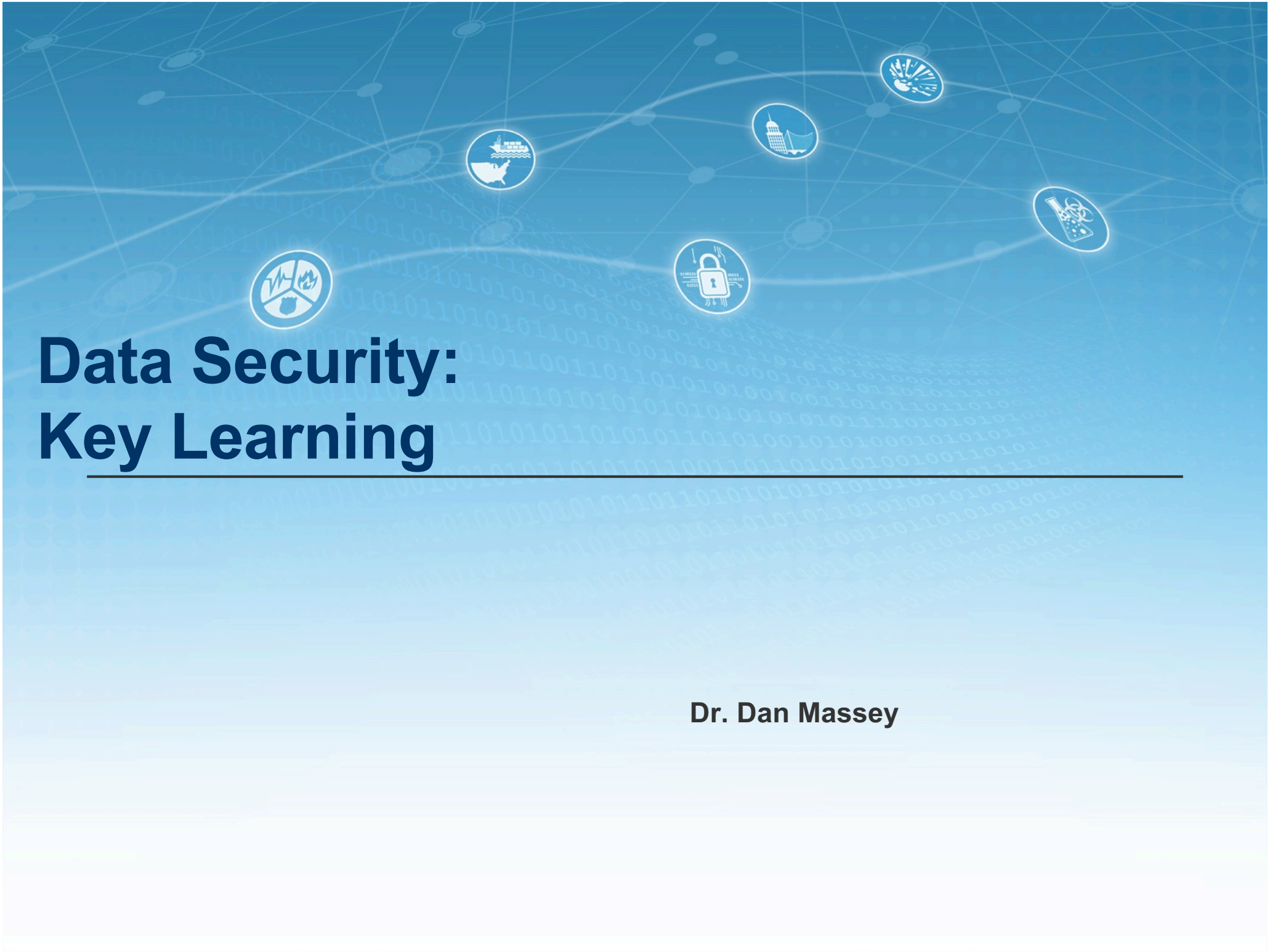


Data Security: Key Learning

Dr. Dan Massey

Returning to Our Motivating Problems:

Confidentiality: how could we encrypt a message? (email, web/http, sms, etc)

Encrypt Message with receiver's public key

Integrity: how could we authenticate a message?

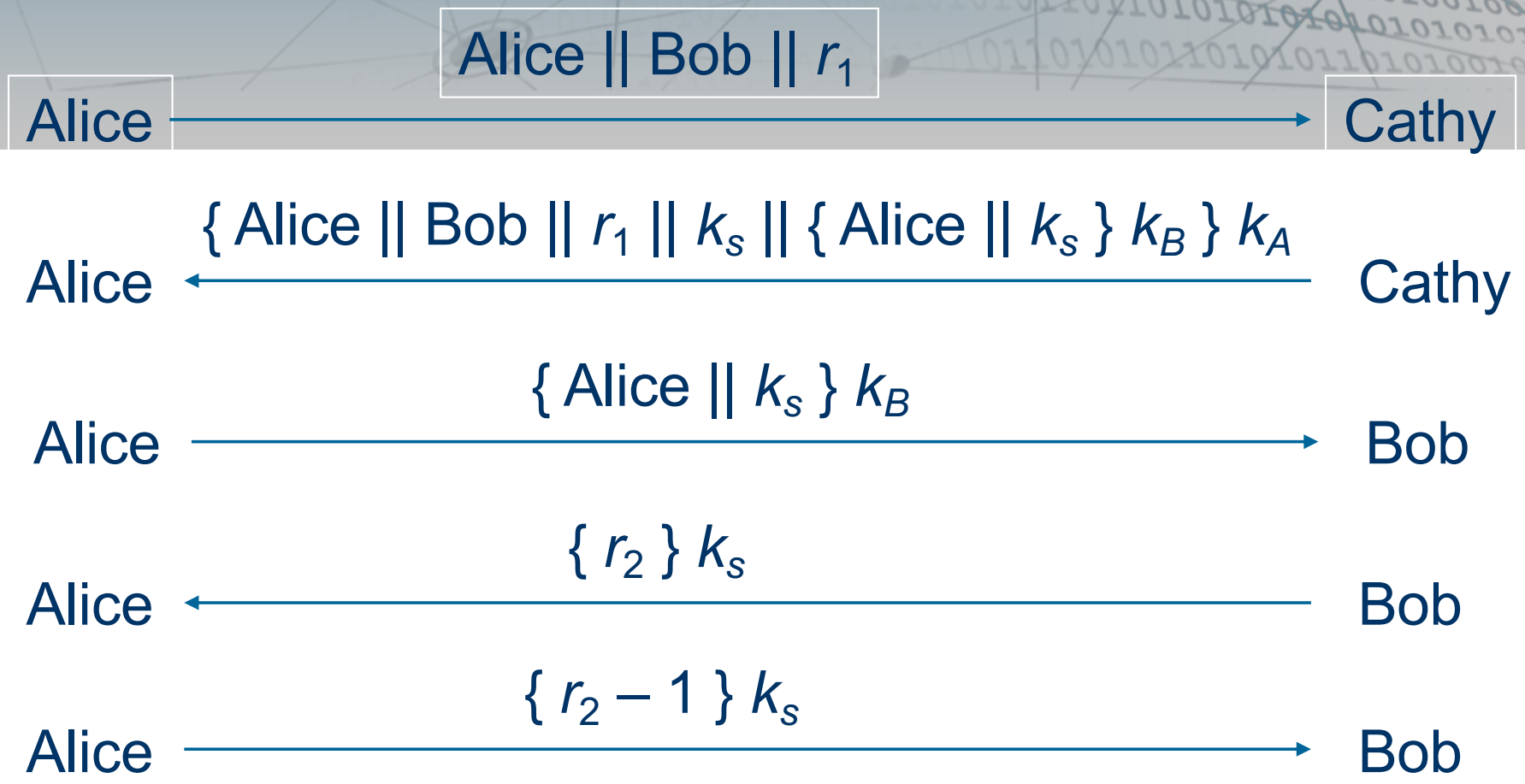
Sign message with sender's private key

(availability – not primary motivation now, provided the approach is feasible)

Establishing a Symmetric Key

- Alice and Bob want to establish a symmetric key
  - AES (symmetric) is faster and more efficient than RSA (asymmetric)
- Previously relied on a trusted third party Cathy
  - See previous slides on learning symmetric keys and replay attacks!
- New approach is to leverage asymmetric keys
  - Alice has a public/private key pair.
  - Bob has a public/private key pair.
- Can we use the public/private keys to establish a symmetric key?

Recall: Needham-Schroeder



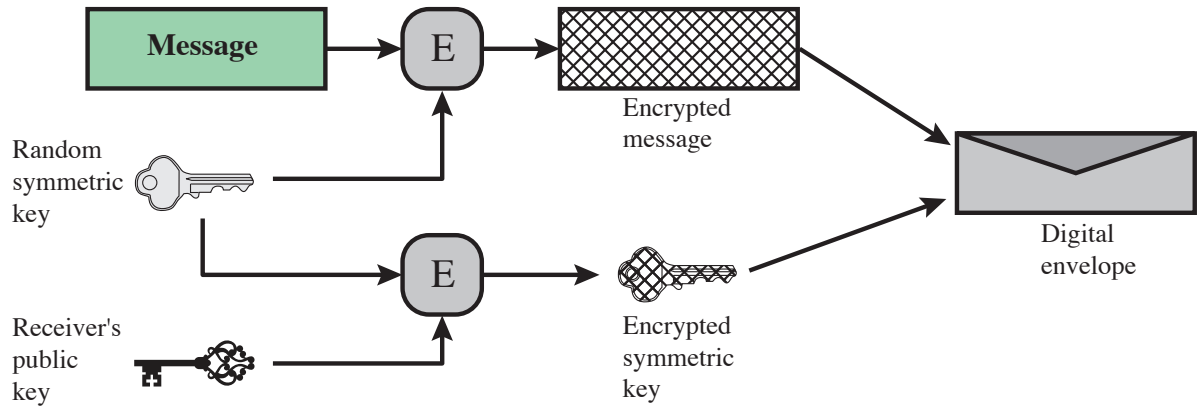
Worked entirely with symmetric keys….
Ka, Kb, and Ks are all symmetric keys (e.g. AES keys)

Key Exchange Using Public Keys

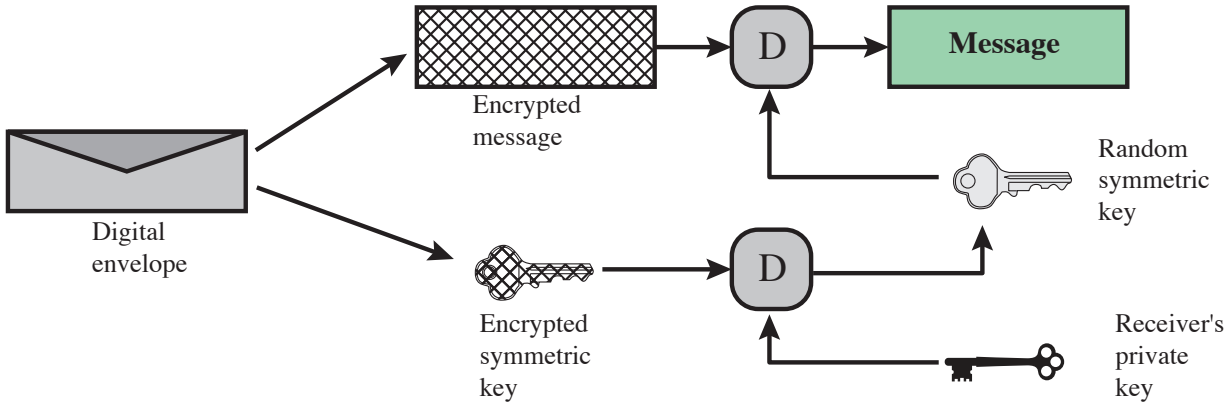
- Public Key Definitions and Assumptions
  - e_A, e_B Alice and Bob's public keys known to all
  - d_A, d_B Alice and Bob's private keys known only to owner
- Simple protocol
  - Alice generates a new symmetric session key
  - k_s is desired session key

Limitation and Solution

- Vulnerable to forgery
  - Because e_B known to anyone, Bob has no assurance that Alice sent message
- Simple fix uses Alice's private key
  - k_s is desired session key



(a) Creation of a digital envelope



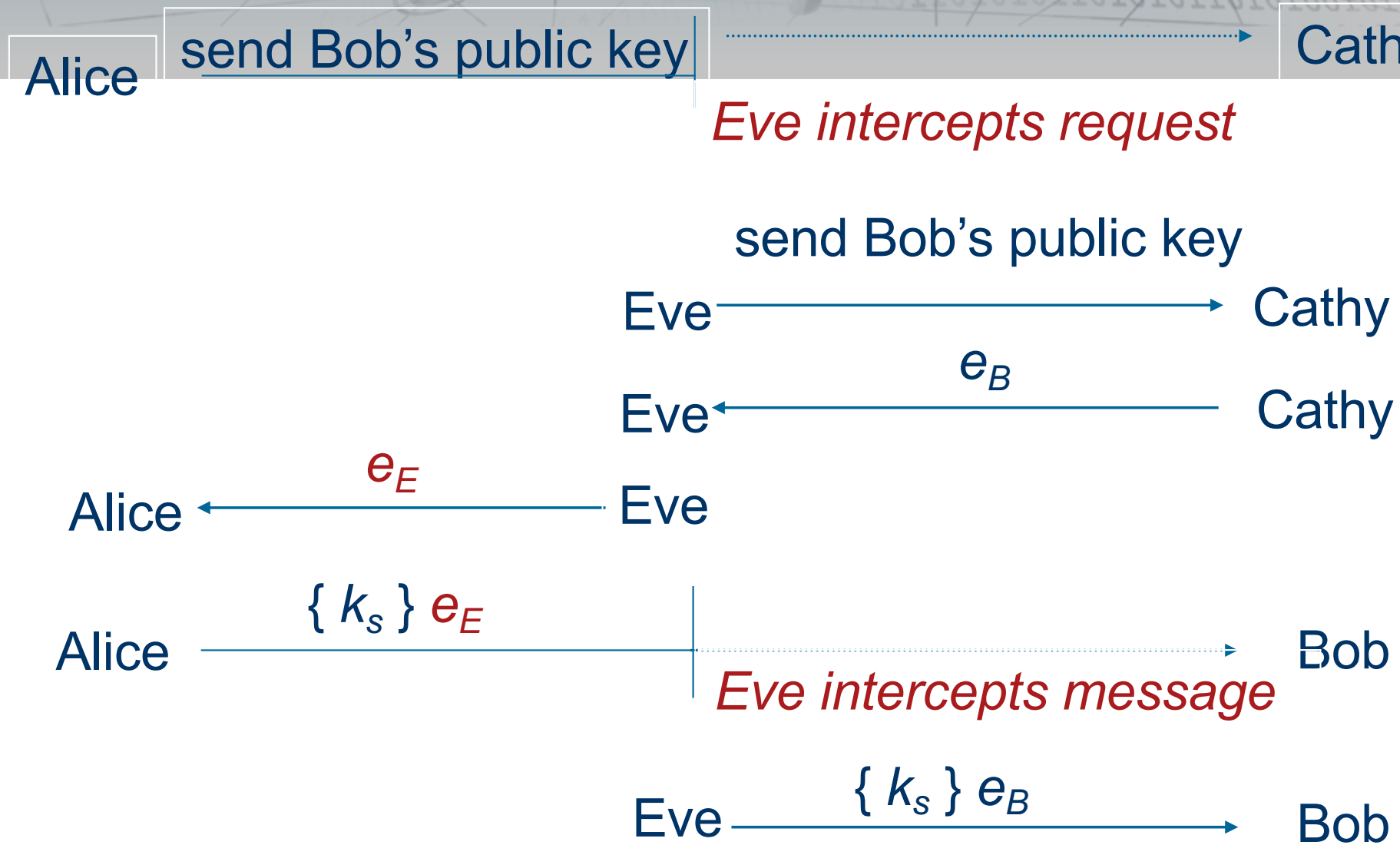
(b) Opening a digital envelope

Figure 2.9 Digital Envelopes

Learning Public Keys

- How Does Alice Learn Bob's Public Key?
  - Previous slide only works if Alice knows the correct e_B
- Much Easier Than Agreeing on a Secret Key
  - For the secret key, adversary must not observe the key
  - For the public key, everyone can observe the key.
- Naïve First Attempt
  - Alice asks trusted third party Cathy for Bob's public key
  - No need to encrypt the message
  - Everyone can (and should) learn Bob's public key

Man In The Middle Attack



Certificate Authorities

- How Does Alice Learn Bob's Public Key?
  - Assume already learned public key for trusted third party Cathy.
- Bob Asks Cathy to Sign His Public Key
  - Bob securely provides his public key to Cathy
  - Cathy signs Bob's public key with Cathy's private key
- Alice Uses Cathy to Verify Bob's Public Key
  - Alice has securely learned Cathy's public key
  - Bob's sends Alice his public key and the signature from Cathy
  - Using Cathy's public key, Alice can verify Bob's public key
- Cathy is a Certificate Authority!

Learning the Public Key Using a CA

Processing Actions at Alice:

Alice knows e_{Cathy} (Cathy's public key) via external means

Using e_{Cathy} (Cathy's public key), Alice can verify e_b (Bob's public key) because it is signed by d_{Cathy} (Cathy's private key)

This assumes

Alice has learned the correct public key for Cathy and Cathy signed the correct public key for Bob

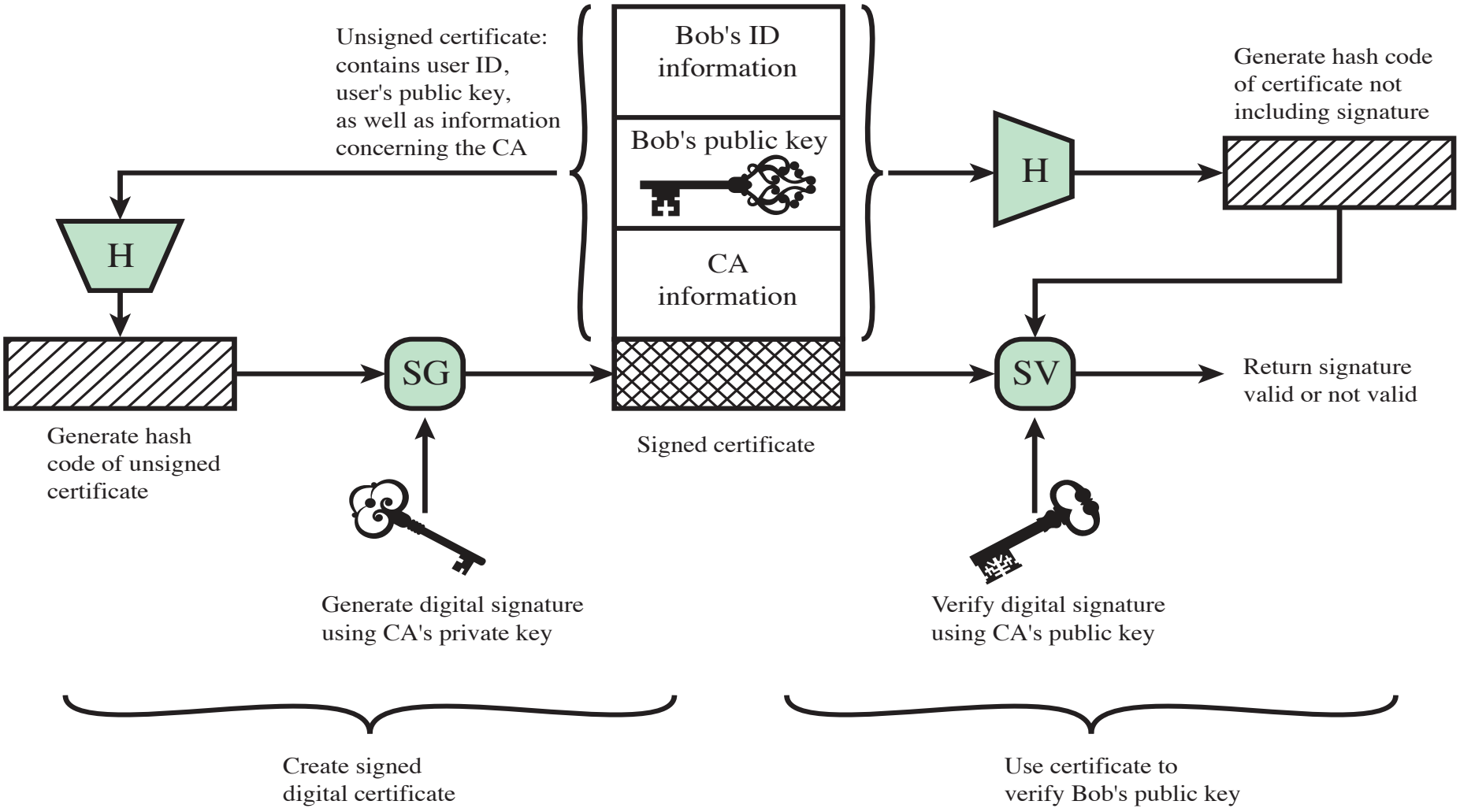


Figure 2.8 Public-Key Certificate Use

Heilmeier Questions

- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you succeed, what difference will it make?
- What are the risks?
- How much will it cost?
- How long will it take?
- What are the mid-term and final “exams” to check for success?