**問題５　次の情報セキュリティに関する各設問に答えよ。**

＜設問１＞ 次の暗号化技術に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

データ通信では，伝送中にデータが盗聴される可能性がある。そこで，データの漏えいを防ぐためデータを暗号化し，盗聴されても復号できないようにする。暗号化技術には，大きく分けて二つの種類がある。

［共通鍵暗号方式］

暗号化と復号に同じ鍵を利用する方式で，送信側は送信しようとするデータ(平文)に共通鍵を用いて,暗号文を作成して送信し,受信側は受信した暗号文を同じ鍵を使って平文に戻す。

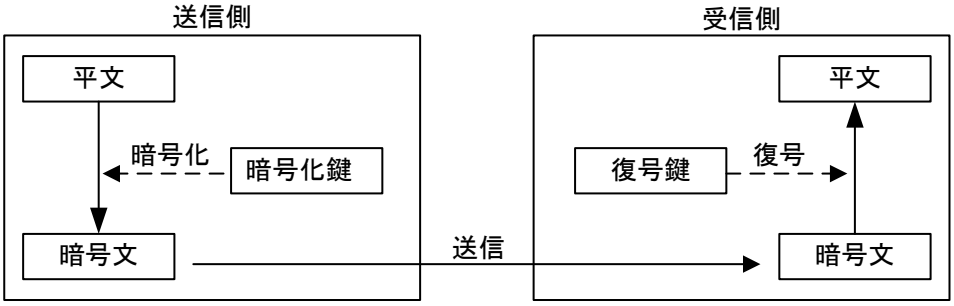


**図１　共通鍵暗号方式を利用した送信**

［公開鍵暗号方式］

対応する二つの鍵を作成し，一方の鍵で暗号化すると他方の鍵で復号できる方式である。一方の鍵を秘密鍵として自分で厳重に保管し，他方の鍵を公開鍵として公開する。一般的な公開鍵暗号方式では，送信側は［　(1)　］を使って暗号文を作り送信し，受信側は［　(2)　］で復号する。

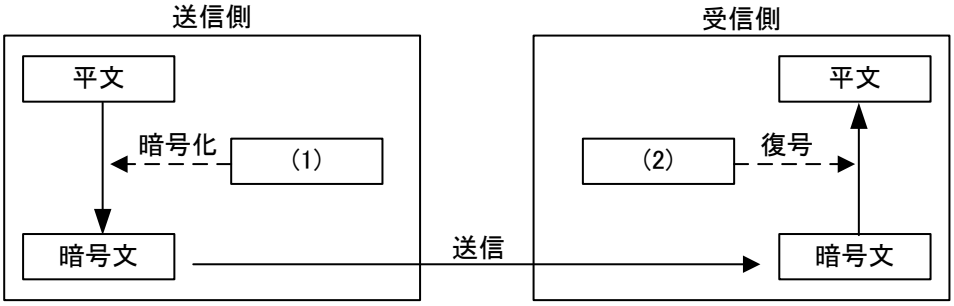


**図２　公開鍵暗号方式を利用した送信**

(1)，(2) の解答群

ア．受信者の公開鍵　　イ．受信者の秘密鍵

ウ．送信者の公開鍵　　エ．送信者の秘密鍵

＜設問２＞ 次のハイブリッド暗号方式に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ハイブリッド暗号方式は，共通鍵暗号方式と公開鍵暗号方式を組み合わせた暗号方式である。その仕組みを次に示す。

［ハイブリッド暗号方式の仕組み］

① 共通鍵を生成する。

② 共通鍵を受信者の公開鍵で暗号化する。

③ 暗号化された鍵を送信する。

④ 暗号化された鍵を［ (3) ］で復号する。

以降の通信を次のように行う。

⑤ 平文を［ (4) ］で暗号化する。

⑥ 暗号文を送信する。

⑦ 暗号文を［ (4) ］で復号する。

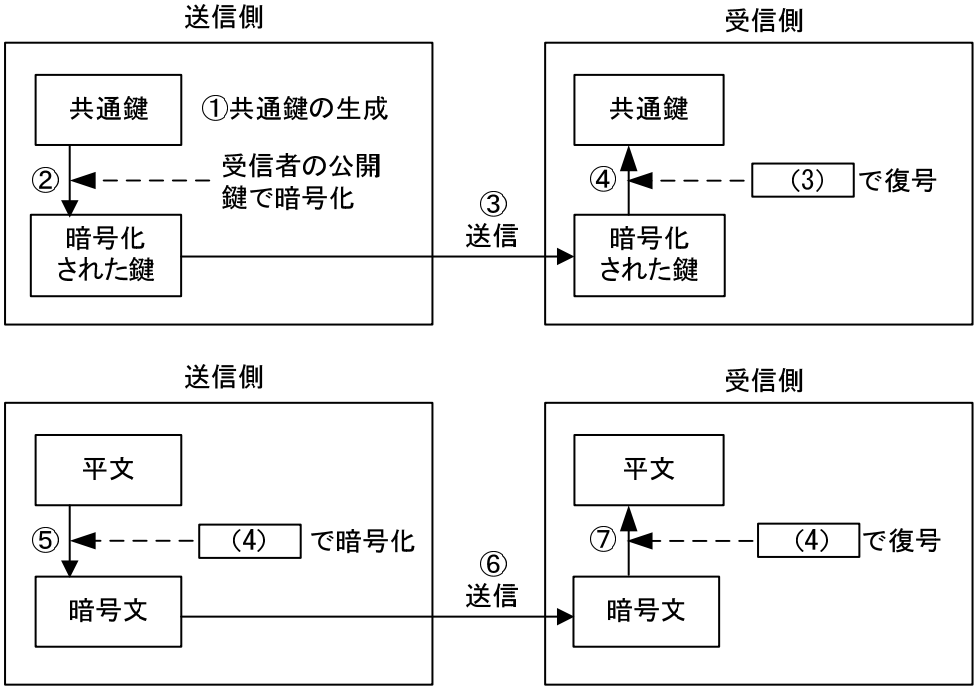


図３　ハイブリッド暗号方式の仕組み

**(3) ～ (4) の解答群**

ア．共通鍵　　イ．受信者の公開鍵
ウ．受信者の秘密鍵　　エ．送信者の公開鍵
オ．送信者の秘密鍵

＜設問３＞　次のなりすまし防止に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

なりすまし防止には，紙に記されるサインや押印と同じような役割を電子データで表し，送信データに付加する仕組みがある。これには，公開鍵暗号方式を利用した［(5)］があり，［(5)］にメッセージダイジェストを利用することで，送信者の正当性だけでなくデータの改ざんの有無も検知できる。

その手順を次に示す。

A 送信者は，平文のメッセージからハッシュ関数を利用してメッセージダイジェストを作成する。

B メッセージダイジェストを［(6)］で暗号化したものを［(5)］として利用し，平文のメッセージに付加して送信する。

C 受信者は受信した平文のメッセージから，Aと同じハッシュ関数を利用してメッセージダイジェストを生成する。

D 受信した［(5)］を［(7)］で復号して得たメッセージダイジェストと，Cで生成したメッセージダイジェストを比較する。比較結果が一致していれば受信したデータは改ざんされていないことと送信者の正当性を確認できる。

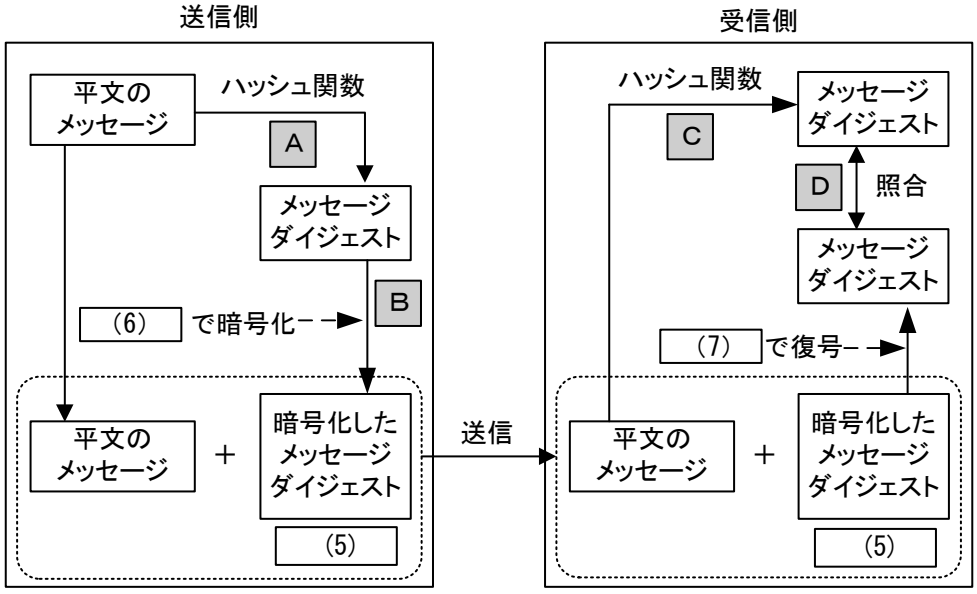


**図４　なりすまし防止の仕組み**

**(5) の解答群**

ア．サーバ証明書　　イ．ディジタル証明書
ウ．ディジタル署名　　エ．ルート証明書

**(6)，(7) の解答群**

ア．受信者の公開鍵　　イ．受信者の秘密鍵
ウ．送信者の公開鍵　　エ．送信者の秘密鍵