

プログラム作成の課題

1. RSA暗号の暗号化および復号化のプログラムを作成せよ. 具体的には、次の暗号化と復号化の仕様を満たすこと.

暗号化	入力: 暗号化鍵 (e, n) とメッセージ(ひら文)のファイル 出力: 暗号化されたファイル
復号化	入力: 復号化鍵 (d_e, n) と暗号化されたファイル 出力: 元のメッセージ(ひら文)ファイル

具体的な操作例

暗号化の操作

`./rsa.out -e 9929 32399 foo goo`

ただし、

- `rsa.out` : RSA暗号プログラムの実行ファイル
- `-e` : 暗号化を指定するオプション
- `(9929, 32399)`: 暗号化鍵
- `foo` : 暗号化するメッセージ(ひら文)のファイル名
- `goo` : 暗号化されたデータ(暗号文)を出力するファイル名

具体的な操作例

復号化の操作

`./rsa.out -d 9329 32399 goo hoo`

ただし、

- `rsa.out` : RSA暗号プログラムの実行ファイル
- `-d` : 復号化を指定するオプション
- `(9329, 32399)` : 復号化鍵
- `goo` : 暗号文のファイル名
- `hoo` : 復号した元のメッセージ(ひら文)を出力するファイル名

上記の例では、暗号化と復号化の操作をオプションの指定で分けているが、暗号化と復号化のプログラムを別々に作成しても構わない。