

Picleis 使用方法

1. Picleis とは

「Picleis（ピクレイス）」は、**共通鍵暗号方式**と**公開鍵暗号方式**を一人で体験的に学習できるアプリケーションです。共通鍵暗号方式を学習する場合は「共通鍵モード」を、公開鍵暗号方式を学習する場合は「公開鍵モード」を選択してください。



▲ Picleis のトップ画面

【名前について】

Picleis（ピクレイス）は、「ピクトグラム」とギリシャ語で“鍵”を意味する「クレイス」を合わせた造語です。

2. 共通鍵モード

共通鍵暗号方式を学習するモードです。「**C** チャット画面」は、SNS 等で馴染みのある「メッセージのやり取り」を模した構成になっています。

「**A** 説明領域」の指示を確認しながら、「**B** 送信者領域」あるいは「**D** 受信者領域」を操作してください。手順 1 は、「**B** 送信者領域」からスタートで、操作結果は、「**C** チャット画面」に表示されます。



▲ 共通鍵モードの画面

(上部「**A** 説明領域」、左部「**B** 送信者領域」、中央部「**C** チャット画面」、右部「**D** 受信者領域」)

【利用時のポイント】

次の観点を意識しながら使ってみてください！

- 鍵の名前
 - ☐ 暗号化に使われた**鍵の名前**は？
 - ☐ 復号に使われた**鍵の名前**は？
- 鍵の作成者
 - ☐ 暗号化に使われた**鍵は誰が作成した？**
 - ☐ 復号に使われた**鍵は誰が作成した？**
- やり取り
 - ☐ **鍵は誰から誰へ、どのような状態で渡された？** 鍵の渡し方の**安全性**はどのように感じた？
- 全体の流れ
 - ☐ メッセージ送信から受信までの**全体の流れ**を振り返りたい場合は、全ての手順の終了後、「**C** チャット画面」を見てみてください！

送信者のメッセージを、受信者以外の第三者が読める危険性は高いか？

3. 公開鍵モード

公開鍵暗号方式を学習するモードです。共通鍵モードと同様に、「メッセージのやり取り」を模した画面構成となっています。「**A**説明領域」の指示を確認しながら、「**B**質問者領域」あるいは「**D**回答者領域」を操作しましょう。手順1は、「**B**質問者領域」からスタートで、操作結果は、「**C**チャット画面」に表示されます。

The screenshot shows the Picleis application interface. At the top, it says 'Picleis' and '©Aino Yamasaki'. Below this, there's a header bar with 'あなたは質問者です。' (You are the questioner). The main area is divided into four sections: A (Explanation), B (Questioner), C (Chat), and D (Responder). Section A contains instructions for the user. Section B shows steps for generating a secret key and a public key. Section C is the chat area where the questioner starts. Section D shows steps for receiving a question and sending an answer.

▲ 公開鍵モードの画面

(上部「**A**説明領域」、左部「**B**質問者領域」、中央部「**C**チャット画面」、右部「**D**回答者領域」)

【利用時のポイント】

次の観点を意識しながら使ってみてください！

- 鍵の名前
 - 暗号化に使われた**鍵の名前**は？
 - 復号に使われた**鍵の名前**は？
- 鍵の作成者
 - 暗号化に使われた**鍵は誰が作成した**？
 - 復号に使われた**鍵は誰が作成した**？
- やり取り
 - **鍵は誰から誰へ、どのような状態で渡された**？この鍵の渡し方の**安全性**はどのように感じた？
 - 共通鍵暗号方式とも比較してみてください。
- 全体の流れ
 - 質問送信から回答受信までの**全体の流れ**を振り返りたい場合は、全ての手順の終了後、「**C**チャット画面」を見てみてください！

回答者の回答を、質問者以外の第三者が読める危険性は高いか？