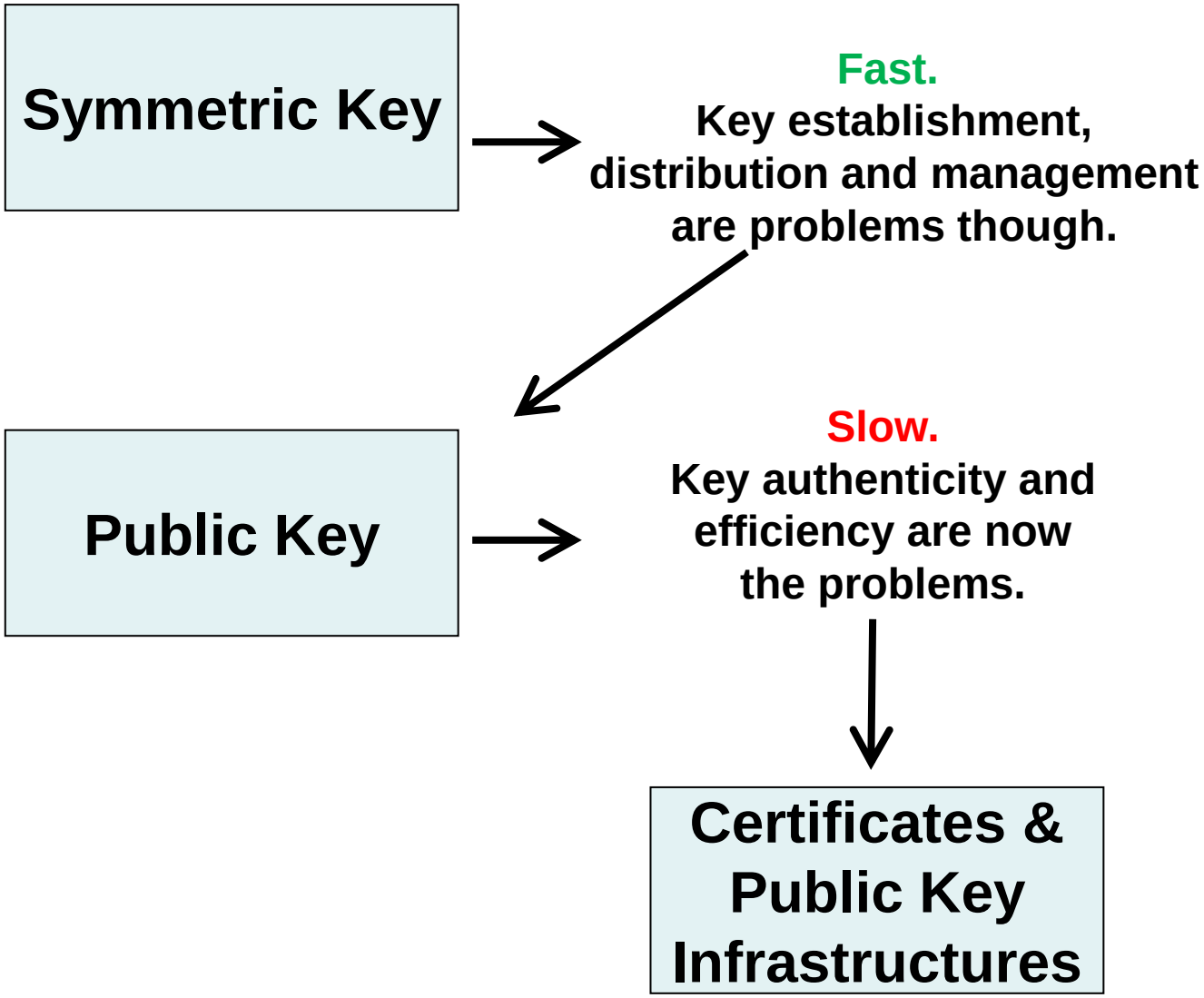
Secure Message Transmission



Hybrid System: PKC (with PKI) + one-time Symm Key

Hybrid approach

- AKE + symmetric key technique
- PKC + symmetric key technique

Message Encryption

- A and B completes an AKE protocol
  - A and B share a secret session key K
- A wants to send a message M to B

  $A \rightarrow B: E_K(M)$
- Achieve confidentiality
- Does encryption provide authenticity/integrity?
  - When M is a meaningful/structured message
  - When M is a random message

Random Message Encryption

Internal error control

- A and B share a secret key K

  $A \rightarrow B: E_K(M, H(M))$

- B believes that A sent the message, if the message can be obtained by decryption and H(M) = H(M)
- It provides confidentiality and (weak) authentication

Random Message Encryption

External error control

- A and B share a secret key K

  $A \rightarrow B: E_K(M), H(E_K(M))$

- B believes that A sent the message, if the message can be obtained by decryption and $H(E_K(M)) = H(E_K(M))$
- Insecure!

Message Authentication Code (MAC)

- Cryptographic checksum
  - E.g. HMAC
- Assume C(•) is a MAC function
- A and B share a secret key K

  A → B: M, T = C(K,M)
- B checks if C(K,M) = T
- Achieve authentication only

MAC Then Encrypt

- Assume C(•) is a MAC function
- A and B share two secret keys K1, K2

  $A \rightarrow B: E_{K2}(M, C(K1,M))$

- B decrypts it and checks if

  $C(K1,M) = C(K1,M)$

- Achieve authentication and confidentiality

Note that for B → A, a new pair of MAC and encryption keys should be used

Encrypt Then MAC

- Assume C(•) is a MAC function
- A and B share two secret keys K1, K2

  $A \rightarrow B: E_{K2}(M), C_{K1}(E_{K2}(M))$

- B decrypts it and checks if

  $C_{K1}(E_{K2}(M)) = C_{K1}(E_{K2}(M))$

- Achieve authentication and confidentiality

Note that for B → A, a new pair of MAC and encryption keys should be used

Message Transmission by PKC

- Sometimes two users may not be able to do an AKE to establish a secure session key
  - E.g. email
- How to do secure message transmission in this setting?
  - Hybrid encryption

Message Encryption by Hybrid Encryption

- B has a pair of key (d', e'), where d' is private and e' is public

  $A \rightarrow B: PKE_{e'}(K), SKE_K(M)$

- It provides confidentiality only

Sign Then Encrypt

- A has a pair of keys (d, e), where d is private and e is public
- B has a pair of keys (d', e'), where d' is private and e' is public

$$A \rightarrow B: E_{e'}(K) , SKE_K(M, Sign_d(M))$$

- B believes that A sent the message, if the message and signature can be verified with e.
- A believes that only B can receive the signed M
- It provides confidentiality, authentication, and sender non-repudiation