問040005解説

◆解答

設問１　ａ　エ　　ｂ　ア

設問２　ア、イ

設問３　エ

設問４　ア

◆解説

秘密鍵方式、公開鍵暗号方式に関する問題である。

暗号化には次のような種々の問題がある。

①　通信文を秘密の共通鍵を利用して、暗号化、復号する問題。

②　通信文を受け手の公開鍵で暗号化し、受け手の秘密鍵で復号する問題。

③　秘密の共通鍵を相手に渡す場合、受け手の公開鍵で共通鍵を暗号化し、受け手の秘密鍵で共通鍵を復号する。

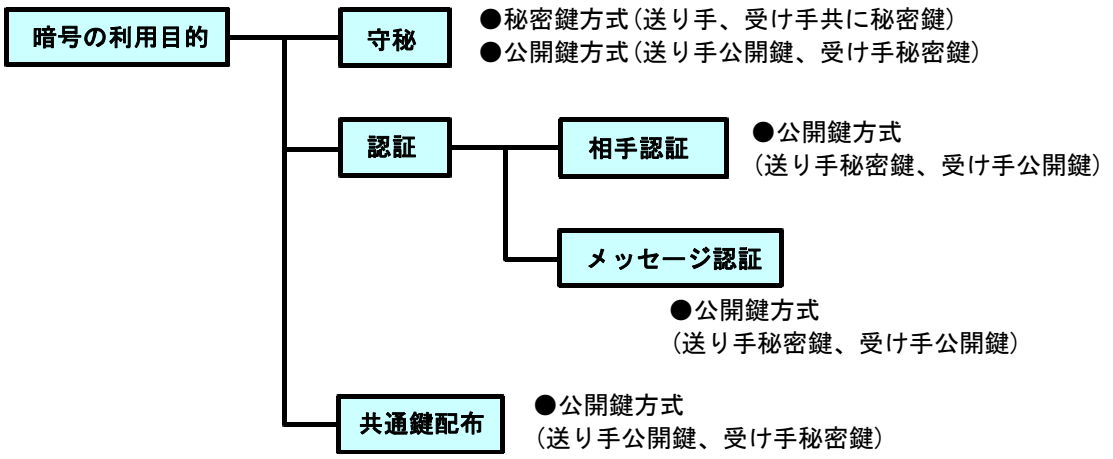
④　署名などの場合、署名を送り手の秘密鍵で暗号文を作り、受け手は送り手の公開鍵で暗号文を平文に変換する。

暗号化の利用目的

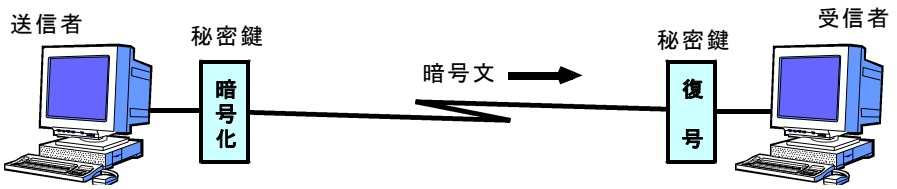
鍵を利用することによって、情報を保証されるのは送り手なのか受け手なのかを十分に考慮して検討する必要がある。特に、公開鍵を利用する場合、秘密鍵を利用するのは保証される必要がある人であり、公開鍵は秘密鍵を用いる人のものが利用される。

署名やメッセージ認証の場合、他の送り手の「なりすまし」による悪用を避けるために、送り手が自分の秘密鍵を使用して署名やメッセージの暗号文を作成し、送り手の公開鍵で受け手が暗号文から平文を作成させることになる。この方法を利用することによって、送り手が唯一になり、送り手の保証が可能となる。署名もメッセージも保証された送り手のみが送信したものになる。

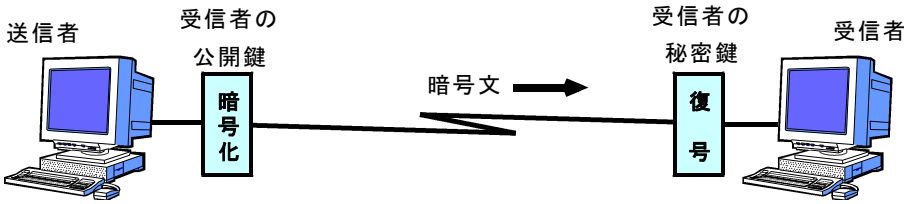
秘密鍵を配布する場合、受け手に安全に秘密鍵を届けるためには、送り手は受け手の公開鍵で暗号化し、受け手のみが自分の秘密鍵で復号できると、安全に鍵を配布することができる。



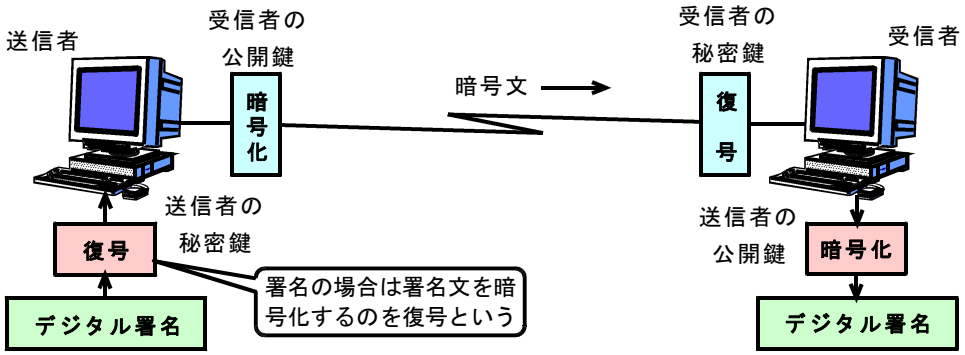
秘密鍵方式を用いた通信文の暗号化



公開鍵方式を用いた通信文の暗号化



公開鍵を用いて通信文に署名して暗号化し、送信する場合



設問１

送り手の名前などを非対称鍵による暗号化に用いるのは送り手の秘密鍵である。従って、ａの求める答えはエである。

ｂは通信文の暗号化に用いた共通鍵の暗号化には受け手の公開鍵を用いる。従って、ｂの求める答えはアである。

設問２

図２はプログラムの階層構造図を示している。暗号ファイルの作成は、初期処理、鍵の準備、表題部・暗号処理、終了処理の４モジュールから構成される。

暗号化処理部分は、署名の暗号化、共通鍵の暗号化、通信文の暗号化の３モジュールから構成されている。

通信文の暗号化に用いる共通鍵の暗号化は、受け手の公開鍵で暗号化し、受け手の秘密鍵で復号する非対称鍵による暗号化である。また、送り手の名前などを送り手の秘密鍵を用いて暗号化し、受け手は送り手の公開鍵で復号する場合も非対称鍵による暗号化である。従って、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は送り手の名前などの暗号化と共通鍵の暗号化である。求める答えはアとイである。

設問３

通信文の暗号化には、共通鍵の方式と公開鍵の方式があり、共通鍵による通信文の暗号化の場合には共通鍵が必要になる。従って、図２で共通鍵が必要なモジュールは通信文の暗号化である。求める答えはエである。

設問４

階層構造図の最下位モジュールは機能処理するモジュールである。階層構造図において、機能処理モジュールを左から右に逐次辿ると、実行処理順序を求めることができる。ただし、トランザクション処理に相当するモジュールは要求仕様に基づいて、実行されたり実行されなかったりする。機能処理するモジュールの実行順序は次のようになる。

初期処理→共通鍵の生成→公開鍵の読込み→秘密鍵の読込み→表題部の作成→送り手の名前などの暗号化→共通鍵の暗号化→通信文の暗号化→終了部の作成→終了処理

このうち送り手の名前などの暗号化が求める答えである。求める答えはアである。