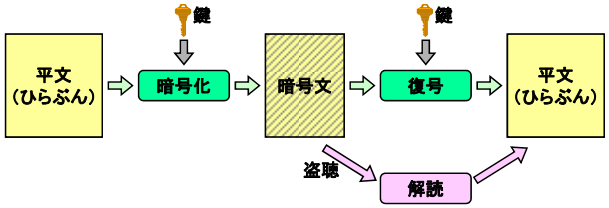
# 3. 暗号技術と認証



## 暗号とは



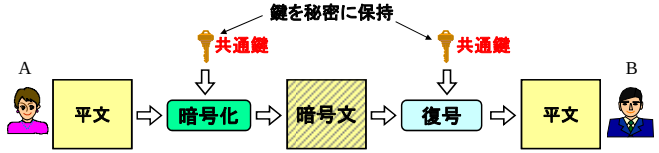

**平文(ひらぶん)**:通常の文
**暗号文**:そのままでは理解不能な文(暗号化された文)
**暗号化**:平文を暗号文に変換すること
**復号**:鍵を使って暗号文を平文に変換すること
**解読**:暗号文を不正な方法で(通常は鍵を使わず)平文に変換すること

**設問**:鍵は何故必要か?



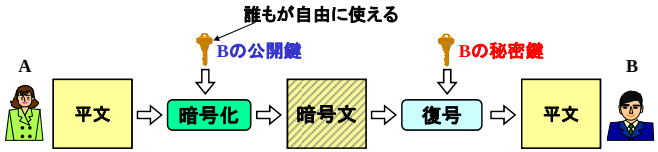
## 共通鍵暗号と公開鍵暗号

**●共通鍵暗号方式(同じ鍵を使用)**




AとBの間で、同じ鍵を誰にも知られずに共有する必要がある

**●公開鍵暗号方式(対になった鍵を使用)**



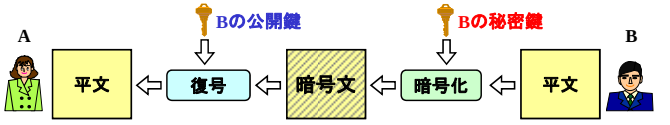

秘密鍵は誰にも渡す必要がない(共通鍵は相手に渡す必要がある)



## 公開鍵暗号は双方向

一方の鍵で暗号化し、他方の鍵で復号
- 公開鍵:誰もが自由に使用できる鍵
- 秘密鍵:本人だけが使用できる鍵(鍵を秘密に保持)

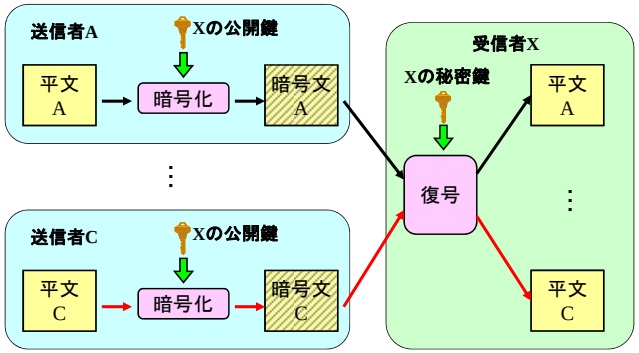

暗号文は秘密鍵所有者しか、復号できないので、安全




誰でも復号できるので、暗号化の意味がない

## 公開鍵暗号による暗号化

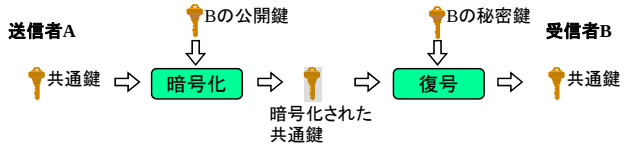
○公開鍵は誰でも使えるので、誰でも暗号文を作れる
○復号できるのは、秘密鍵の所有者のみ



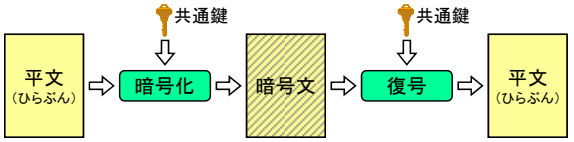

5

## 公開鍵暗号と共通鍵暗号の利用法

① 公開鍵暗号を使用し、共通鍵を安全に送信（鍵共有）




② 共通鍵暗号を使用し、情報を安全に送信



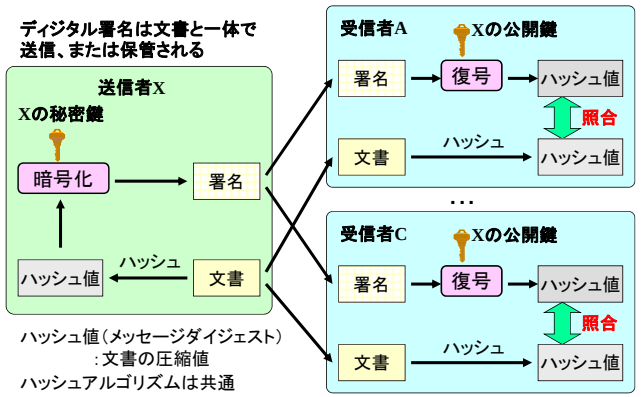

この共通鍵を**セッション鍵**とも呼ぶ

6

## ディジタル署名

○秘密鍵を持っている所有者しか暗号化（署名）ができない
○公開鍵は誰でも使えるので、誰でも復号（署名検証）できる

ディジタル署名は文書と一体で送信、または保管される

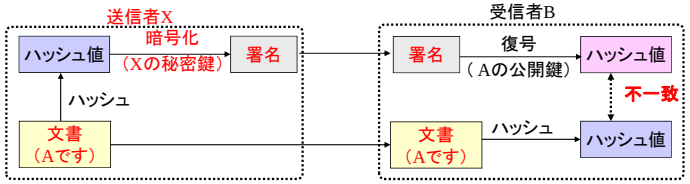



ハッシュ値（メッセージダイジェスト）
：文書の圧縮値
ハッシュアルゴリズムは共通

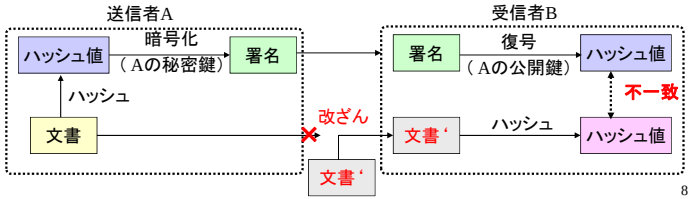
7

## ディジタル署名の効果

1. 署名偽造の検出



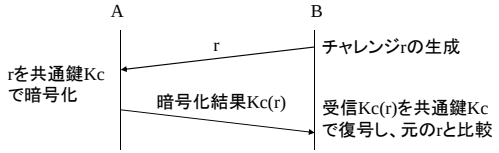

2. 改ざんの検出



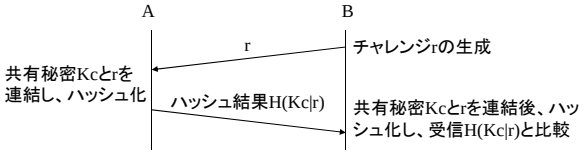

8

## 共通鍵暗号やハッシュによる認証

**共通鍵暗号による認証**



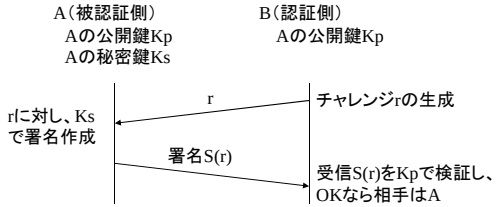

**ハッシュによる認証**




**両方式とも、秘密情報を通信路に流すことなく、認証を行える**

9

## ディジタル署名による認証




**秘密情報共有の必要性はない**

10