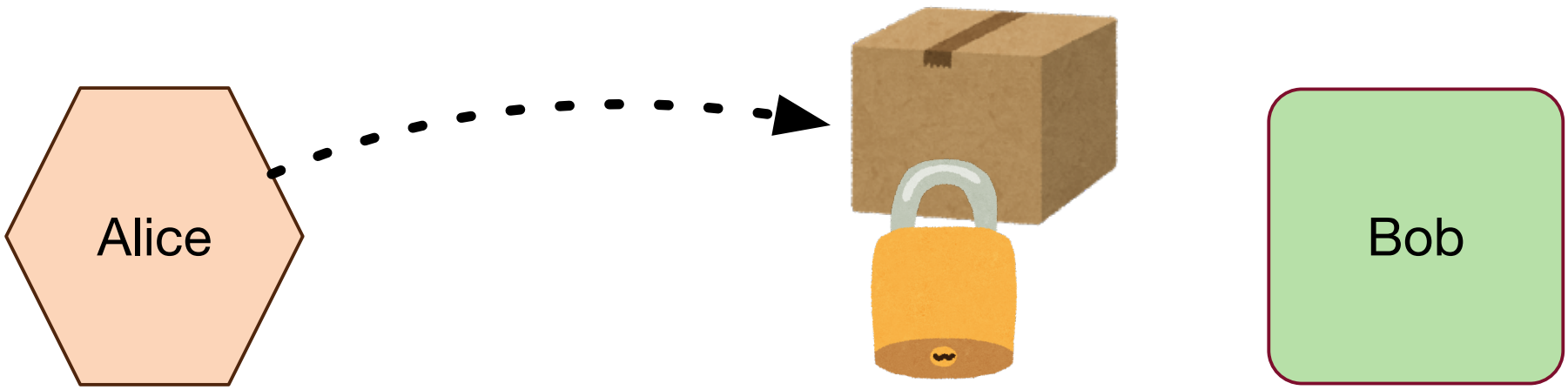
Public-key cryptography
公開鍵暗号

計算科学演習

陰山

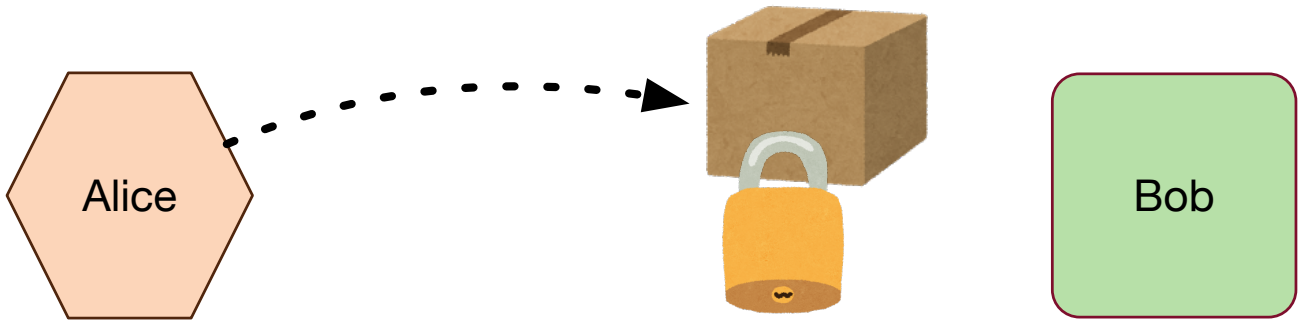
2017.04.13

Encrypted message

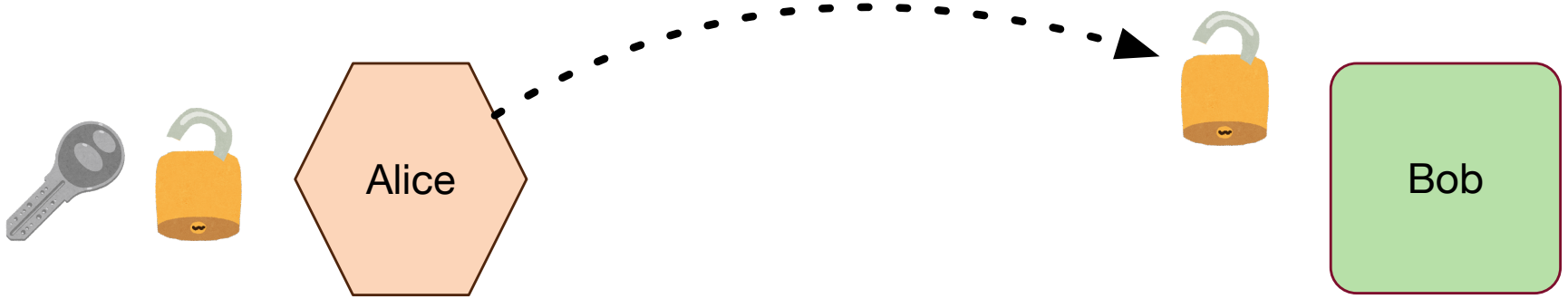


Symmetric-key encryption 共通鍵暗号

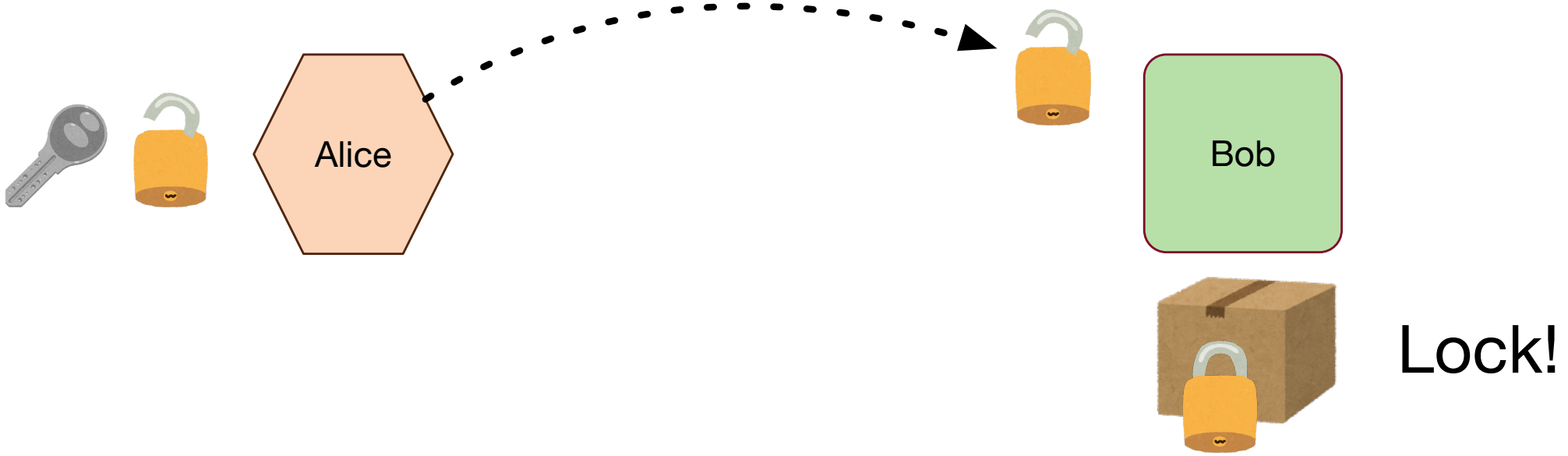
- E.g., Caesar's cipher
- kobe ⇒ ptgj (shift for 5 letters in alphabet)
- abcdefghijklmnopqrstuvwxyz



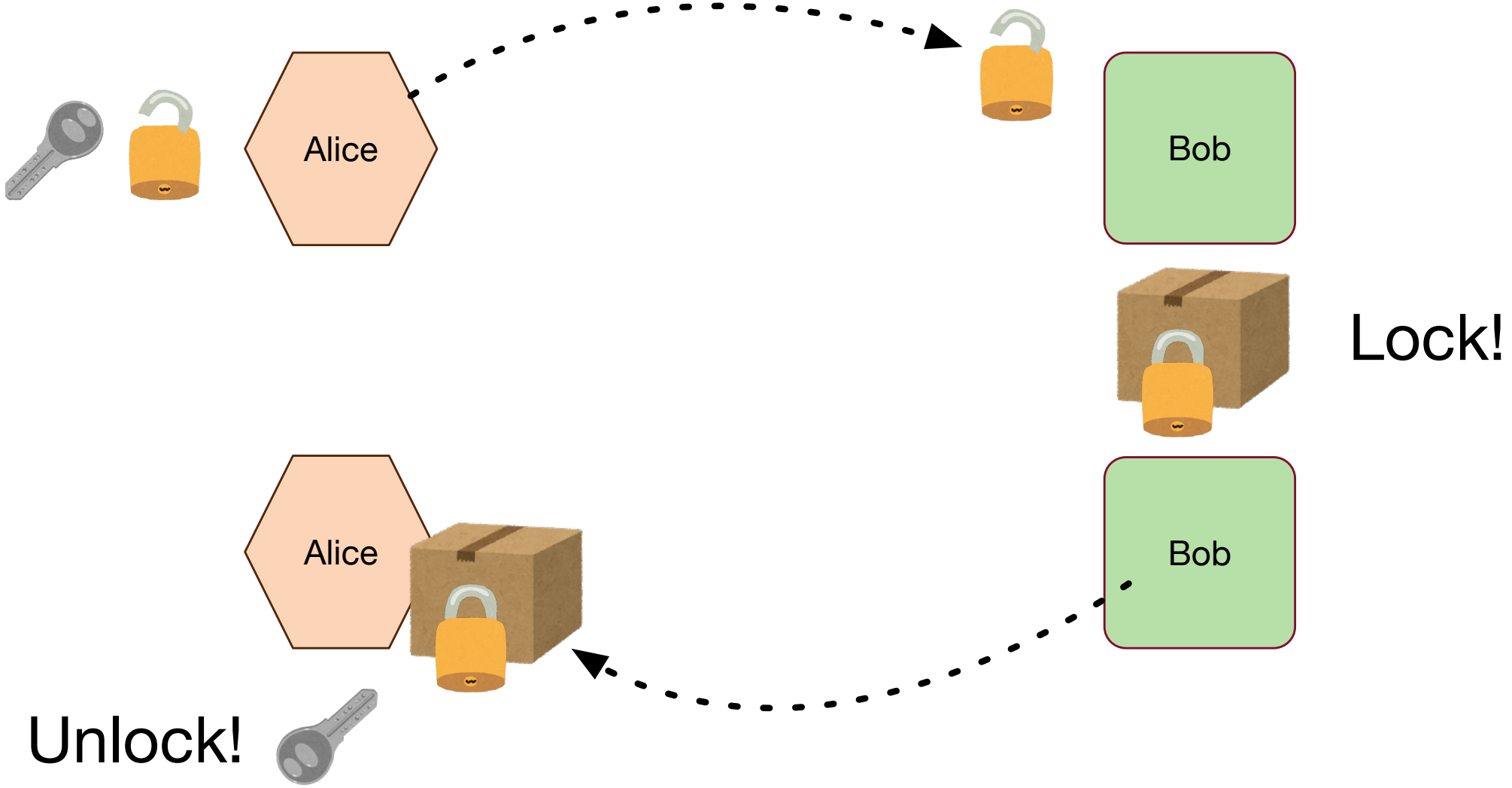
Public-key cryptography 公開鍵暗号



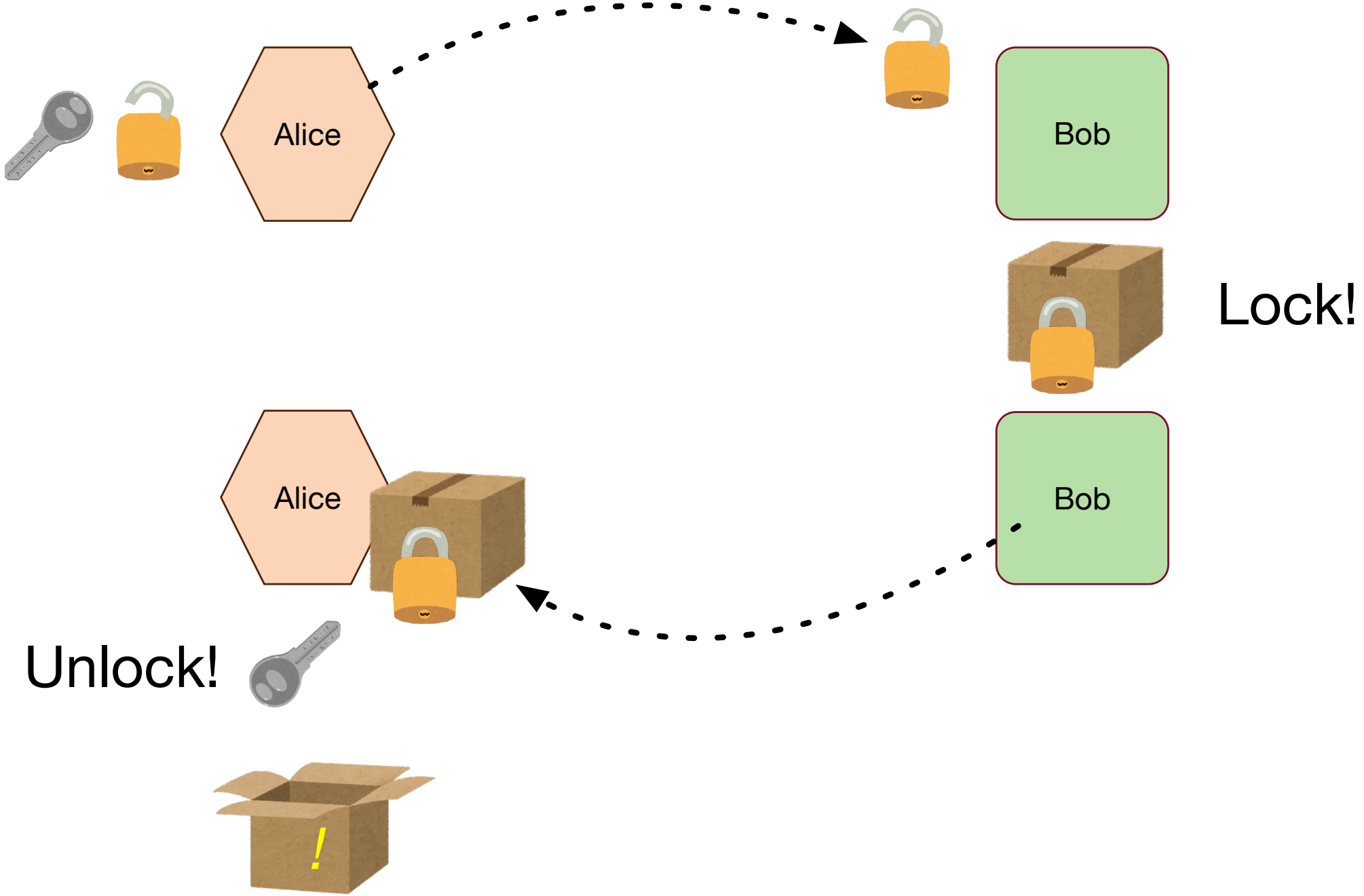
Public-key cryptography 公開鍵暗号



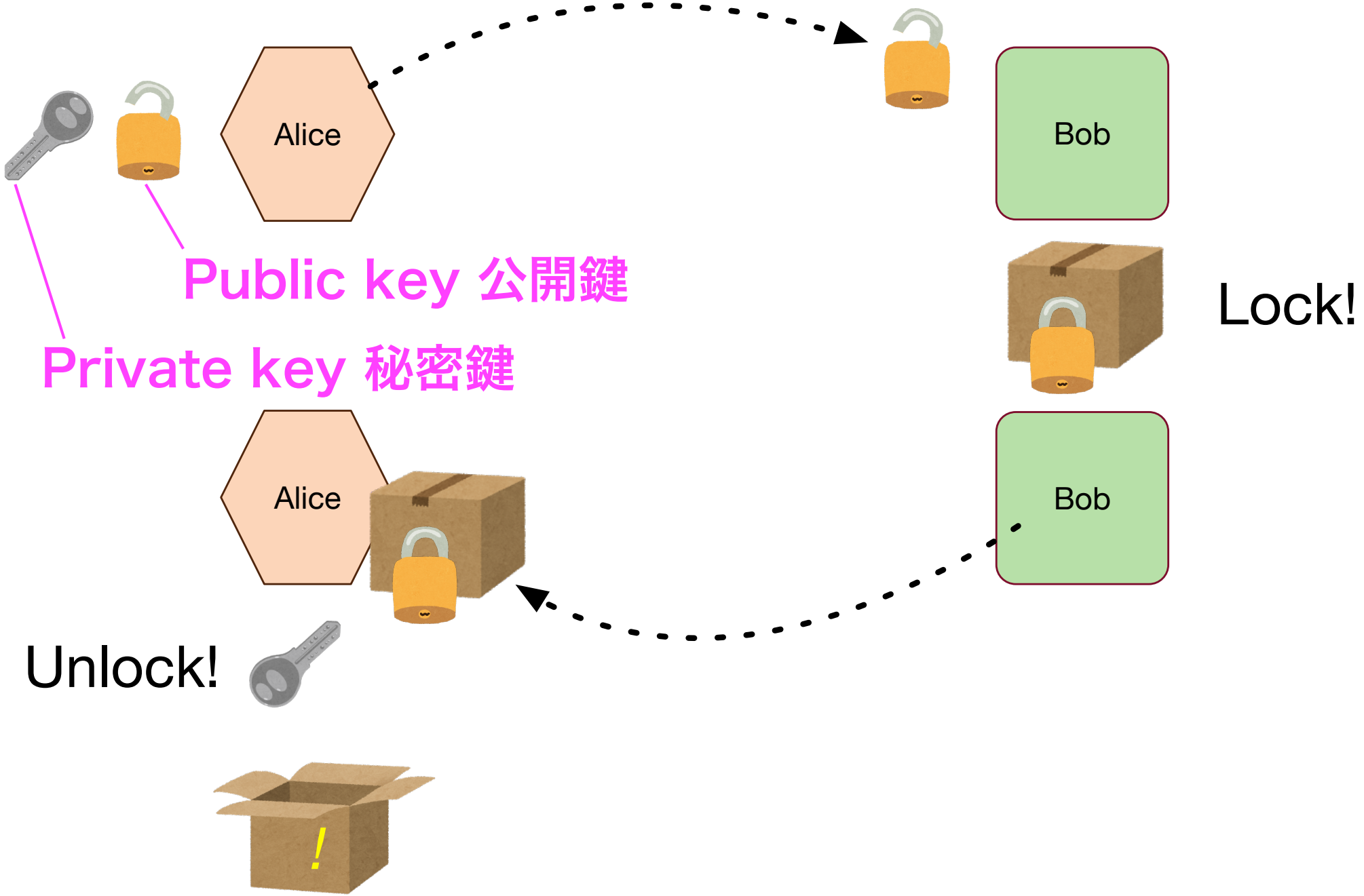
Public-key cryptography 公開鍵暗号



Public-key cryptography 公開鍵暗号



Public-key cryptography 公開鍵暗号



Note

- You can release your public key, but you must not release your private key.
    - 公開鍵は公開可。しかし、秘密鍵を公開してはいけない。
- You must not send your private key by email.
    - 秘密鍵をメール等で送ってはいけない。