



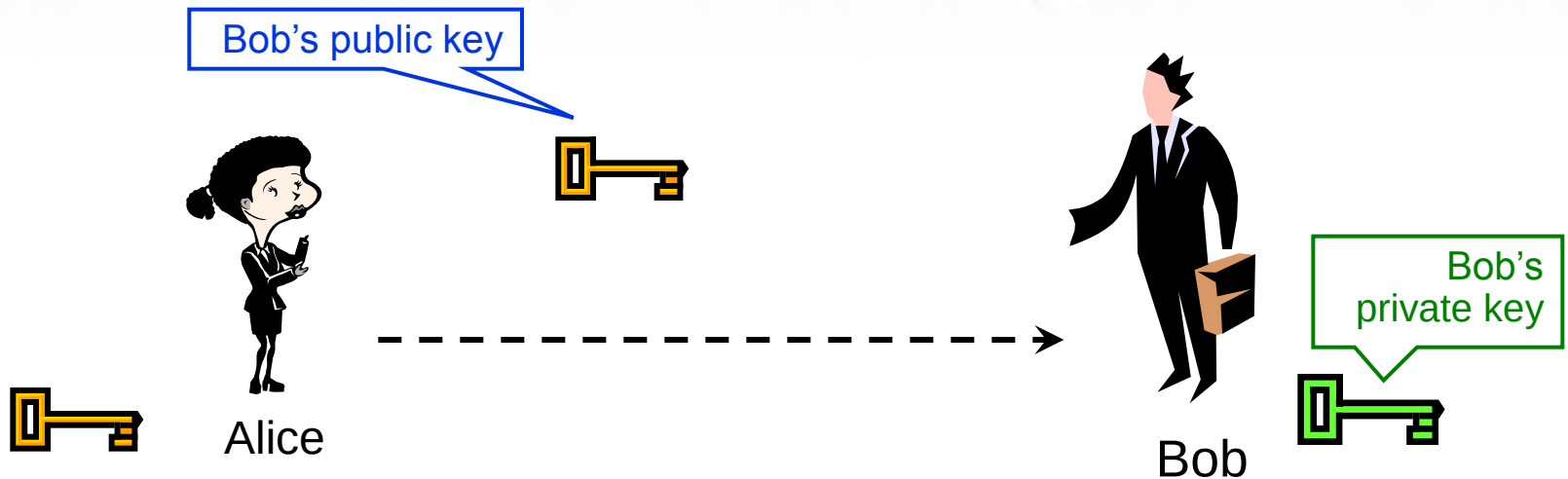
# **Information security**

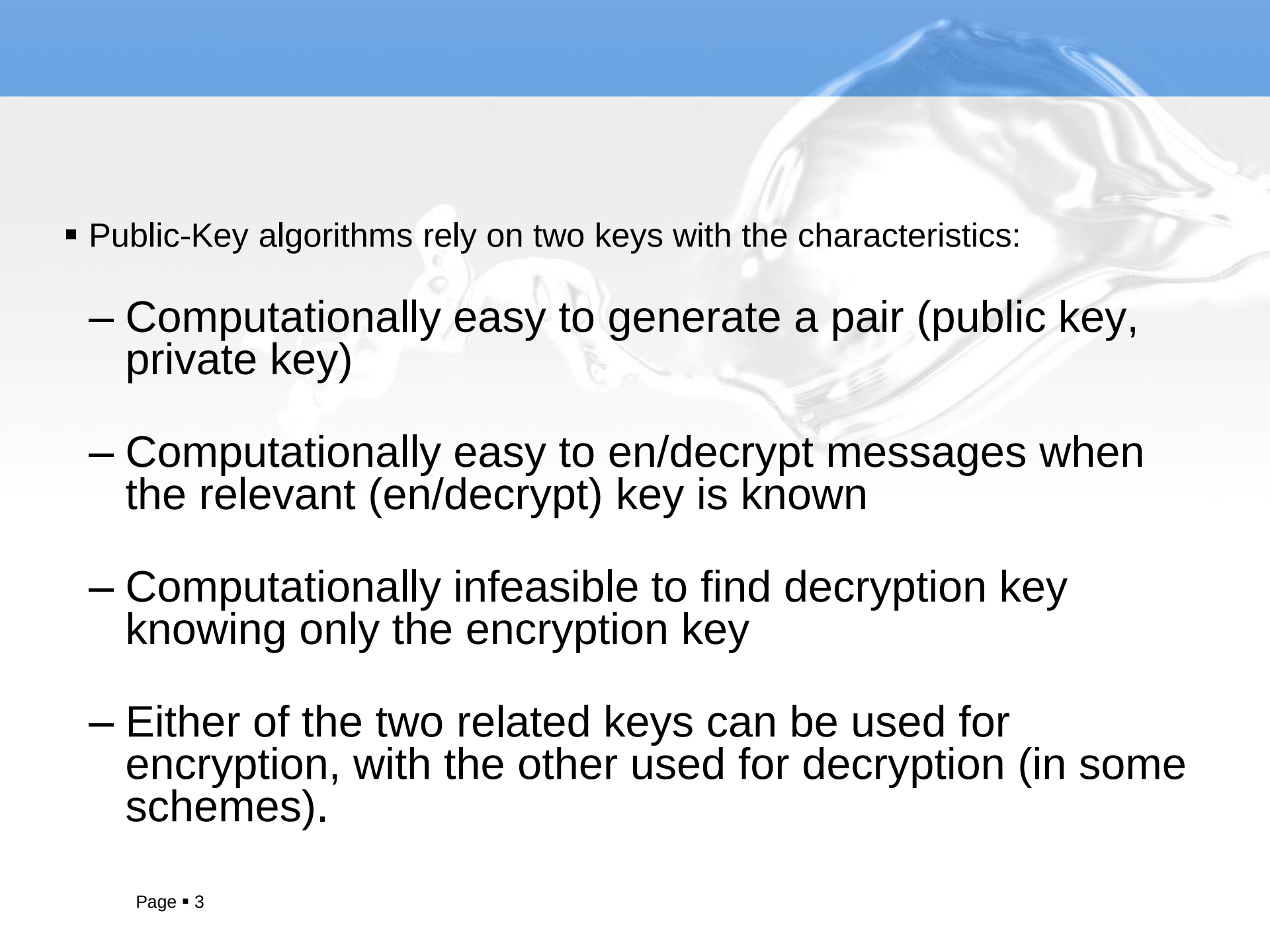
*Lecture-6*

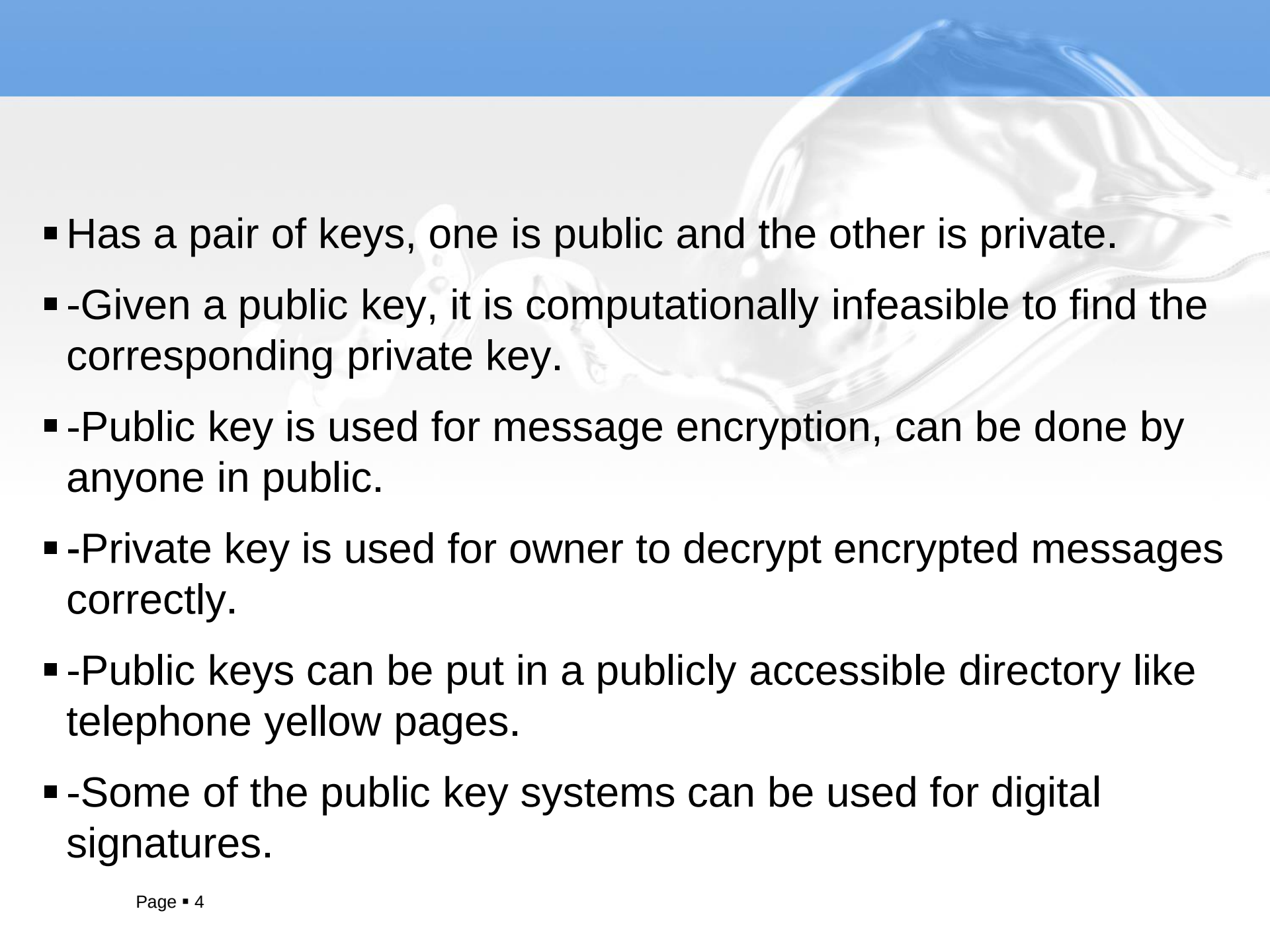
*Eng. Taghreed Harfoush*

# Public-Key Cryptography

- Everybody knows Bob's **public key**
- Only Bob knows the corresponding **private key**



- 
- Public-Key algorithms rely on two keys with the characteristics:
    - Computationally easy to generate a pair (public key, private key)
    - Computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
    - Computationally infeasible to find decryption key knowing only the encryption key
    - Either of the two related keys can be used for encryption, with the other used for decryption (in some schemes).

- 
- Has a pair of keys, one is public and the other is private.
  - -Given a public key, it is computationally infeasible to find the corresponding private key.
  - -Public key is used for message encryption, can be done by anyone in public.
  - -Private key is used for owner to decrypt encrypted messages correctly.
  - -Public keys can be put in a publicly accessible directory like telephone yellow pages.
  - -Some of the public key systems can be used for digital signatures.

# Public-Key Applications

- Three major categories:
  - Encryption/decryption (provide secrecy)
  - Digital signatures (provide authentication)
  - Key exchange (of session keys)
- Some algorithms are suitable for all uses, others are specific to one

# Encryption for confidentiality

- Anyone can encrypt a message
  - With symmetric crypto, must know secret key to encrypt
- Only someone who knows private key can decrypt
- Key management is simpler (maybe)
  - Secret is stored only at one site: good for open environments

# Digital signatures for authentication

- Can “sign” a message with your private key

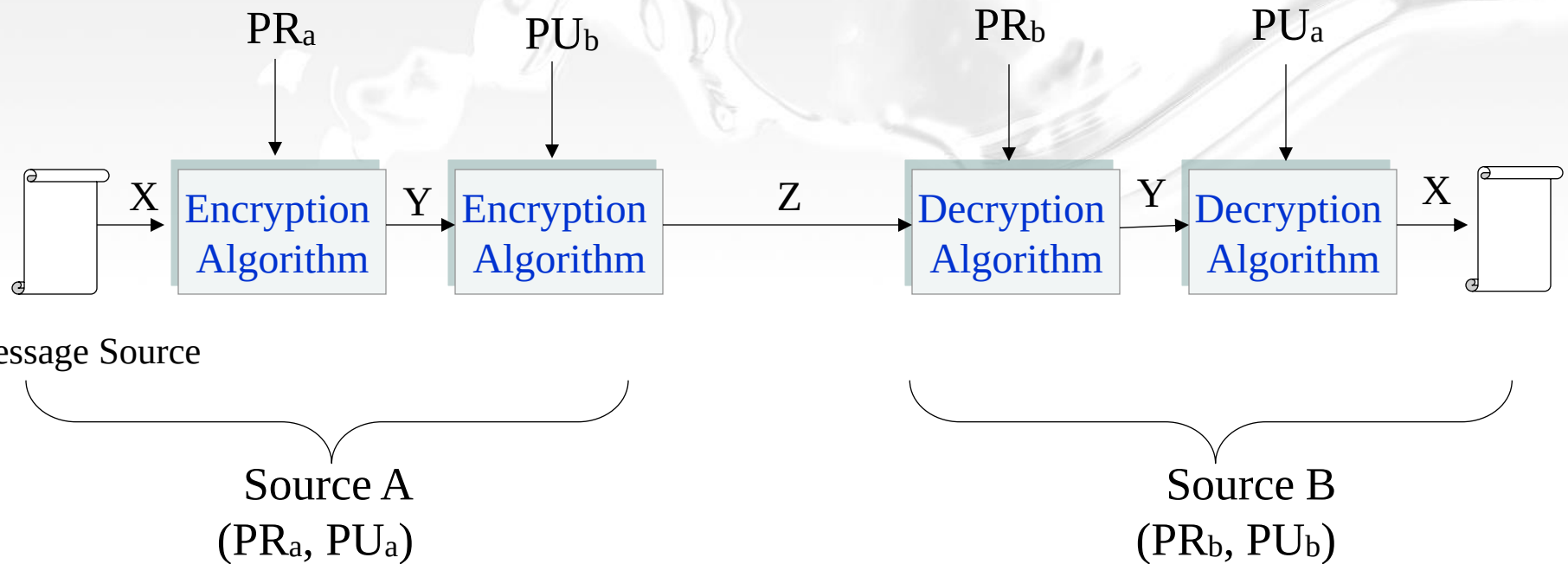
# Session key establishment

- Exchange messages to create a secret **session key**
- Then switch to symmetric cryptography (**why?**)



# Public-Key Cryptosystem

## Authentication and Confidentiality



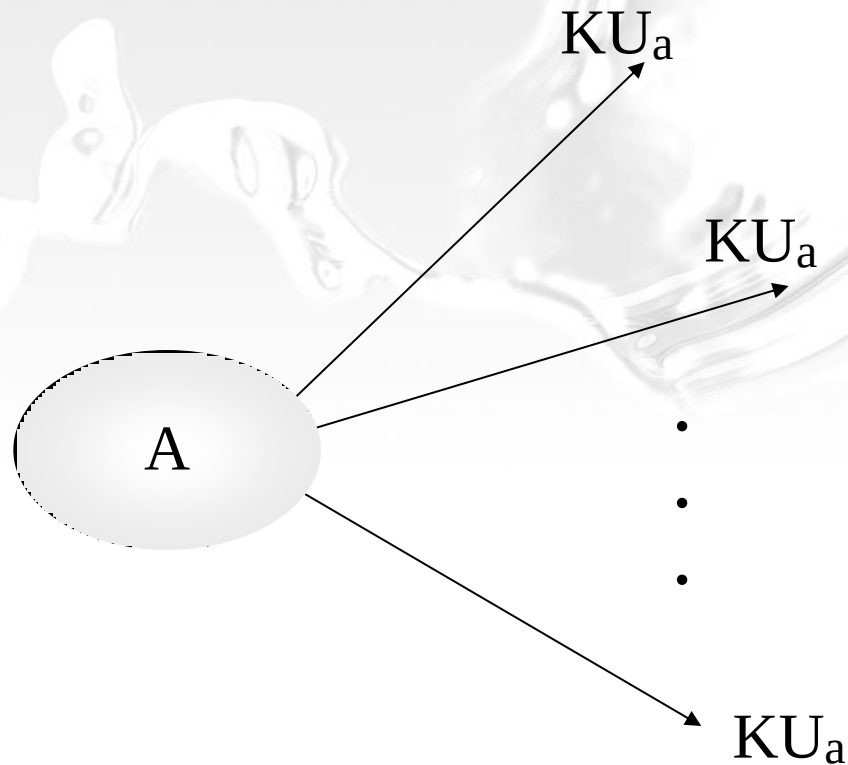


# Public Key Distribution

# General schemes:

- Public announcement
- Publicly available directory
- Public-key authority
- Public-key certificates

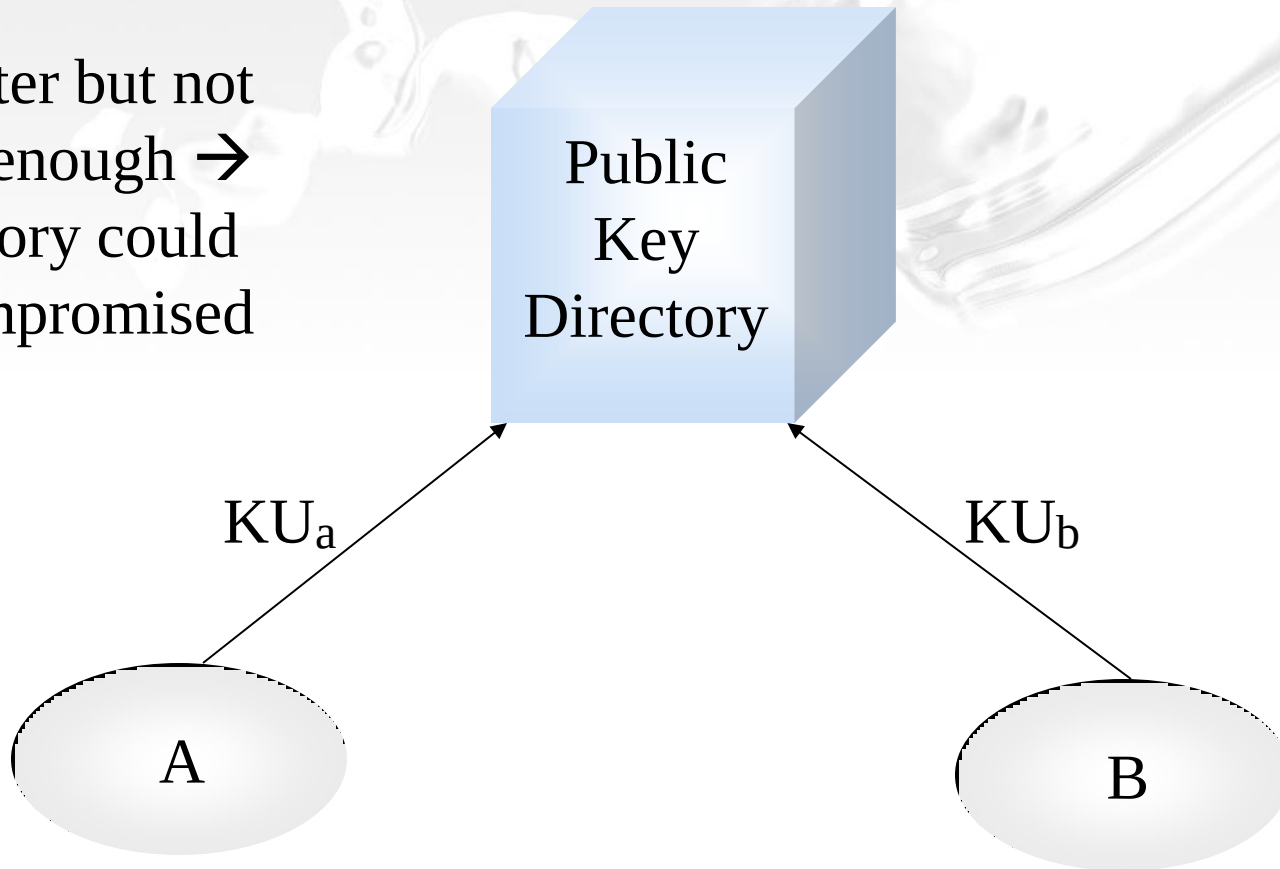
# Public announcement



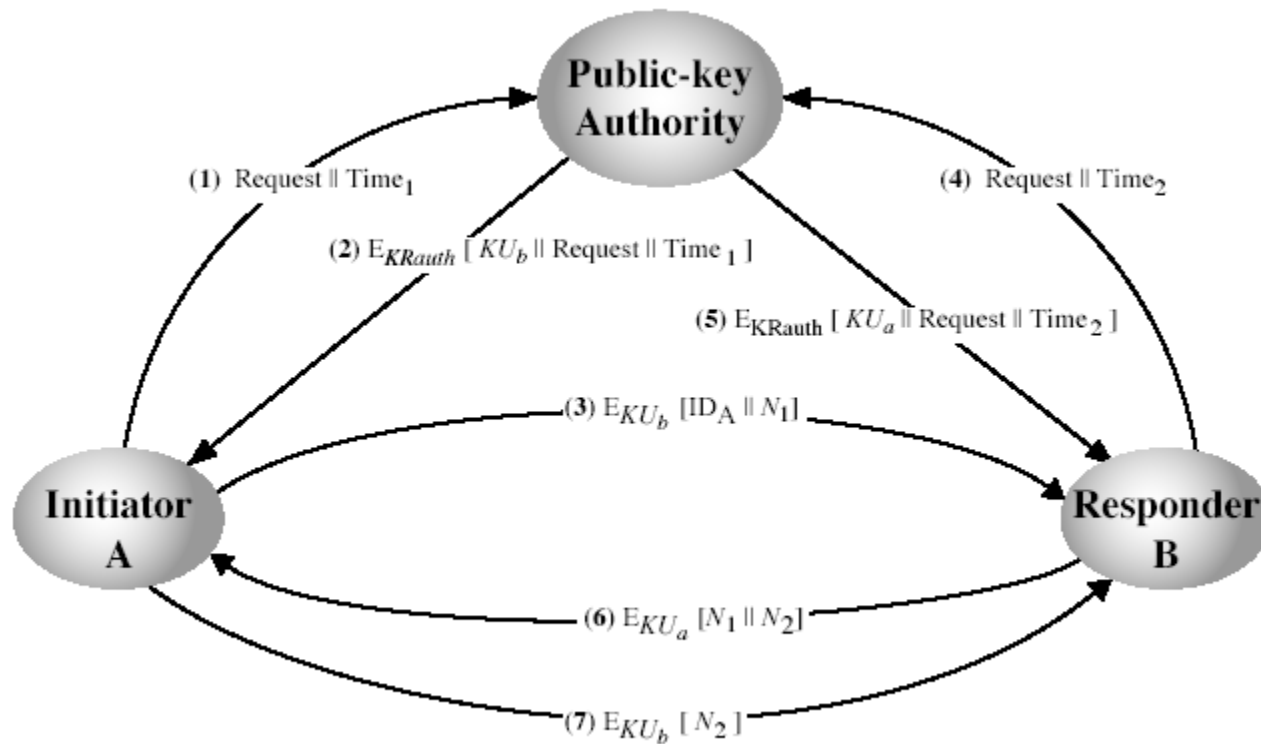
Bad: Uncontrolled  
distribution  $\rightarrow$  easy to forge

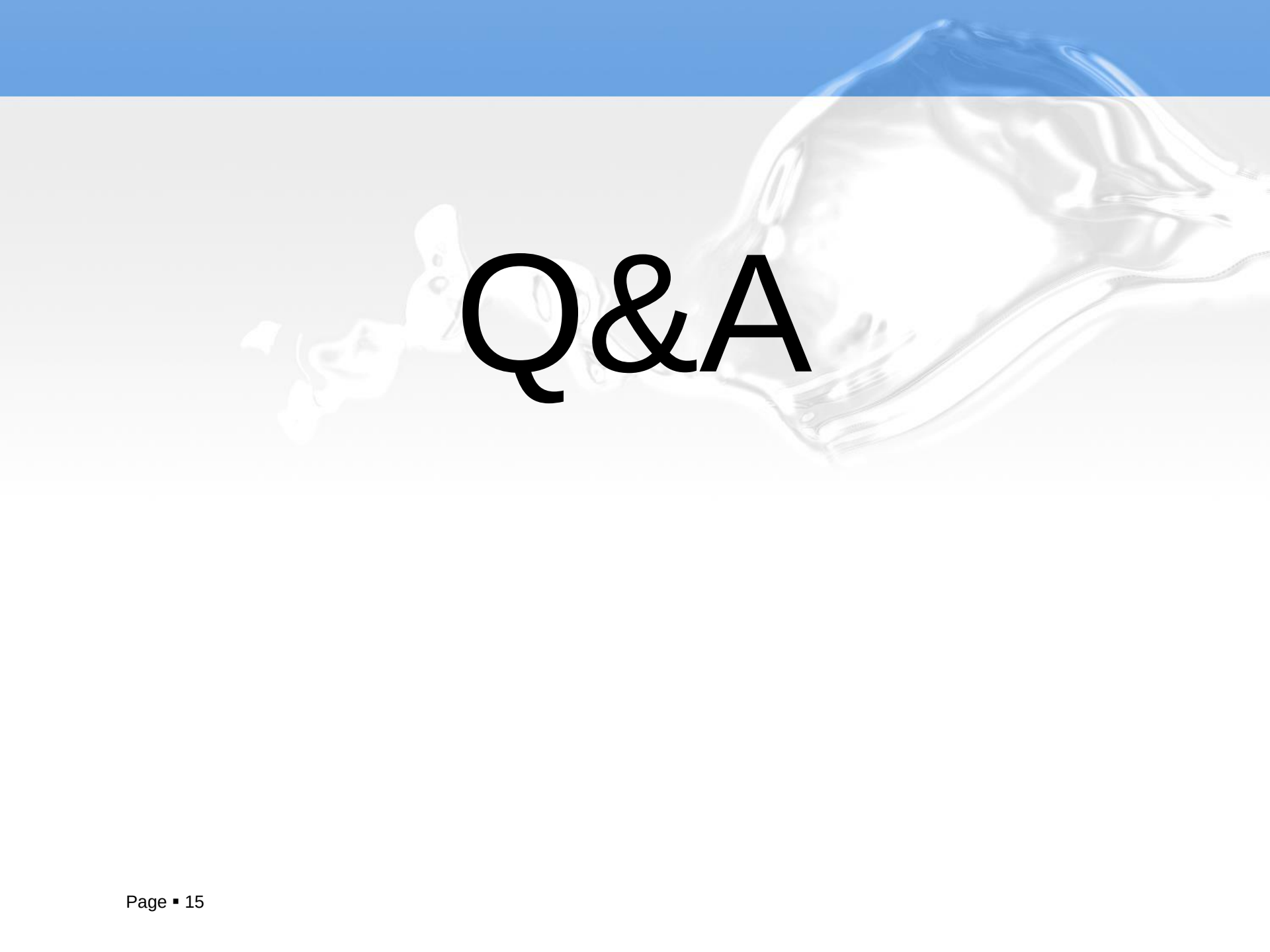
# Publicly available directory

Better but not  
Good enough →  
Directory could  
Be compromised



# Public-Key Authority





# Q&A