問040005問題

プログラム設計に関する次の記述を読んで，設問１～４に答えよ。

データを送るとき，伝送路上での内容秘匿のために，データを暗号化して送る方法がある。ここでは，データから暗号化ファイルを作成するプログラムについて考える。

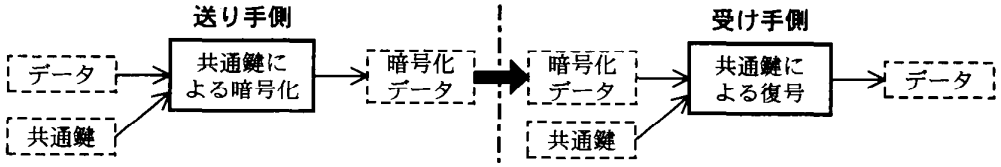
〔暗号化，復号及び鍵の説明〕

送り手と受け手が了解して決められた関数とその逆関数及びそれぞれに与える鍵と呼ばれるパラメタを用い，データを変換する。送り手側の処理を暗号化，受け手側での処理を復号という。

〔共通鍵暗号方式の説明〕

次のように暗号化と複号に同一の鍵を用いる方式である。この鍵を“共通鍵”と呼び，送り手と受け手が共有する。

この方式を使うと暗号化及び復号の処理を比較的高速に行えるので，このプログラムでは，通信文の暗号化に用いる。



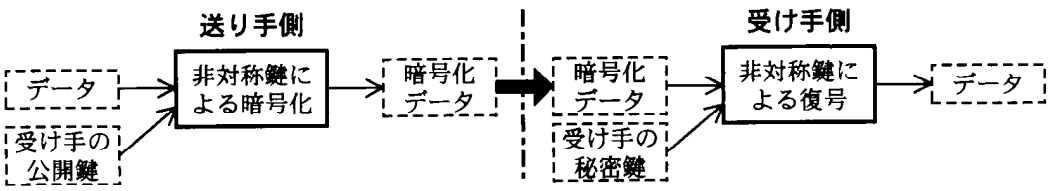
〔非対称鍵暗号方式(公開鍵暗号方式)の説明〕

公開鍵と秘密鍵の一対の鍵を用いる方式である。ここでは，公開鍵で暗号化されたデータは対応する秘密鍵でしか復号できず，秘密鍵で暗号化されたデータは対応する公開鍵でしか復号できないものとする。

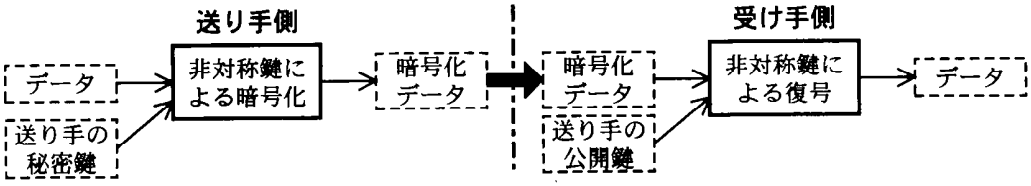
秘密鍵は，作成した本人だけが所有する。公開鍵は公開しているので，だれでも入手が可能であり，改めて相互に受け渡す必要はない。

このプログラムでは，非対称鍵暗号方式を次のように用いる。

（１） 受け手の公開鍵を用いて通信文の暗号化に用いた共通鍵を暗号化する。これによって，共通鍵を受け手に安全に渡すことができる。



（２） 送り手の秘密鍵を用いて送り手の名前などを暗号化する。受け手がこれを送り手の公開鍵で復号し，送り手の名前などが正しく復号できれば，送り手の正当性が確認できる。



〔暗号化ファイルとモジュールの説明〕

暗号化ファイルの作成には，暗号化関連のセグメント(サブルーチン)を利用する。暗号化ファイルの構成要素と各セグメントとの関係は，図１に示すとおりである。

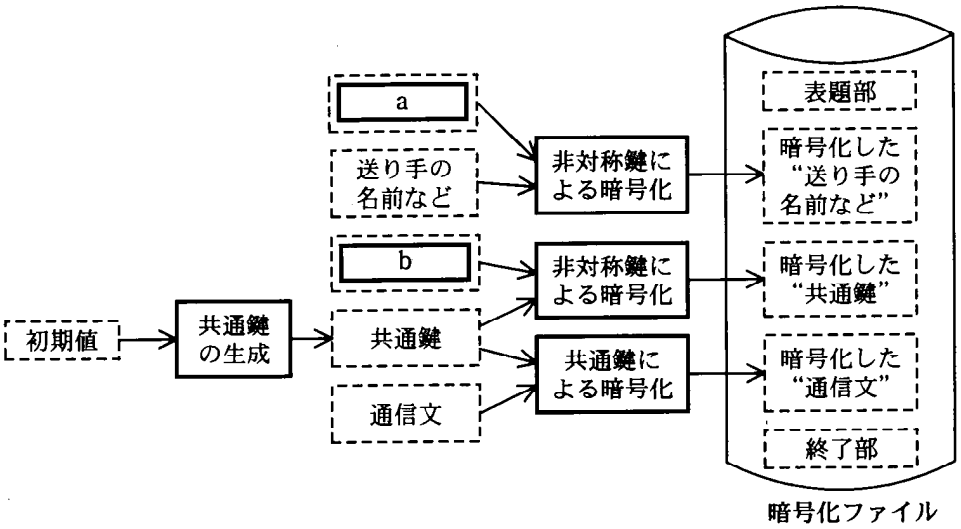


図１　暗号化ファイルの作成

設問１ 図１の［　　］に入れる正しし塔えを，解答群の中から選べ。

解答群

ア　受け手の公開鍵　　イ　受け手の秘密鍵
ウ　送り手の公開鍵　　エ　送り手の秘密鍵
オ　共通鍵　　カ　初期値

設問２ 図２は，プログラムの構造図である。図中のモジュールのうち，“非対称鍵による暗号化”のセグメントを呼び出す必要があるモジュールを，解答群の中から二つ選べ。

解答群

ア　送り手の名前などの暗号化　　イ　共通鍵の暗号化
ウ　共通鍵の生成　　エ　公開鍵の読込み
オ　通信文の暗号化　　カ　秘密鍵の読込み

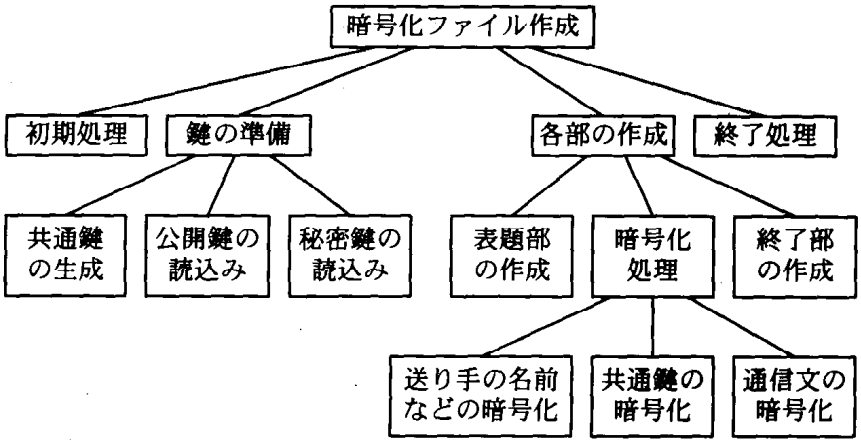


図２　プログラムの構造

設問３ 図２中の“共通鍵の暗号化”以外のモジュールで，上位のモジュールからの入力として，“共通鍵”が必要なモジュールを，解答群の中から選べ。

解答群

ア　送り手の名前などの暗号化　　イ　共通鍵の生成

ウ　終了部の作成　　エ　通信文の暗号化

オ　表題部の作成

設問４ 図３は，図２の最下位のモジュールの実行の順番を表している。この図を完成したとき，［　　］に入れる正しい答えを，解答群の中から選べ。ここで，暗号化ファイルへの各項目の書込みは，図２の“各部の作成”で行われる。また，各項目は，作成後すぐにファイルへ書き込み，主記憶に保持しないものとする。

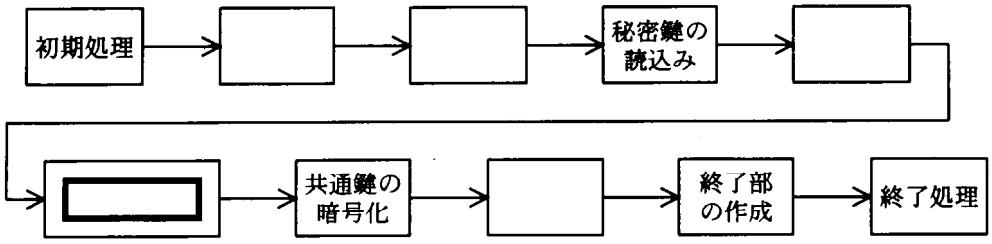


図３　最下位モジュールの実行の順番

解答群

ア　送り手の名前などの暗号化　　イ　共通鍵の生成

ウ　公開鍵の読込み　　エ　通信文の暗号化

オ　表題部の作成