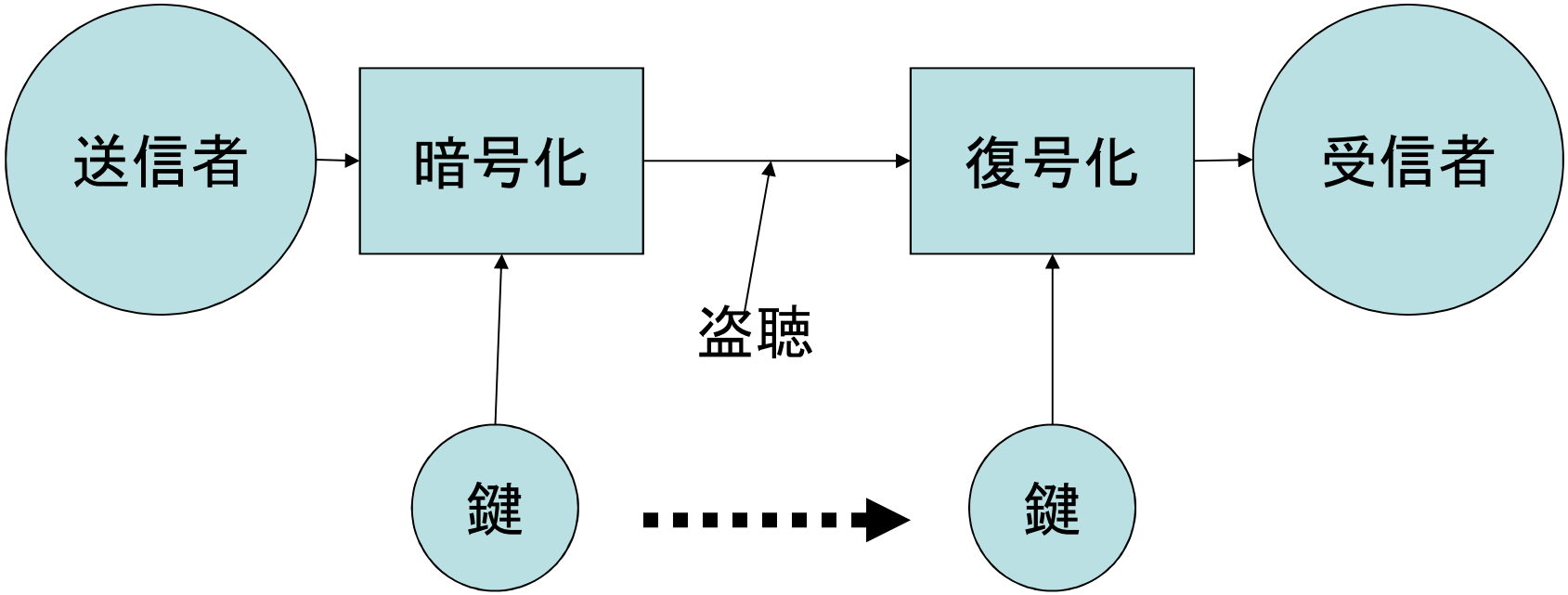
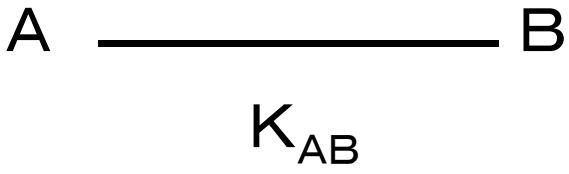
従来の暗号の問題点（1）



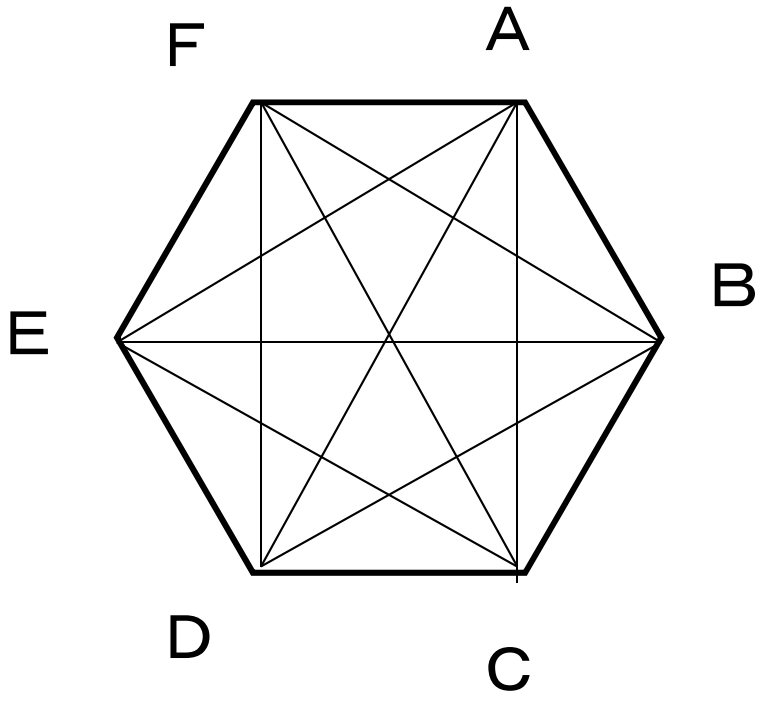
あらかじめ秘密に伝えないといけない

従来の暗号の問題点（2）



ユーザ数＝2の場合、
鍵の数＝1

ユーザ数n人では、鍵の数は
${}_nC_2$となる（1ユーザ当りn-1の
鍵を秘密に管理する必要あり）

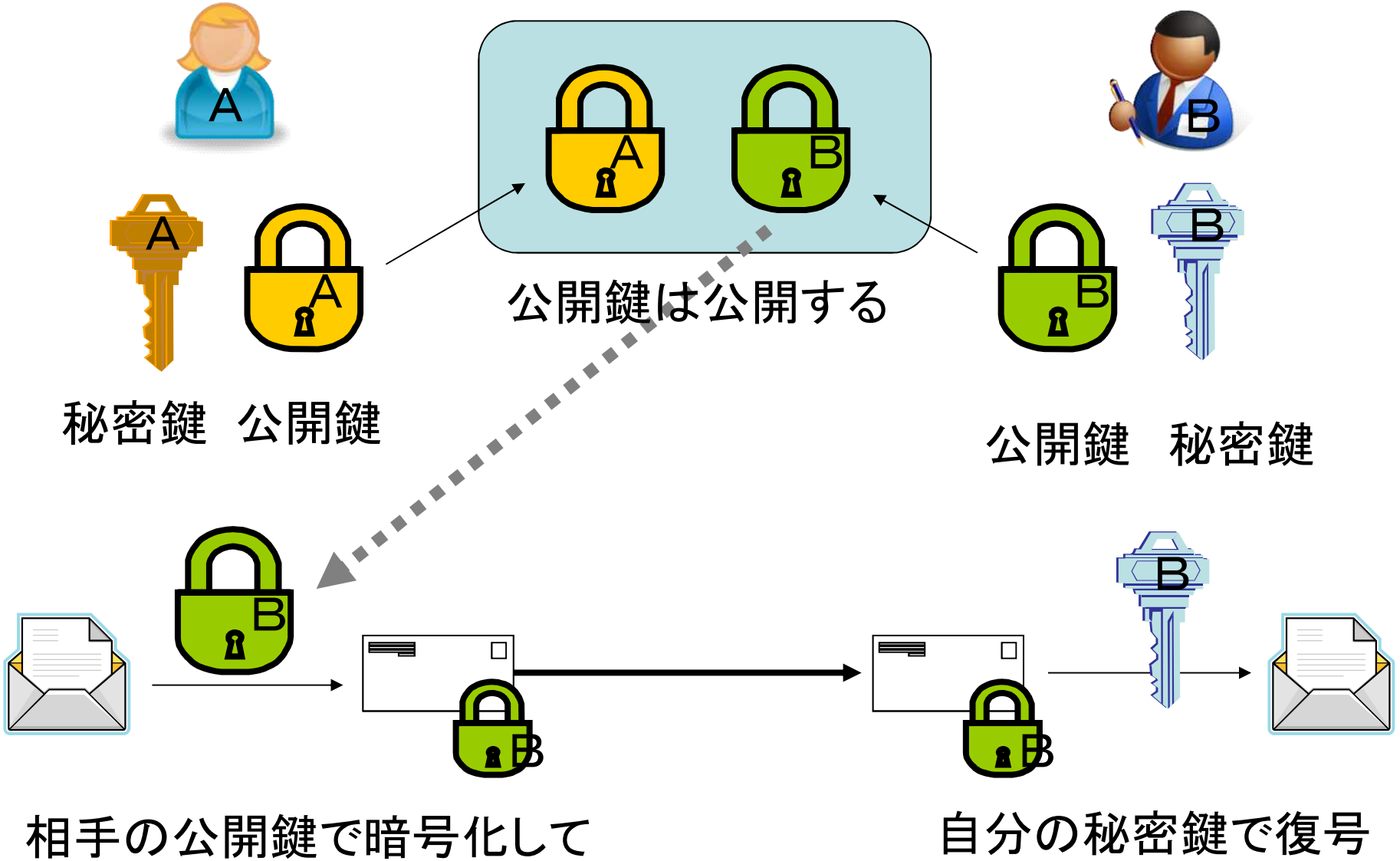


ユーザ数＝8では、
鍵の数＝28

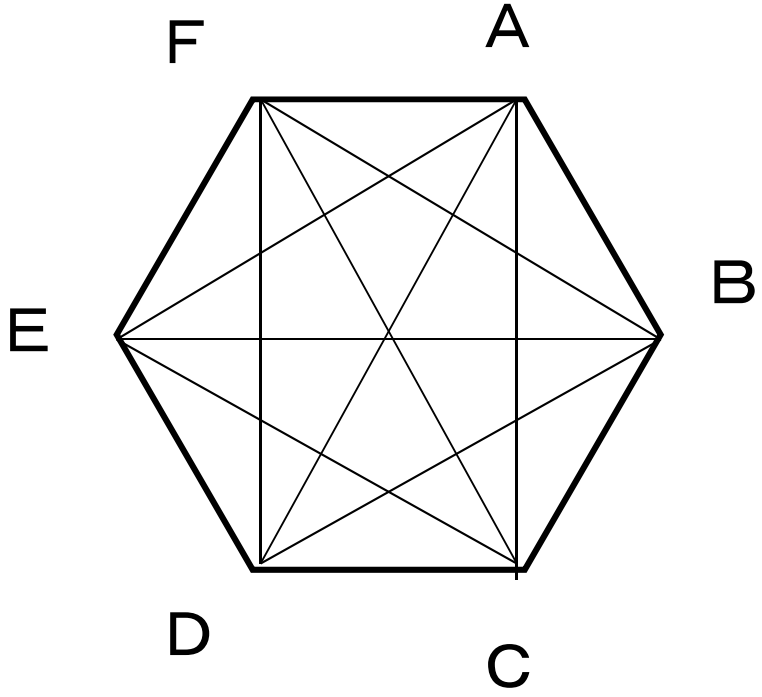
公開鍵暗号

- 1976年、DiffieとHellmanによりその概念が示された
- 公開鍵暗号方式の特徴：
  - 鍵の配送が容易
  - 秘密に保持する鍵の種類が少ない
  - 認証機能がある
- RSA方式が最もひろく使用されている方式
- WWWや電子メールの暗号、認証を行うために広く用いられている

公開鍵暗号とは


A
A
A
秘密鍵　公開鍵
公開鍵は公開する
B
B
B
公開鍵　秘密鍵
B
B
B
B
相手の公開鍵で暗号化して
自分の秘密鍵で復号

公開鍵暗号の利点



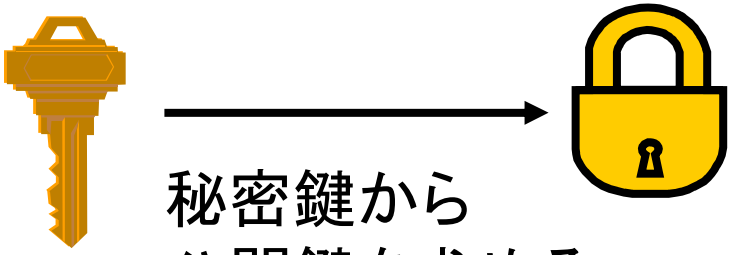
あらかじめ安全な通信チャンネル
を用いて、鍵を共有する必要なし

ユーザ数が多くなっても、
各ユーザが秘密に管理する
鍵は、自分の秘密鍵のみ。

→不特定多数の相手と通信をするネットワーク社会では
必要不可欠な技術

公開鍵暗号の数学的原理

公開鍵から
秘密鍵を求める
のは非常に困難



秘密鍵から
公開鍵を求める
のは容易

一方向性関数の利用
$y \leftarrow f(x)$の計算は容易だが、
$f^{-1}(y) \rightarrow x$の計算は非常に困難

公開鍵暗号を作るには、
「落し戸付き」一方向性関数が必要
$f^{-1}(y) \rightarrow x$の計算は非常に困難だが
ある情報を知っている者には簡単