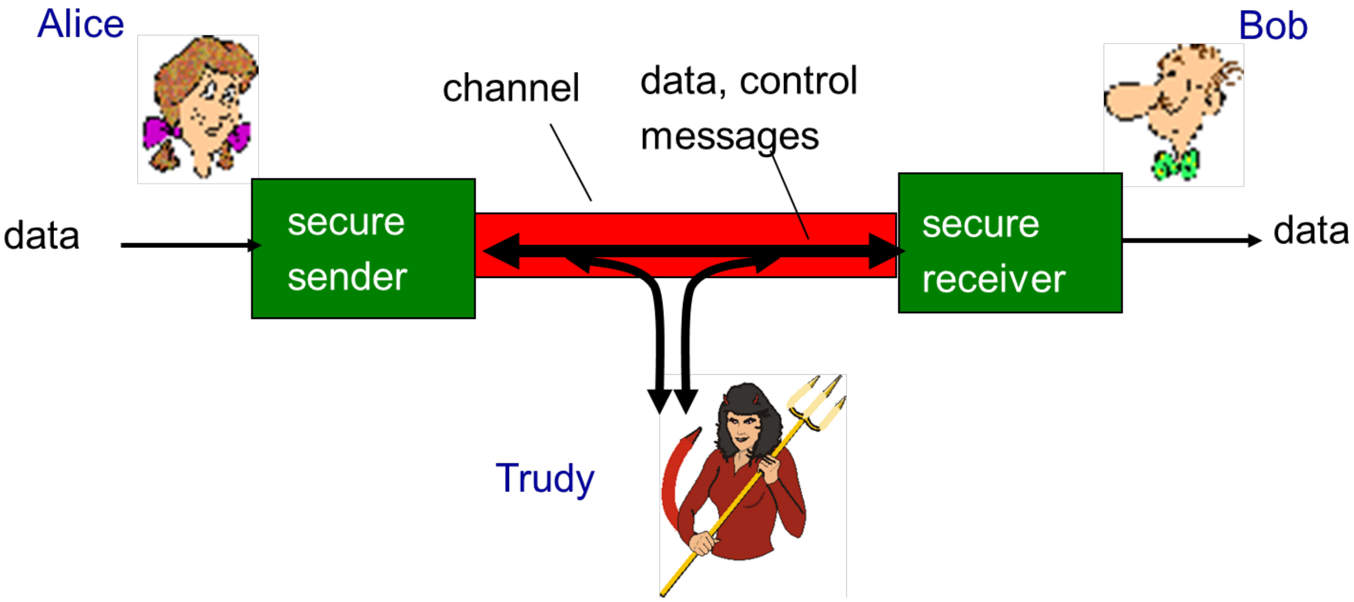
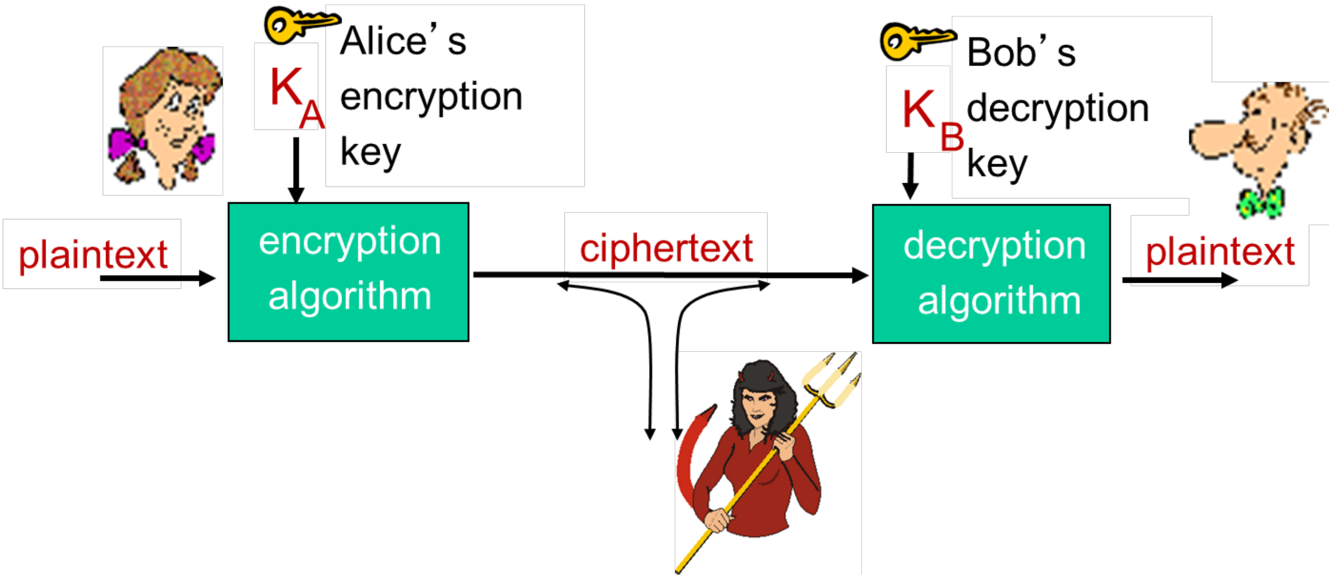
Security services

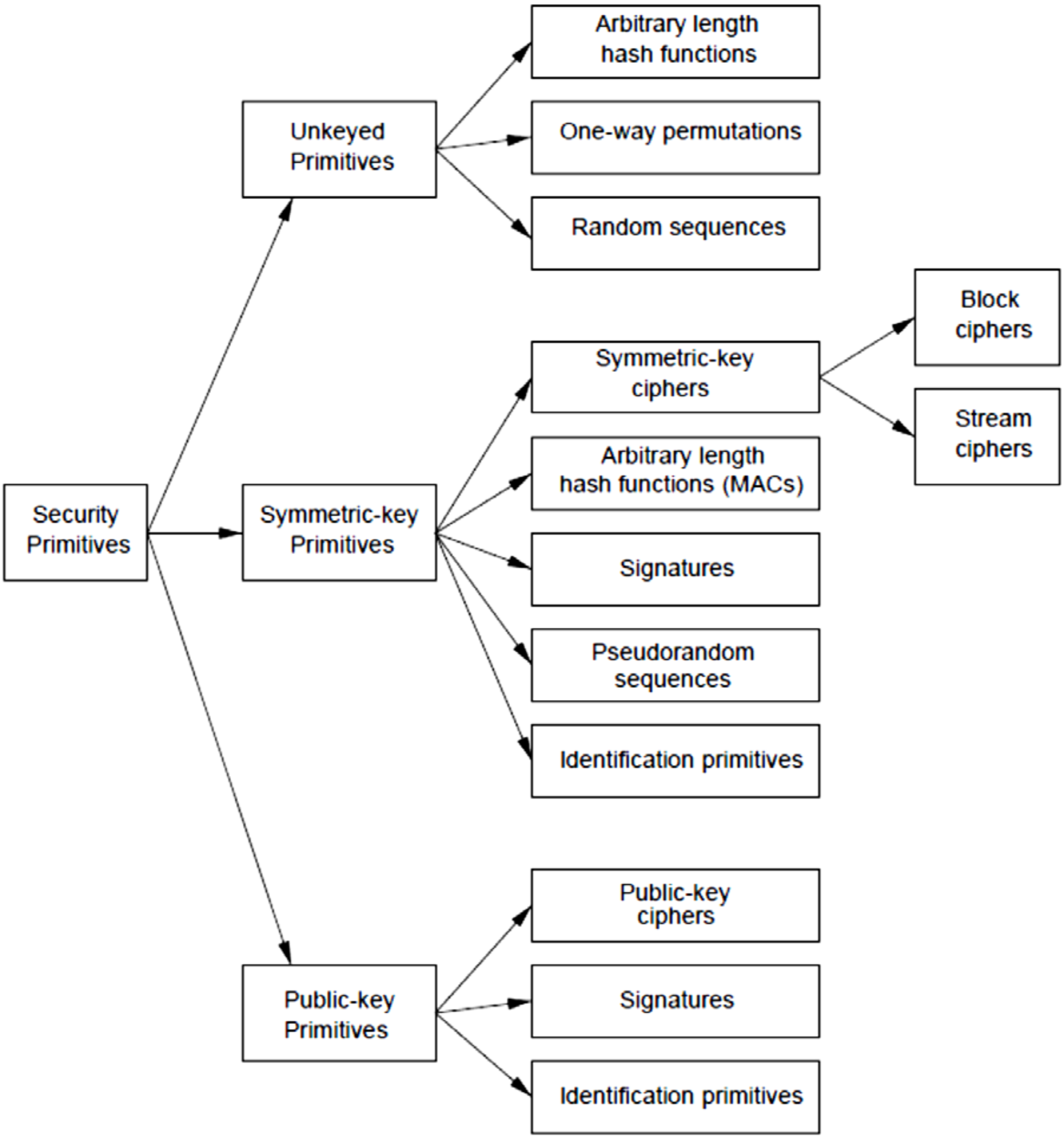


- Who are *real-life* Bobs and Alices?

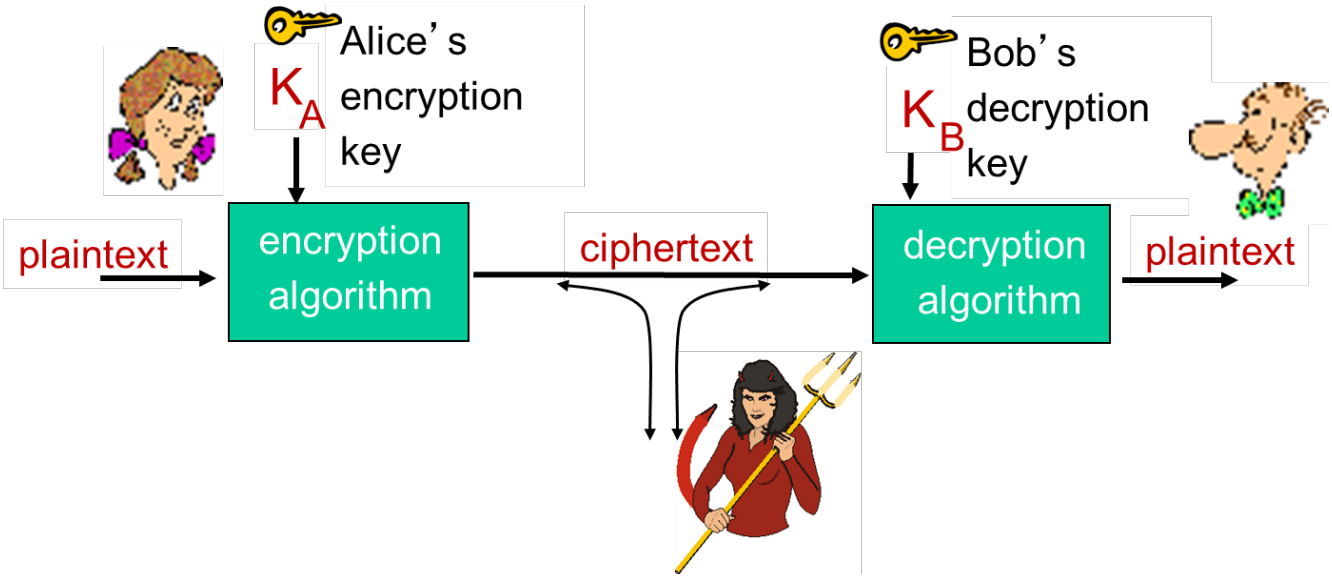
The language of cryptography



Taxonomy of Crytographic Primitives



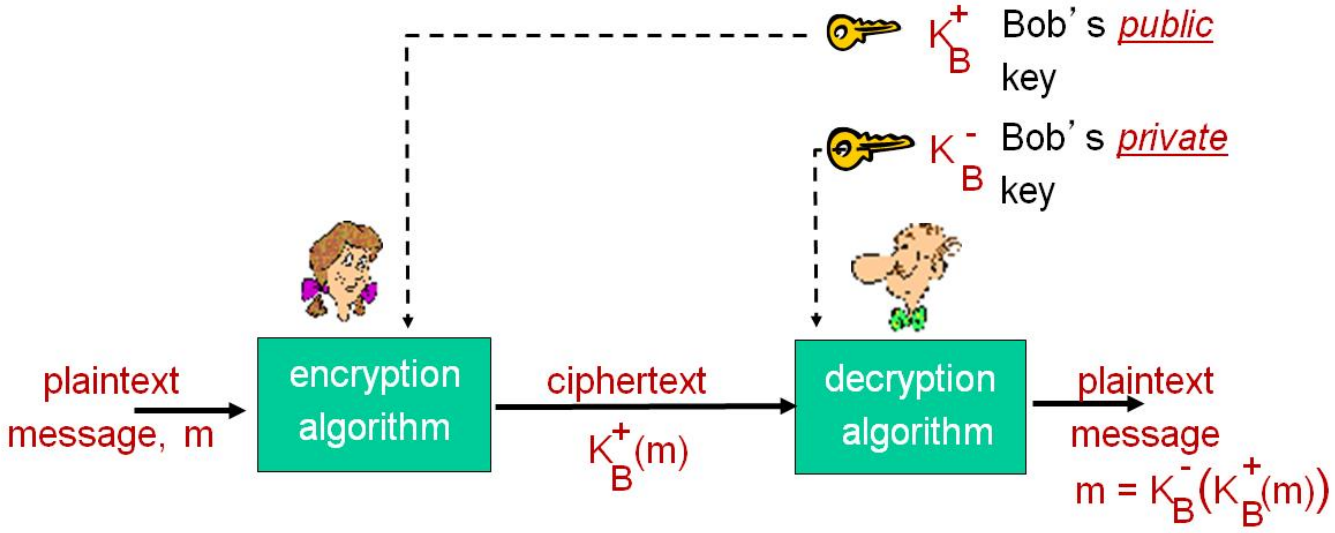
Symmetric key Encryption



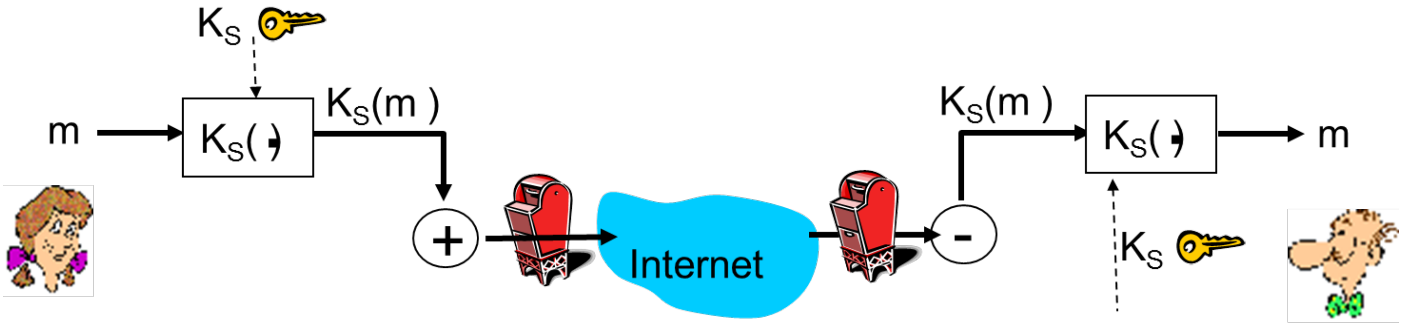
- Block cipher =>

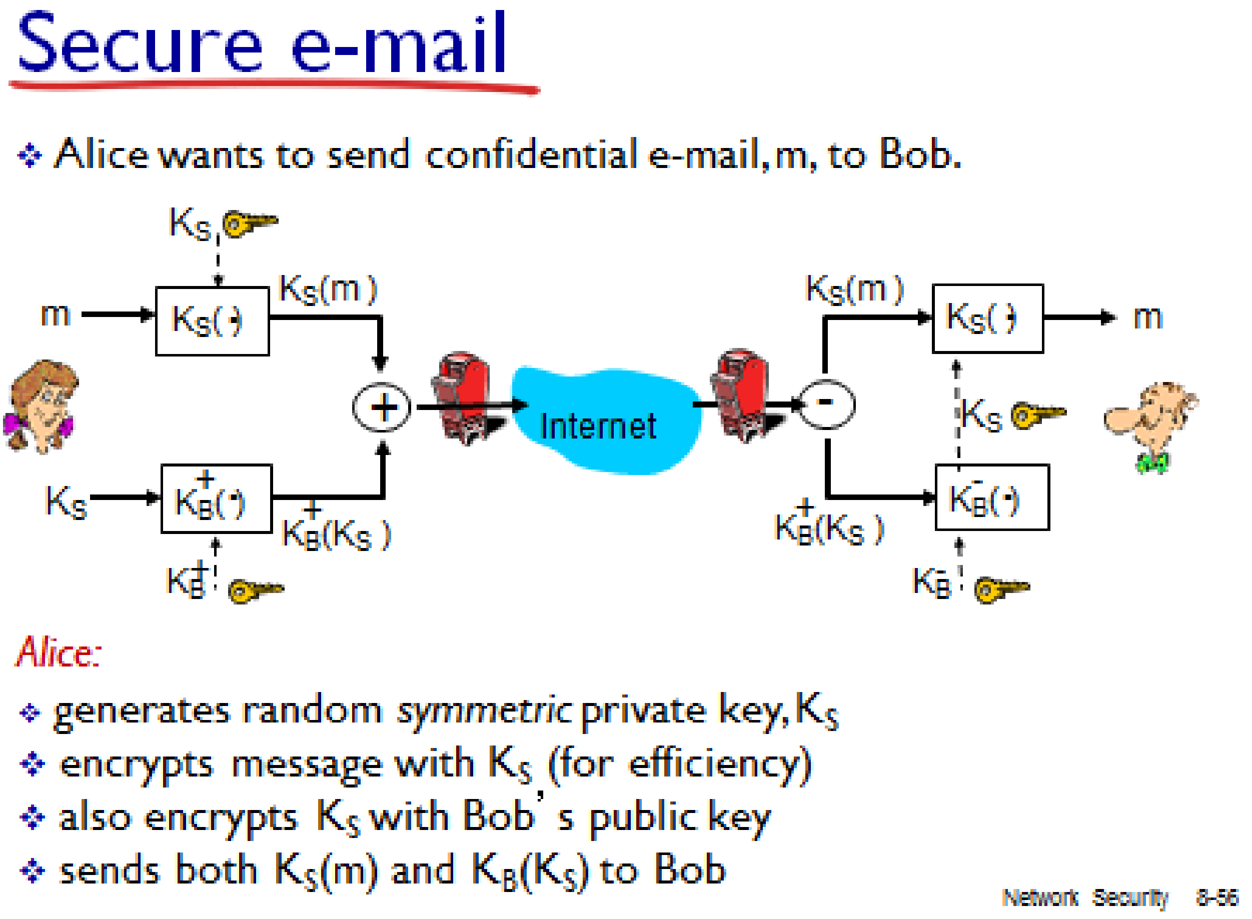
- Stream cipher =>

Public key cryptography



Secure e-mail





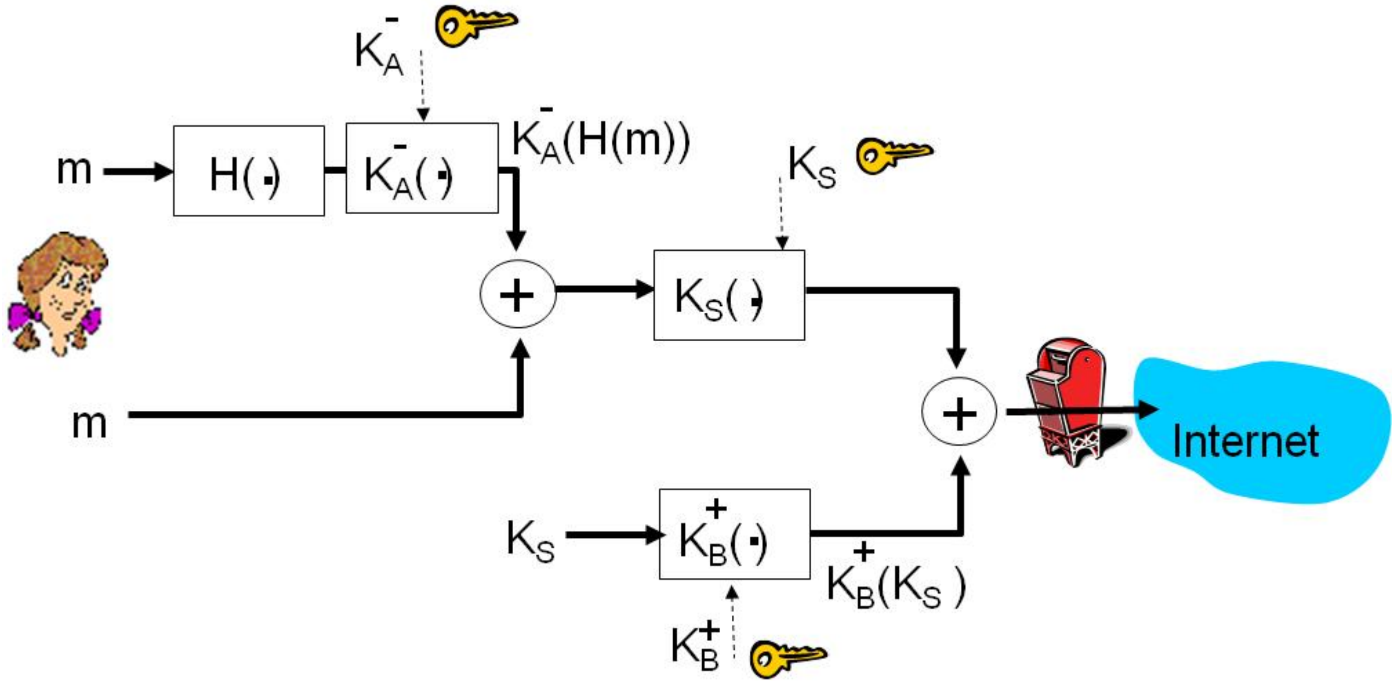
Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

Alice:

- generates random *symmetric* private key, K_S
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob

Confidentiality, Message Integrity, Authentication


K_A^-
m
$H(\cdot)$
$K_A^-(\cdot)$
$K_A^-(H(m))$
K_S
+
$K_S(\cdot)$
m
+
Internet
K_S
$K_B^+(\cdot)$
$K_B^+(K_S)$
K_B^+