ファイル暗号化実習

－公開鍵暗号方式によるファイルの暗号化と復号－

年 組 番氏名

目標：（この課題でできるようにしたい目標を書きなさい）

|  |
| --- |
| 情報セキュリティの確保のため，ウェブサイトを閲覧する際など，日常的に公開鍵暗号方式の技術が利用されているが，その手順を確認する機会は少ない。公開鍵・秘密鍵の作成と暗号化，復号を通して，その有用性を確認する。 |

**はじめに**

公開鍵暗号方式が活用されているサービスや技術にはどのようなものがあるだろうか。

**実習方法**

１　説明用ファイルを参考に，公開鍵暗号方式の仕組みを理解する。

授業説明ファイル１，授業説明ファイル２

２　暗号化ソフトを利用し，公開鍵・秘密鍵を実際に作成する。

３　相手の公開鍵を使って暗号化する。

４　暗号文を相手に送信する。

５　取得した相手の暗号文を自分の秘密鍵で復号する。

６　他の生徒が暗号化した暗号文は自分の秘密鍵では復号できないことを確認する。

**報告書の作成** ～各自，次の項目について報告書を作成すること～

１　公開鍵暗号方式について，その仕組みを簡単にまとめなさい。

|  |
| --- |
|  |

２　公開鍵暗号方式について，その特徴についてまとめなさい。

|  |
| --- |
|  |

３　電子署名について調べたことをまとめなさい。

|  |
| --- |
|  |