



# IT日本語2

## 9.3\_暗号化と認証(1)

# 授業の目的・目標

## 目的

- FEの内容を理解する
- IT用語を使った日本語の文章を理解する
- IT業界よく使われるIT用語を覚える

## 目標

- 新しい言葉を正しく読み、意味を理解できる
- 日本語の文法を理解することができる
- 日本語の文章をベトナム語に翻訳することができる
- FE内容についての質問に日本語で答えられる



# 目次

1. カタカナ語の発声練習
2. 言葉の確認
3. 文章の理解: データの暗号化
  - ・ 共通鍵暗号方式
  - ・ 公開鍵暗号方式
4. 問題練習
5. 次の授業予告

# カタカナ語

# アルファベット語の発声練習

No	英語	カタカタ
1	DES	
2	AES	
3	RSA	



# 言葉の確認

# 言葉確認

「コンピュータウイルス(2)」の単語リストをペアで聞き取りを練習します。

言葉を覚えるには、以下の練習が

活動①と②を事前学習で自習したため、授業中で活動③と④を実施します。

- ・活動① 言葉の音読練習
- ・活動② 言葉を見て理解する練習
- ・活動③ 言葉を聞いて理解する練習
- ・活動④ 覚えた語彙のアウトプット練習



# 言葉確認

## 活動③ 言葉を聞いて理解する練習

1. Aさんは単語リストを見て、**単語を読む**
2. Bさんは単語リストを見なく、**ベトナム語で意味を答える**
3. 5問やったら役割チェンジをする

## 活動④ 覚えた語彙のアウトプット練習

1. Aさんは単語リストを見て、**ベトナム語の意味を言う**
2. Bさんは単語リストを見なく、**日本語で単語を答える**
3. 5問やったら役割チェンジをする

※ 制限時間: 5分



# Quizletで勉強しましょう！

## Quizlet



Quizletによって勉強しましょう！



# 文章の理解



# 暗号化と認証の全体内容

①データの暗号化

②デジタル署名



暗号化と認証

③認証局 (CA)

④SSL (Secure Socket Layer)





**Warm up !**



# Warm up

以下の会話を確認しましょう！

どういう  
意味？



# Warm up

39	
893	
4649	
084	
3476	
889	
154	

参考: [語呂合わせ - Wikipedia](#)



# データの暗号化



# データの暗号化



暗号化とは、その名のとおり、データを第三者には解読できない「暗号文」に変換することです。暗号化することによって、たとえば通信中にデータが他の人に盗まれてしまっても、データの内容を知られることはありません。暗号化したデータを元に戻すことを復号といいます。

暗号化と復号には、それぞれ鍵を使ってデータを変換します。

鍵とは、データを変換するための特別なデータです。この鍵の違いによって、さまざまな暗号方式があります。

- 共通鍵暗号方式
- 公開鍵暗号方式





翻訳してみよう！

# データの暗号化

## Mã hóa dữ liệu

**暗号化**とは、その名のとおり、データを第三者には解読できない「暗号文」に変換することです。暗号化することによって、たとえ通信中にデータが他の人に盗まれてしまっても、データの内容を知られることはありません。暗号化したデータを元に戻すことを**復号**といいます。





# データの暗号化

## Mã hóa dữ liệu

暗号化と復号には、それぞれ鍵を使ってデータを変換します。

鍵とは、データを変換するための特別なデータです。この鍵の違いによって、さまざまな暗号方式があります。

- 共通鍵暗号方式
- 公開鍵暗号方式





# 練習問題



「暗号化」とは何ですか。



暗号化のメリットを教えてください。



# 練習問題



暗号化は、情報セキュリティのどんなリスク対策に当たりますか。



暗号化と復号用の「鍵」とは何ですか。







# 共通鍵暗号方式 と 公開鍵暗号方式



# 暗号方式の導入

「共通鍵暗号方式」と「公開鍵暗号方式」  
を勉強する前に、  
次の場面を確認して考えましょう！





# 暗号化方式の導入

## 場面：

- AnさんはBinhさんに凄く大切な資料を送るつもり  
その資料は、BinhさんとAnさん以外誰も見ることはできない
- Anさんは暗号方式を使って、資料を暗号化してから送ります



# 暗号化方式の導入

## 場面：

- AnさんはBinhさんに凄く大切な資料を送る。  
その資料は、BinhさんとAnさん以外には見せたくありません。
- Anさんは暗号方式を使って、資料を送ります。

Anさんは「共通鍵暗号方式」と「共通鍵暗号方式」をどのように使って、暗号化する？





# 共通鍵暗号方式



暗号化と復号に同じ鍵を使う暗号方式を共通鍵暗号方式といいます。

データの送信者と受信者が同じ共通鍵をもっている必要があります。

鍵はあらかじめ送信者から受信者へ配布しておきますが、鍵を盗まれてしまうと誰でも復号できてしまうので、鍵の受け渡しには注意が必要です。

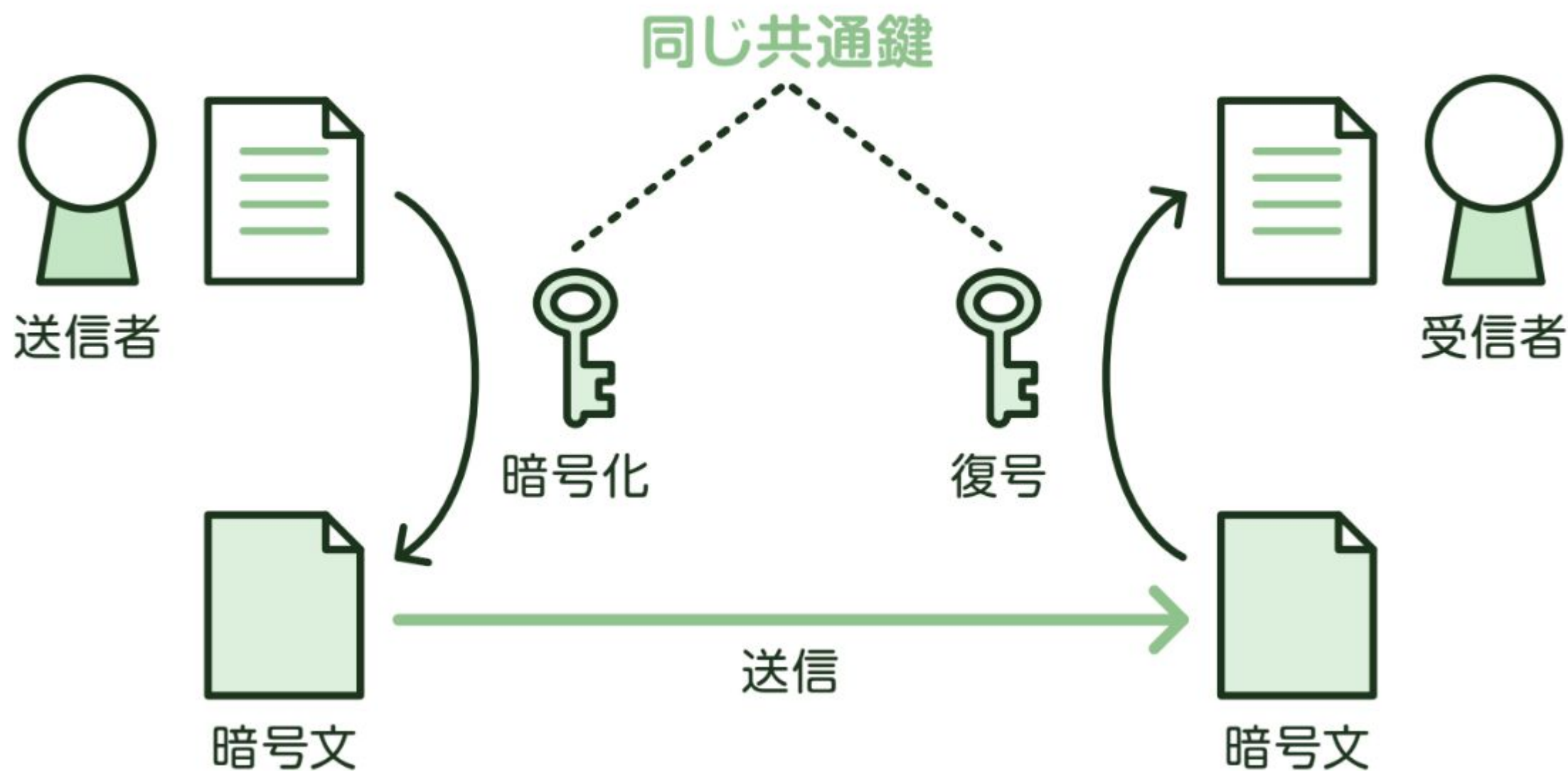
共通鍵暗号方式は、暗号化と復号の処理が速いのが特徴です。しかし、データを送る相手の数だけ鍵を作成する必要があるので、不特定多数の人にデータを送るときには不向きです。

代表的な共通鍵暗号方式には、DESやAESなどがあります。

# 共通鍵暗号方式



〈共通鍵暗号方式〉





# 公開鍵暗号方式



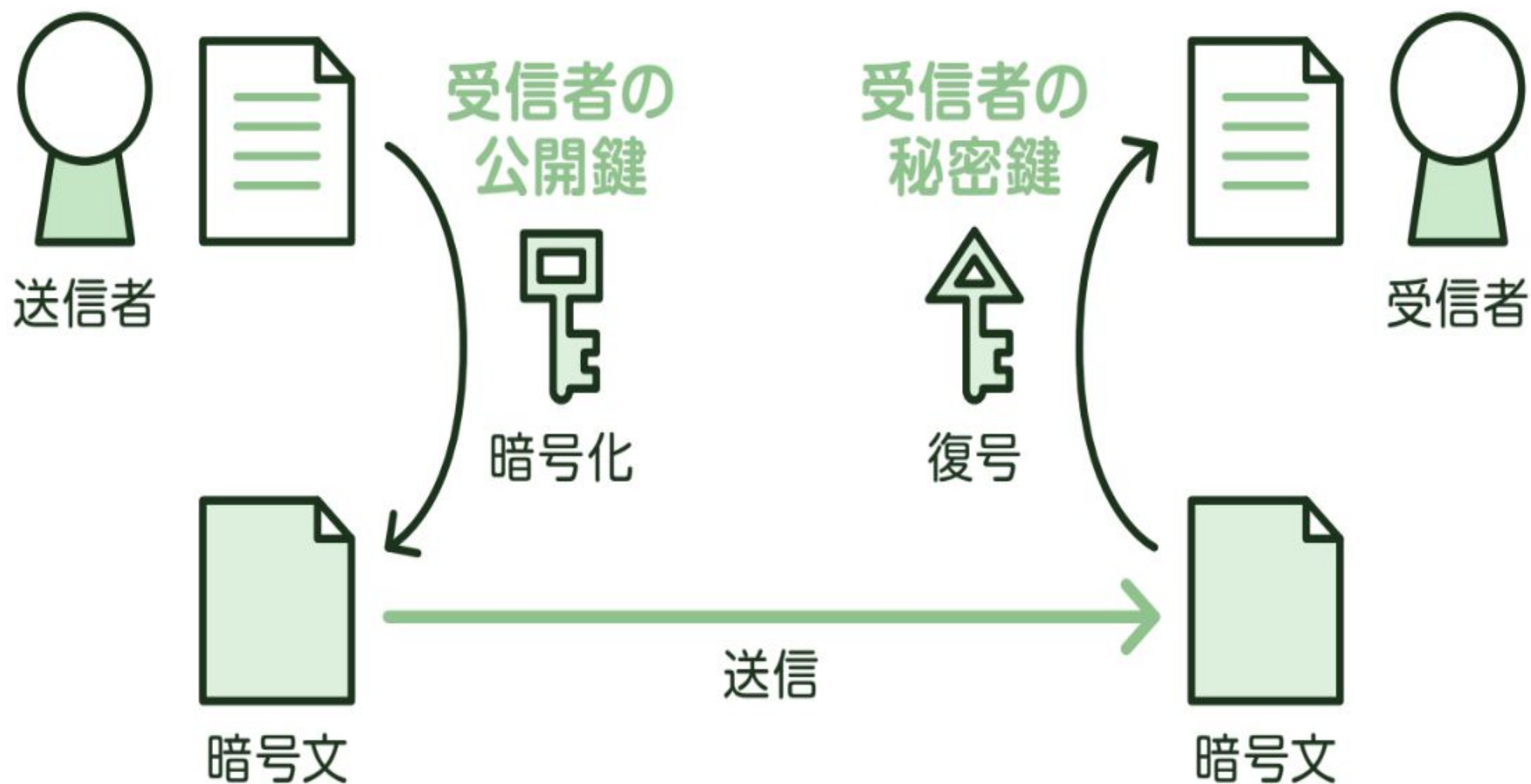
暗号化するときと復号するとき、それぞれ対になる2つの鍵を使う暗号方式を公開鍵暗号方式といいます。受信者は、あらかじめ暗号化に使う公開鍵をインターネットなどで公開しておき、送信者はその鍵を使ってデータを暗号化します。復号は、受信者がもっている秘密鍵で行います。公開鍵は公開してもかまいませんが、秘密鍵は受信者以外には知られないようにしてはなりません。

鍵を公開しているので、不特定多数の相手からデータを受け取るのに向いていますが、暗号化と復号の処理に時間がかかるという短所があります。代表的な公開鍵暗号方式には、巨大な数の素因数分解の困難さを利用したRSAや楕円曲線暗号などがあります。

# 公開鍵暗号方式



〈公開鍵暗号方式〉



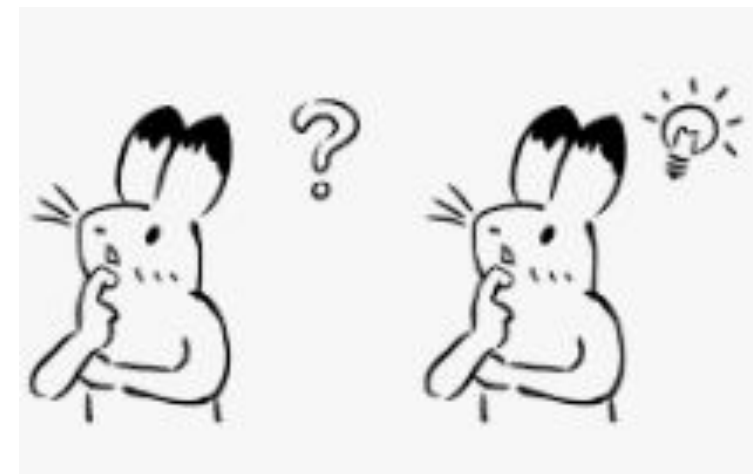


# チームワーク



- ★ 言葉を思い出しながら、文章を読む
- ★ 友達と一緒にベトナム語に翻訳して、理解した内容をキーワードとしてまとめる
- ★ 日本語のQuizを準備する(※)

(※) 大切に覚える必要な内容について  
他の各チームに対する質問を考えましょう！



# ワーク準備

- 1) ワークシートをコピーし、ファイル名を変更する
- 2) クラスのフォルダに保存する
- 3) 「チームの情報」のシートに情報を記入する
- 4) 各案方式の内容をキーワードとしてまとめて  
Quizの質問を考える

暗号方式	内容まとめ	Quiz
①共通鍵暗号方式		

★ 制限時間: **20分**



# 実践1

# 実践1



チームで準備した内容を使って、実践しましょう！

- ✓ 発表チームを決める
- ✓ チームの代表者が内容を説明する
- ✓ Quizを実施する
  - ・内容担当チームが質問を発表する
  - ・他のチームに準備する時間を与える
  - ・答え合わせる



# 共通鍵暗号方式

## Mật mã khóa chung

暗号化と復号に同じ鍵を使う暗号方式を共通鍵暗号方式といいます。データの送信者と受信者が同じ共通鍵をもっている必要があります。

鍵はあらかじめ送信者から受信者へ配布しておきますが、鍵を盗まれてしまうと誰でも復号できてしまうので、鍵の受け渡しには注意が必要です。



# 共通鍵暗号方式

## Mật mã khóa chung

共通鍵暗号方式は、暗号化と復号の処理が速いのが特徴です。しかし、データを送る相手の数だけ鍵を作成する必要がある**ので**、不特定多数の人にデータを送るときには不向きです。

代表的な共通鍵暗号方式には、DESやAESなどがあります。





# 公開鍵暗号方式

## Mật mã khóa công khai

暗号化するときと復号するとき、それぞれ対になる2つの鍵を使う暗号方式を公開鍵暗号方式**といいます**。**受信者**は、あらかじめ暗号化に使う**公開鍵**をインターネットなどで公開**しておき**、**送信者**はその鍵を使ってデータを暗号化します。復号は、受信者がもっている**秘密鍵**で行います。公開鍵は公開してもかまいませんが、秘密鍵は受信者以外には知られないようにしなくてはなりません。



# 公開鍵暗号方式

## Mật mã khóa công khai

鍵を公開している**ので**、不特定多数の相手からデータを受け取るのに向いています**が**、暗号化と復号の処理に時間がかかる**という**短所があります。代表的な公開鍵暗号方式には、巨大な数の素因数分解の困難さを利用したRSAや楕円曲線暗号などがあります。





# 導入場面の回答

場面：

- AnさんはBinhさんに凄く大切な資料を渡す
- その資料は、BinhさんとAnさん以外に誰も見ない
- Anさんは暗号方式を使って、資料を暗号化する

Anさんは「共通鍵暗号方式」と「共通鍵暗号方式」をどのように使って、暗号化する？





# 実践2



# 実践2



各暗号方式の画像を説明しましょう！

- ✓ 個人で理解した内容を使って説明してみる：**3分**
- ✓ チームで話し合って、内容説明を練習する：**7分**
- ✓ 指名された人はクラス全員に説明する

## ❖ 注意点：

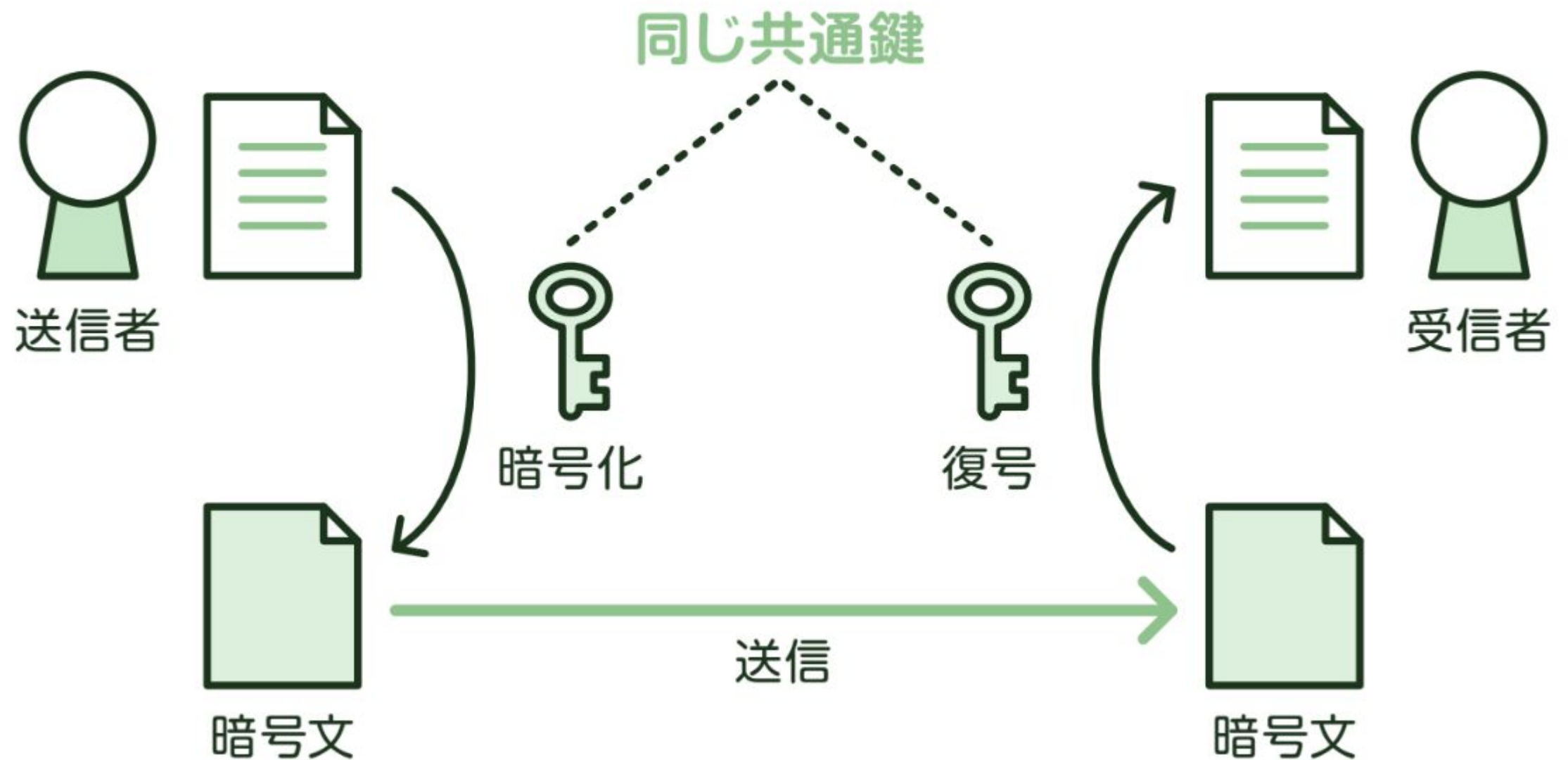
指名された人が上手に説明できなくても、減点されませんが  
何も説明できなければ、**チーム全員に減点されます**



# 共通鍵暗号方式

## Mật mã khóa chung

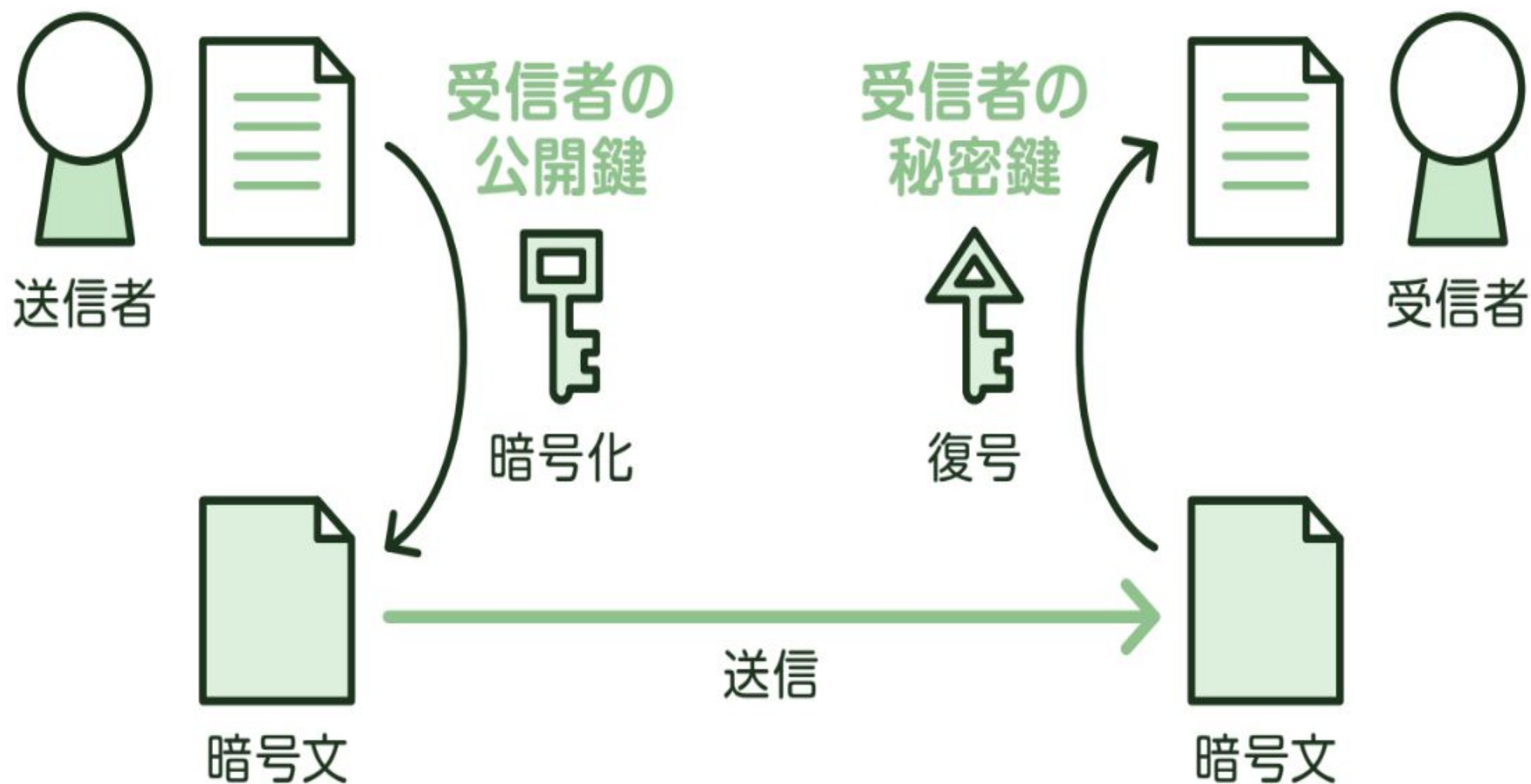
〈共通鍵暗号方式〉



# 公開鍵暗号方式

## Mật mã khóa công khai

〈公開鍵暗号方式〉





# まとめ



# まとめ

Q:どんな鍵を使いますか。

暗号方式	暗号化の鍵	復号の鍵
共通鍵暗号方式		
公開鍵暗号方式		

# 次の授業予告



# 事前学習

来週の授業は「暗号化と認証(2)」です

授業までに以下の資料を確認して準備しておいてください

1. 単語テスト: <https://sal.vn/32C8jo>
2. 文型リスト: <https://sal.vn/TnmGwC>
3. コンピュータウイルス: <https://sal.vn/NRuicn> (P334～P339)

評価しますので、  
必ず事前学習のスライドを確認してください



# 事前学習

来週の授業は「暗号化と認証(2)」です

授業までに以下の資料を確認して準備しておいてください

1. 単語テスト: <https://sal.vn/32C8jo>
2. 文型リスト: <https://sal.vn/TnmGwC>
3. コンピュータウイルス: <https://sal.vn/NRuicn> (P334～P339)

- 予習してから、[予習フォーム](#)を実施します
- 予習フォームをサブミットしたら、[クラスのSlack](#)で報告します

**提出と報告期限: 次の授業の前日 13:00 まで**


# 小テスト



来週の授業で  
勉強した内容について  
小テストを実施します

しっかり復習しておいてください！



The background of the slide is a scenic view of Mount Fuji under a clear blue sky with some light clouds. In the foreground, there are cherry blossom trees in full bloom, their pink flowers creating a dense canopy. To the right, a traditional Japanese temple with a red wooden structure and a dark tiled roof is visible. The text is overlaid on a semi-transparent white rectangular area in the center.

今日の授業は終わりです  
また会いましょう

*Hẹn gặp lại lần sau*