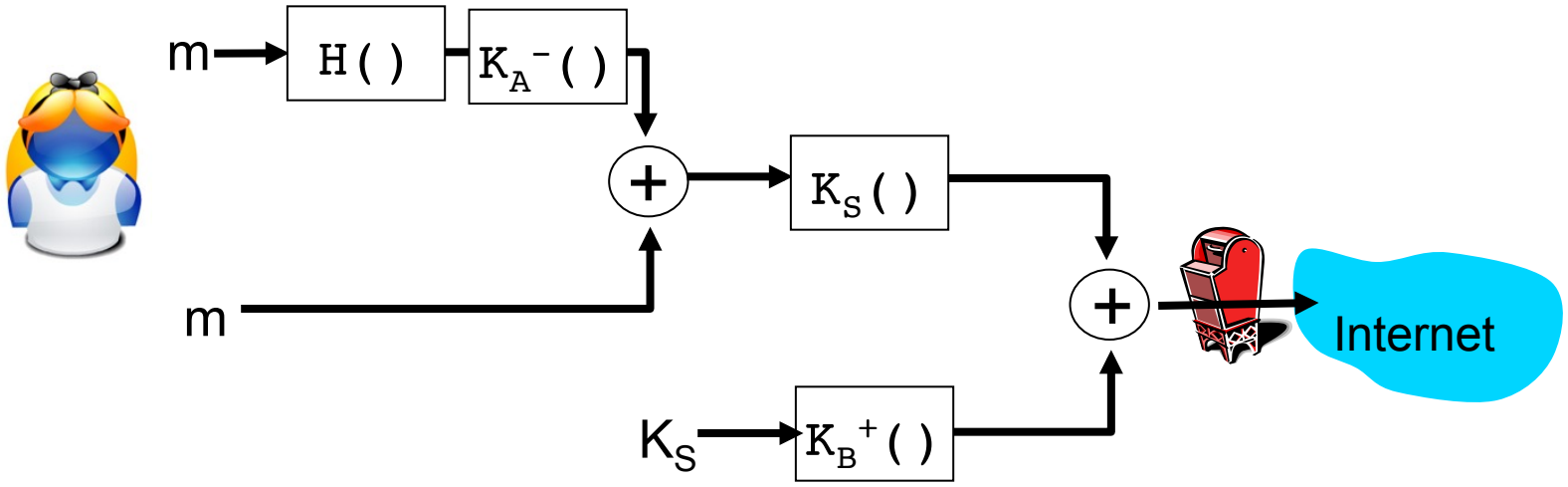
- Hash: $H()$
- Encrypt with Shared Private Key: $K_S()$
- Encrypt with Alice's Public/Private Key: $K_A^+()$, $K_A^-()$
- Encrypt with Bob's Public/Private Key: $K_B^+()$, $K_B^-()$

What does Bob have to do to get the original message (m) and verify its integrity?





Does the order of H and K_A^- matter?



A.	**Yes**, for correctness.
B.	**Yes**, but only for efficiency.
C.	**No**.

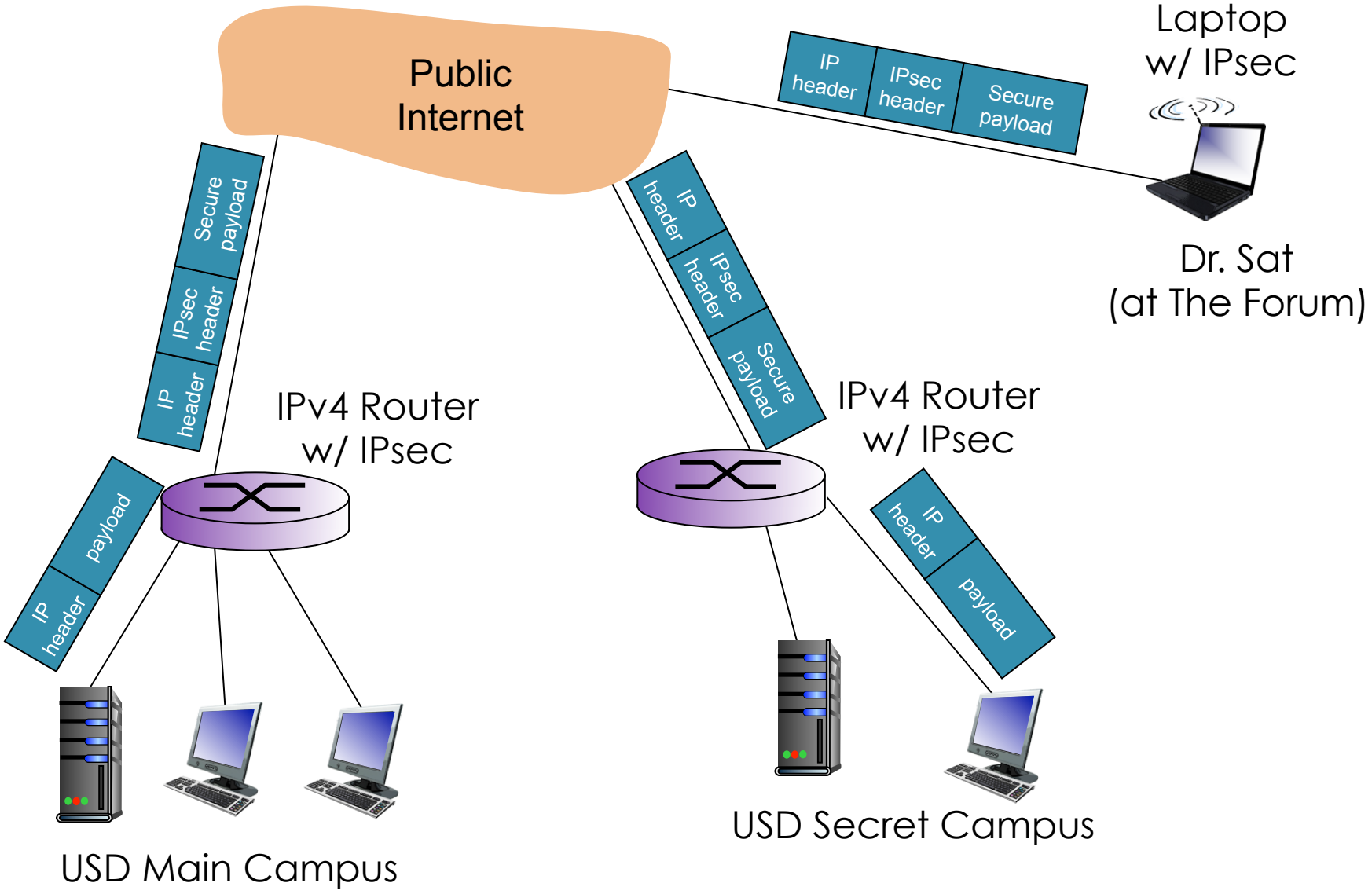
Section 8.6

NETWORK LAYER SECURITY

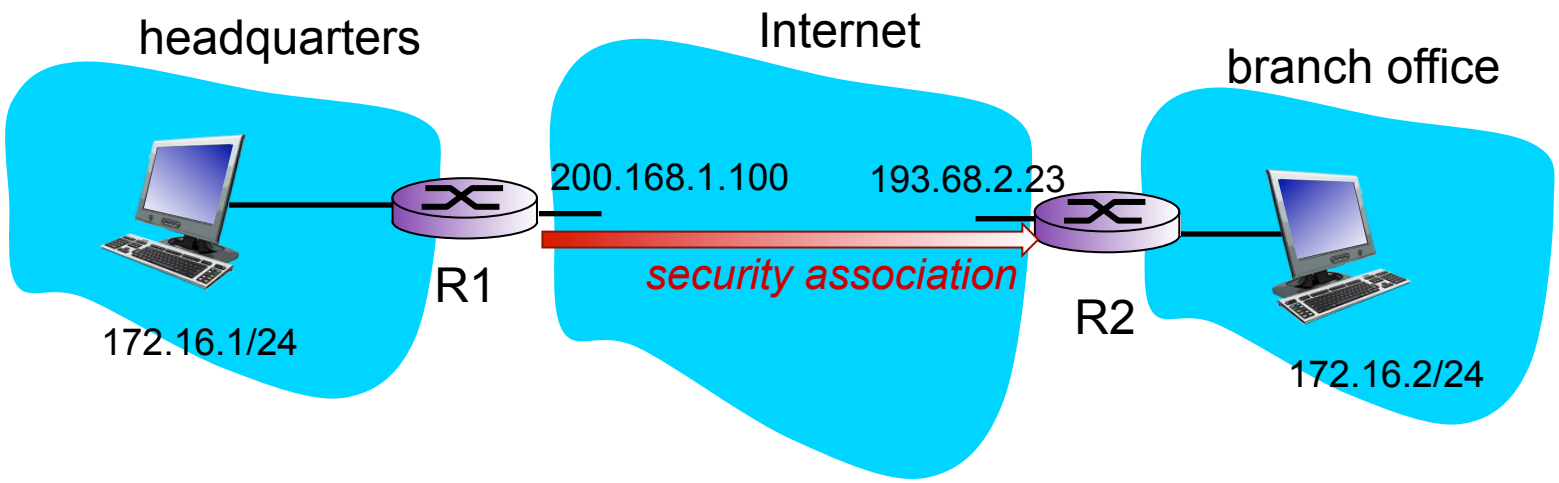
Discussion Question

What is a Virtual Private Network (VPN)?

VPNs are formed using IPsec.



Entities establish **security associations** before sending IPsec datagrams.

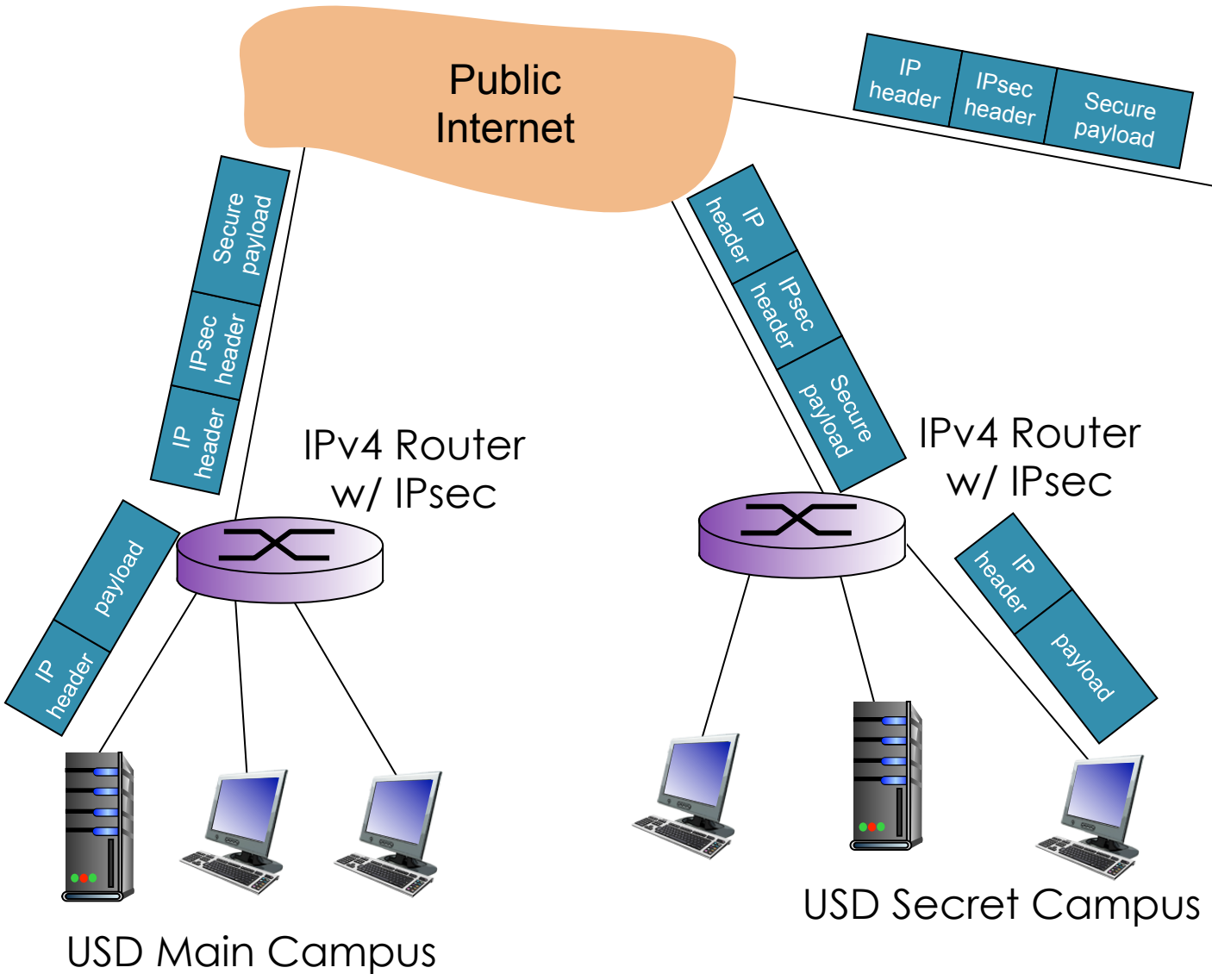


- Each entity maintains a **security association database** (SAD) to track all of its associations.
- Sender uses a **security policy database** (SPD) to decide if datagram needs to use IPsec.

Which of the following is **not** part of a IPsec security association (SA)?

A.	Encryption key
B.	Type of encryption used
C.	Data to be encrypted
D.	More than one of the above
E.	None of the above (*i.e.* all three are part of the SA)

How many SAs are required here?



A.	1
B.	3
C	6
D.	7
E.	14