Encryption Methods:

- (**Diffie-Hellman** key exchange)
  - a method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
- **RSA** - Rivest, Shamir, and Adleman
  - 1978, public/private key algorithm, 1,024 to 4,096- bit keys (typically)

Authentication

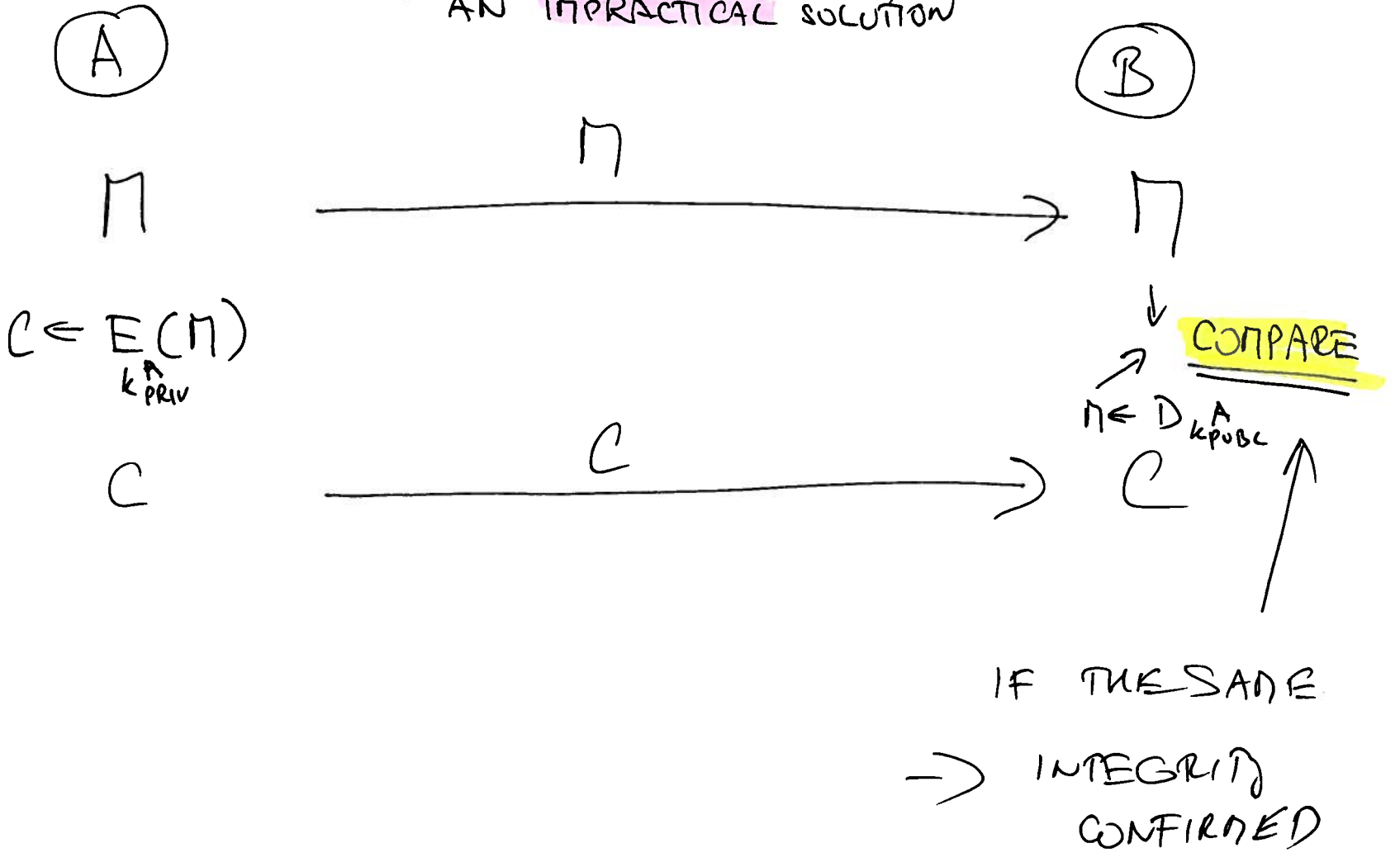
- Basic idea:
  - use public/private key cryptography
  - only possessor of private key could have encrypted something that decrypts using its public key
- Problem: **Replay Attack**
  - solution: use of a nonce
- Still unaddressed: We need a trusted way to obtain someone's public key

Message Integrity

- Basic idea:
  - use public/private key cryptography
  - send encrypted (with senders private key) hash of a message
  - if hash of the received message agrees with decrypted received hash, it is assumed that the message was not altered in transit
- Problems:
  - need a **cryptographic** hash function
  - need a public key distribution method

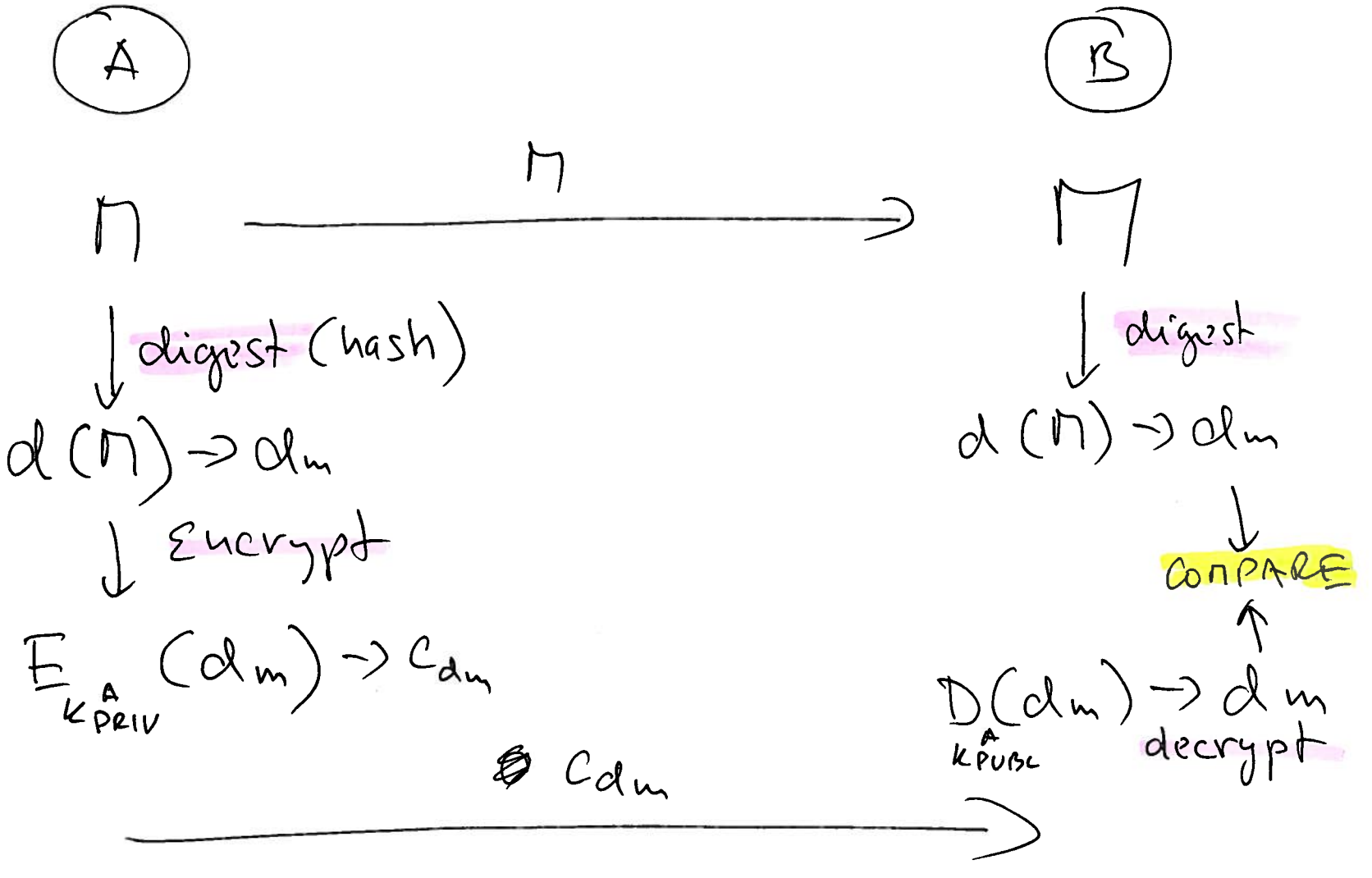
MESSAGE INTEGRITY

AN IMPRACTICAL SOLUTION



MESSAGE INTEGRITY

REAL SOLUTIONS



d(·) - digest function

Cryptographic Hash

- **MD5** - Message Digest Algorithm
  - 1992, R. Rivest, digest size 128 bits
- **SHA-1** - Secure Hash Algorithm
  - 1995, NSA, digest size 160 bits
  - SHA-2, SHA-3 competition at NIST