

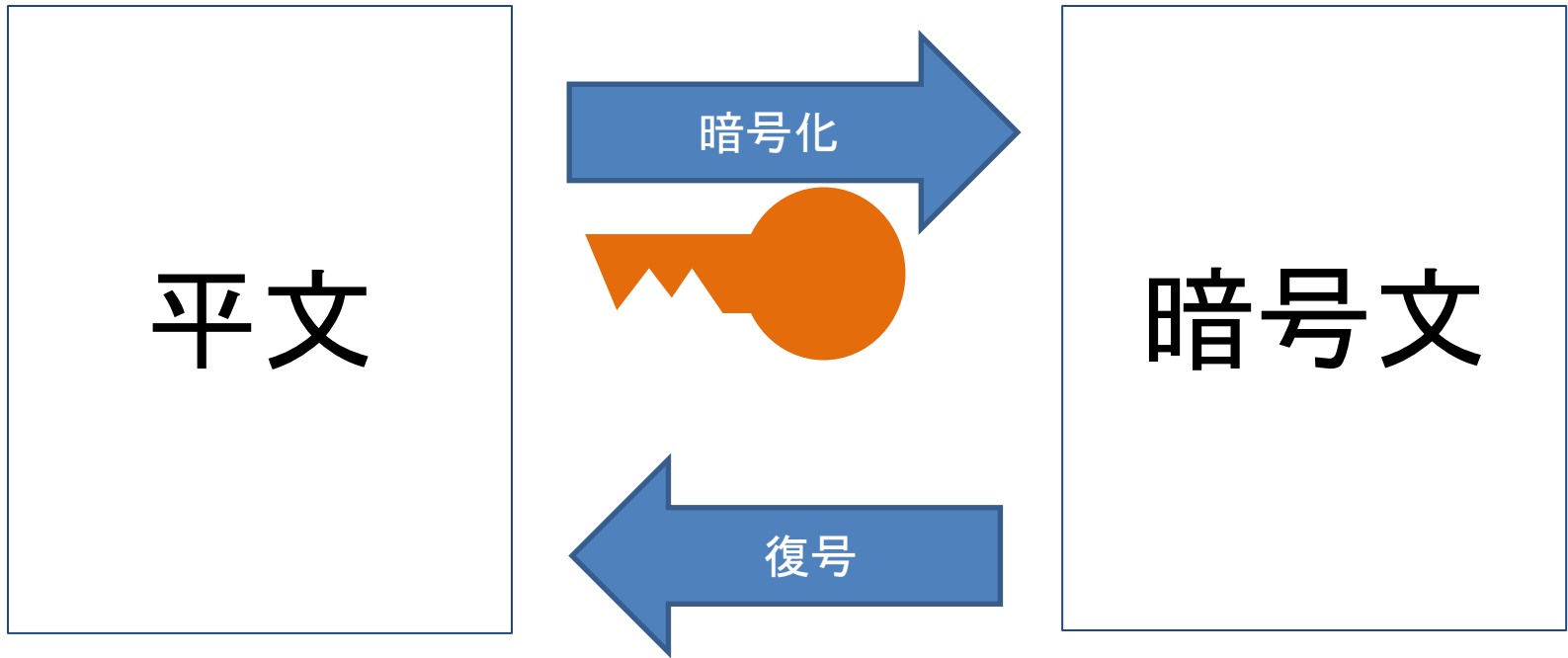
# 暗号化鍵を指導する工夫

共通鍵・公開鍵・秘密鍵をいかにして  
模擬体験させることができるか

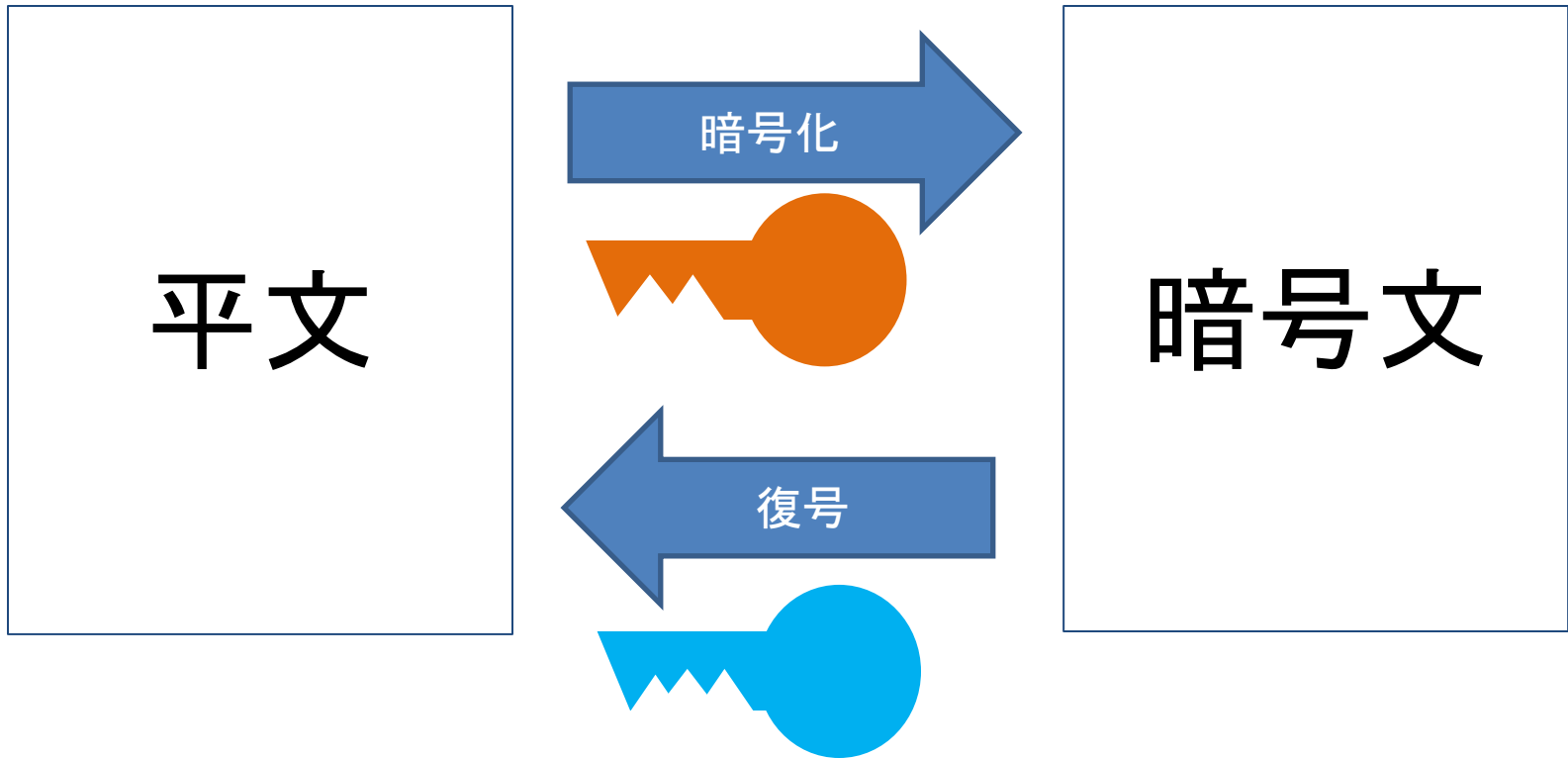
山下裕司

山口県立岩国高等学校 教諭

# 共通鍵



# 公開鍵・秘密鍵



# 公開鍵・秘密鍵の模擬構造を作る

- 手順1 公開鍵から秘密鍵を作成する
- 手順2 公開鍵を公開する
- 手順3 送信先の公開鍵を手に入れる
- 手順4 手に入れた公開鍵で暗号文を作る
- 手順5 暗号文を送信先へ送信する
- 手順6 受信者は自分の秘密鍵で復号する

# 公開鍵・秘密鍵の模擬構造を作る

手順1 公開鍵から秘密鍵を作成する

# 公開鍵・秘密鍵の模擬構造を作る

## 手順1 公開鍵から秘密鍵を作成する

出席番号を利用した関数を定義しておく

Function funckey(x)

kagi = Val(Right(Cells(1, 2), 2))

x = (123 \* kagi \* Cells(1, 8)) Mod 567

funckey = x

End Function

# 公開鍵・秘密鍵の模擬構造を作る

手順1 公開鍵から秘密鍵を作成する

手順2 公開鍵を公開する

手順3 送信先の公開鍵を手に入れる

手順4 手に入れた公開鍵で暗号文を作る

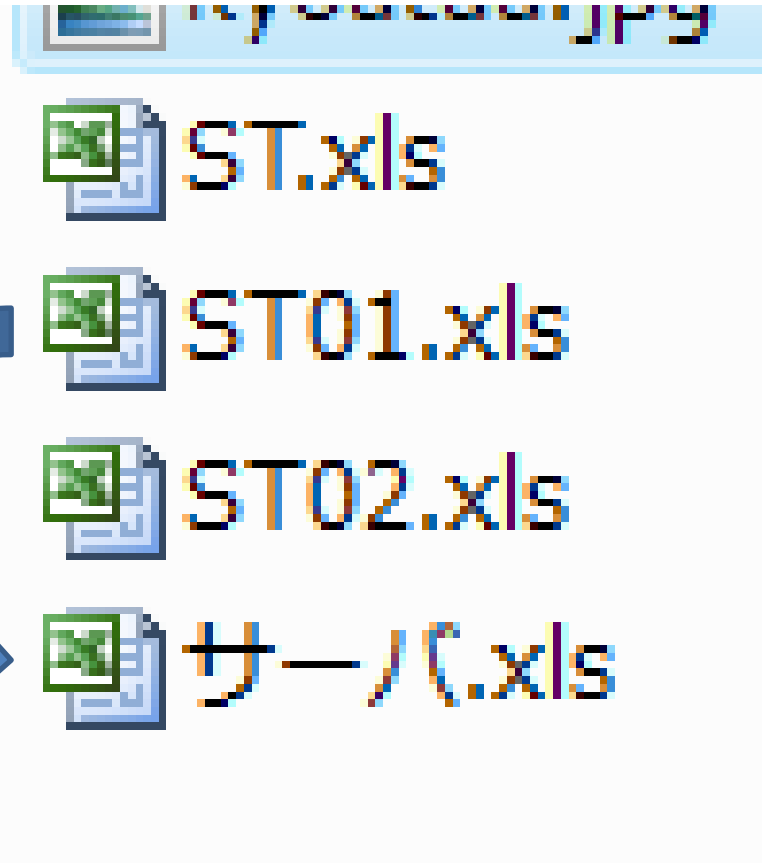
手順5 暗号文を送信先へ送信する

手順6 受信者は自分の秘密鍵で復号する

# 公開鍵・秘密鍵の模擬構造を作る

## 手順2 公開鍵を公開する

```
Sub koukaikagi()  
Application.DisplayAlerts = False  
ate = Cells(3, 2): okuri = Cells(1, 2): koukai = Cells(1, 8)  
d$ = ActiveWorkbook.Path  
ffname = d$ + "¥サーバ\xls"  
Workbooks.Open Filename:=ffname  
actb = ActiveWorkbook.Name  
Sheets("data").Select  
For i = 3 To 53  
If Cells(i, 1) = okuri Then  
Cells(i, 4) = koukai  
Exit For  
End If  
Next  
Workbooks(actb).Save  
Workbooks(actb).Close  
  
End Sub
```





# 公開鍵・秘密鍵の模擬構造を作る

手順1 公開鍵から秘密鍵を作成する

手順2 公開鍵を公開する

手順3 送信先の公開鍵を手に入れる

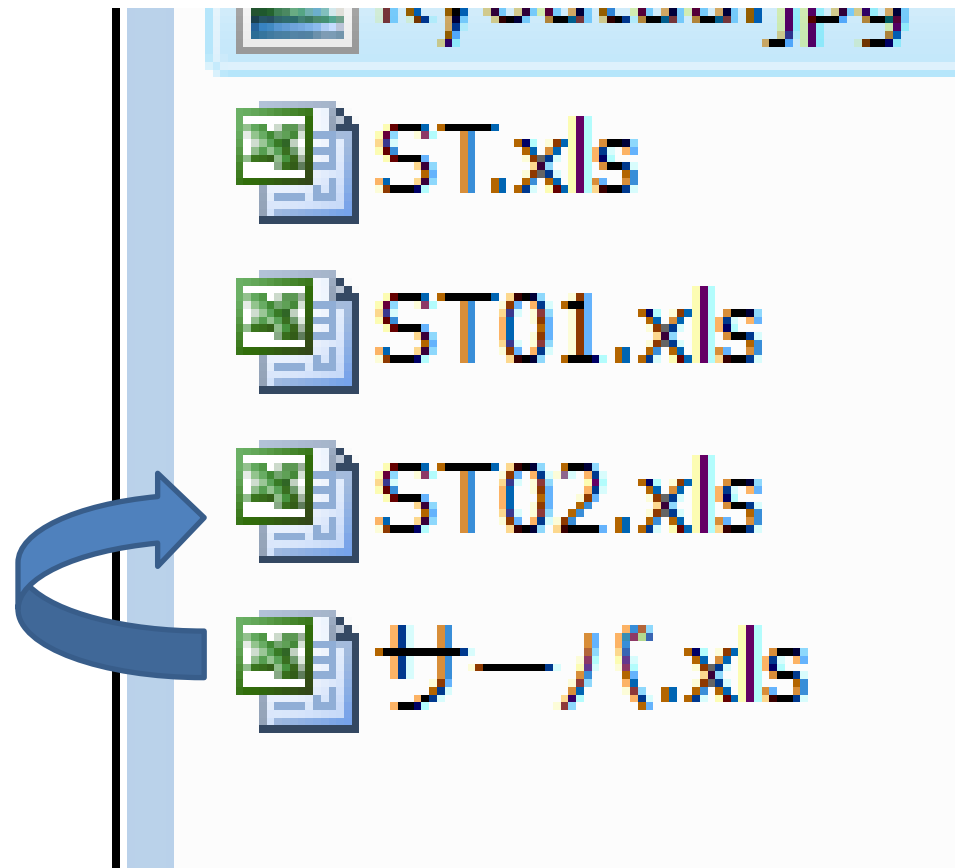
手順4 手に入れた公開鍵で暗号文を作る

手順5 暗号文を送信先へ送信する

手順6 受信者は自分の秘密鍵で復号する

# 公開鍵・秘密鍵の模擬構造を作る

## 手順3 送信先の公開鍵を手に入れる



# 公開鍵・秘密鍵の模擬構造を作る

- 手順1 公開鍵から秘密鍵を作成する
- 手順2 公開鍵を公開する
- 手順3 送信先の公開鍵を手に入れる
- 手順4 手に入れた公開鍵で暗号文を作る
- 手順5 暗号文を送信先へ送信する
- 手順6 受信者は自分の秘密鍵で復号する

# 公開鍵・秘密鍵の模擬構造を作る

- 手順1 公開鍵から秘密鍵を作成する
- 手順2 公開鍵を公開する
- 手順3 送信先の公開鍵を手に入れる
- 手順4 手に入れた公開鍵で暗号文を作る
- 手順5 暗号文を送信先へ送信する
- 手順6 受信者は自分の秘密鍵で復号する

# 公開鍵・秘密鍵の模擬構造を作る

- 手順1 公開鍵から秘密鍵を作成する
- 手順2 公開鍵を公開する
- 手順3 送信先の公開鍵を手に入れる
- 手順4 手に入れた公開鍵で暗号文を作る
- 手順5 暗号文を送信先へ送信する
- 手順6 受信者は自分の秘密鍵で復号する