

Picleis 使用方法

目次

1. Picleis とは.....	2
2. 共通鍵モード.....	3
3. 公開鍵モード.....	4
3.1 (管理者の方へ)公開鍵モードで署名や改ざんを設定する.....	5
4. ハイブリッドモード.....	8

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**1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。

また、実際のインターネット通信では、共通鍵暗号方式と公開鍵暗号方式を組み合わせた**ハイブリッド方式**が基盤となっています。ハイブリッド方式を学習したい場合は「ハイブリッドモード」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**」を模した構成となっており、「**送信者**」と「**受信者**」の役割を 1 人 2 役で行います。

…「**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。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」を見てみましょう。

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おり、「質問者」と「回答者」の役割を 1 人 2 役で行います。

…「**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。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 area with a message: 'あなたは質問者です。' (You are the questioner.) and instructions: '公開鍵暗号方式を学習します。まず、質問者として秘密鍵となる文字列を決めて入力し、「生成」ボタンを押してください。' (Learn the public key encryption method. First, as the questioner, decide on a character string that will be the secret key and enter it, then press the 'Generate' button.) There are two buttons: '1つ前の手順に戻る' (Return to the previous step) and '手順1からやり直す' (Restart from step 1). The main area is divided into three columns. The left column (B) is for the '質問者' (Questioner) and contains two steps: '手順1 秘密鍵を生成' (Step 1: Generate secret key) with a text input field and a '生成' (Generate) button, and '手順2 公開鍵を生成' (Step 2: Generate public key) with a '生成' (Generate) button. The middle column (C) is the '【チャット画面】' (Chat screen) and shows a message: '質問者がチャットを開始しました' (The questioner started the chat). The right column (D) is for the '回答者' (Responder) and contains two steps: '手順4 質問文と公開鍵を受信' (Step 4: Receive question text and public key) and '手順5 回答文を作成し、暗号化' (Step 5: Create answer text and encrypt) with a text input field and buttons for '鍵選択' (Select key) and '暗号化' (Encrypt). There are also buttons for '質問受信・回答送信' (Receive question, send answer) and '1つ前の手順に戻る' (Return to the previous step).

▲ 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」を見てみましょう。

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？

3.1 (管理者の方へ)公開鍵モードで署名や改ざんを設定する

https://www.pictogramming.org/apps/picleis/?mode=koukai&step=1_setting に移動し、左上に表示される「先生方へ」をクリックすると、
「改ざん」や「署名」など、実世界の通信をより意識しながら、公開鍵暗号方式を体験するモードを設定することができます。

設定できるモードは、p.4 で説明した「モード①：通常モード」のほか、次の 3 種類です。学習者の進捗や理解度に応じて、お使いください。

モード名	説明
モード②： 盗聴モード（改ざんあり）	回答の暗号化後に、メッセージが改ざんされます。「作成した回答」と「復号した回答」が一致しないことを体験できます。盗聴や改ざんが「知らずの間に行われてしまうこと」を知ることが目的です。
モード③： 署名モード（改ざんなし）	「知らずの間の盗聴や改ざん」を防ぐための方法の 1 つである「電子署名」を体験できます。回答に電子署名を付与し、復号時にその電子署名を検証すると、「改ざんを検知できること」を知ることが目的です。
モード④： 署名モード（改ざんあり）	

いずれのモードも、通常の公開鍵モードと同様のインターフェースで構成しており、説明を読みながら、1 人で体験的に学習できるようになっています。

▲ 「モード②：盗聴モード（改ざんあり）」の画面例

手順 5 で作成した**平文の回答（りんご）**と、手順 8 で**復号した回答（りん？）**が異なっている。

この例では、**復号された回答（りん？）**から、「回答が改ざんされたかもしれない」と勘付くことはできるが、**改ざんを「確かに検知」するためにはどうしたら良いかを考えるきっかけを作る。**

Picleis ©Aino Yamasaki

モード③

あなたは質問者です。
検証結果を表示しています。結果を確認してください。

1つ前の手順に戻る
手順1からやり直す

質問者

手順11
復号された回答を検証

検証

署名検証結果:

署名時のハッシュ値:
4261abfc91324dc5319312592125610a16b0b0a996cdfae1d24766b918afae9

復号後のハッシュ値:
4261abfc91324dc5319312592125610a16b0b0a996cdfae1d24766b918afae9

ハッシュ値が一致しています

メッセージは改ざんされていません。回答者本人の署名です。

▲電子証明書を閉じる

所有者: 回答者
公開鍵: ZegJTnbgka2WytQaM0evbgQ14NPowpY7E6FMb1tr426XLUfecsRQyaRoNhf5TRwLGM5XKO1CXmoxpTEZxGiwkFWOOEEN7WbyYd7ZyZUvLWppJcm1nqNTP3MUPmmAar4P92CkRSU4s1PSbE3d6G3RWp6FHZ1QHhg6RPFPM=
発行者: Picleis認証局

回答者

【チャット画面】

署名しました

回答者が公開鍵で回答を暗号化しました

暗号化された回答: DAqY1tbGIS

電子署名: **回答者**

質問者が秘密鍵で回答を復号しました

復号された回答: りんご

回答者

手順5
回答文を作成

りんご

完了

選択された鍵: 公開鍵

手順6
回答文に署名を付与

ハッシュ化 署名

ハッシュ値 (署名時):
4261abfc91324dc5319312592125610a16b0b0a996cdfae1d24766b918afae9

署名: ハンコで表しています

このハンコが本当に回答者のものであることを証明する電子証明書を添付しました

証明書の詳細を非表示

所有者: 回答者
公開鍵: ZegJTnbgka2WytQaM0evbgQ14NPowpY7E6FMb1tr426XLUfecsRQyaRoNhf5TRwLGM5XKO1CXmoxpTEZxGiwkFWOOEEN7WbyYd7ZyZUvLWppJcm1nqNTP3MUPmmAar4P92CkRSU4s1PSbE3d6G3RWp6FHZ1QHhg6RPFPM=
発行者: Picleis認証局

手順7
回答文を暗号化

鍵選択 暗号化

手順8
暗号化された回答文と署名を送信

暗号化された回答: DAqY1tbGIS

送信

▲ 「モード③：署名モード（改ざんなし）」の画面例

平文の回答（りんご）と、復号された回答（りんご）は同一である。

しかし、実際の通信では、質問者は、平文の回答（りんご）を知らないため、復号された回答（りんご）が「改ざんされたものなのか、されていないものなのか」を確かめなければならない。

そのため、平文の回答（りんご）から生成したハッシュ値と、復号された回答（りんご）から生成したハッシュ値を比較する。

比較の結果、2つのハッシュ値の一致、すなわち「回答が改ざんされていないこと」を確かめる。

また、回答に含まれる電子署名（ハンコ）を検証し、「その回答が確かに回答者から送られたものであること」も確かめる。

Picleis ©Aino Yamasaki

モード③

あなたは質問者です。

検証結果を表示しています。結果を確認してください。

1つ前の手順に戻る

手順1からやり直す

質問者

手順11
復号された回答を検証

検証

署名検証結果:

署名時のハッシュ値:
4261abfc91324dc5319312592125610a16b0b0a996fcdfae1d24766b918afae9

復号後のハッシュ値:
d1a252ecc7bbf53e701f392604dcfa549fa8c526aaef5bf5b5c83165bac58a8

ハッシュ値が一致していません

回答者本人の署名ですが、メッセージの内容が改ざんされています。

▲電子証明書を閉じる

所有者: 回答者
公開鍵: ZegJTnBgkga2WytQaM0evbgQ14NPowPy7E6FmBtr426XLUfecsRQyaRoNHf5TRwLGM5XKO1CxmoltPEXzGiwkFWOOEEN7WbyYd7ZYzUoVLWppJcm1nqNTP3MUPmmAar4P92CrSU4s5JP5bE3d6G3RWp6FH21QHhg6PFPFM=
発行者: Picleis認証局

【チャット画面】

署名しました

回答者が公開鍵で回答を暗号化しました

暗号化された回答: DAqY1tbGIS
電子署名: 回答者

質問者が秘密鍵で回答を復号しました

復号された回答: ▼んご

回答者

手順5
回答文を作成

りんご

完了

選択された鍵: 公開鍵

手順6
回答文に署名を付与

ハッシュ化 署名

ハッシュ値 (署名時):
4261abfc91324dc5319312592125610a16b0b0a996fcdfae1d24766b918afae9

署名: ハンコで表しています

このハンコが本当に回答者のものであることを証明する電子証明書を添付しました

証明書の詳細を非表示

所有者: 回答者
公開鍵: ZegJTnBgkga2WytQaM0evbgQ14NPowPy7E6FmBtr426XLUfecsRQyaRoNHf5TRwLGM5XKO1CxmoltPEXzGiwkFWOOEEN7WbyYd7ZYzUoVLWppJcm1nqNTP3MUPmmAar4P92CrSU4s5JP5bE3d6G3RWp6FH21QHhg6PFPFM=
発行者: Picleis認証局

手順7
回答文を暗号化

鍵選択 暗号化

手順8
暗号化された回答文と署名を送信

暗号化された回答: DAqY1tbGIS

送信

▲ 「モード④：署名モード（改ざんあり）」の画面例

平文の回答（りんご）と、復号された回答（▼んご）には差異がある。

しかし、実際の通信では、質問者は、平文の回答（りんご）を知らないため、復号された回答（▼んご）が「改ざんされたものなのか、されていないものなのか」を確かめなければならない。

そのため、平文の回答（りんご）から生成したハッシュ値と、復号された回答（▼んご）から生成したハッシュ値を比較する。

比較の結果、2つのハッシュ値の不一致、すなわち「回答が改ざんされていること」を確かめる。

また、回答に含まれる電子署名（ハンコ）を検証し、「その回答が確かに回答者から送られたものであること」も確かめる。

4. ハイブリッドモード

共通鍵暗号方式と公開鍵暗号方式を組み合わせた**ハイブリッド方式**を学習するモードです。そのため、共通鍵モードの学習および公開鍵モードの学習の発展として、お使いください。

ハイブリッドモードでは、実際の通信をより意識できるように、「サーバ」と「クライアント」の役割を 1 人 2 役で行います。画面構成は、共通鍵モードおよび公開鍵モードと同様です。

…「**A**説明領域」の指示を確認しながら、「**B**サーバ領域」あるいは「**D**クライアント領域」を操作しましょう。操作結果は、「**C**チャット画面」に表示されます。



▲ ハイブリッドモードの画面

(上部「**A**説明領域」、左部「**B**クライアント領域」、中央部「**C**チャット画面」、右部「**D**サーバ領域」)

【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？
- 暗号化や復号の対象
 - 暗号化したものは何？
 - 復号したものは何？
- 鍵の作成
 - 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。