問題５　次の暗号化技術に関する各設問に答えよ。

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

インターネット上を流れるデータは,盗聴や改ざんといった脅威にさらされている。これらの脅威は，暗号化することにより，大幅に低減させることができる。暗号化方式には，次の２つがある。

１．［　(1)　］暗号方式

送信側は，暗号化かぎを使ってメッセージから暗号文を作り送信する。受信側は，暗号化かぎと同じ復号かぎを使用して，暗号文をメッセージに戻す。

この時に使用する暗号化かぎと復号かぎは同じなので，かぎは一方を厳重に管理していればよい。

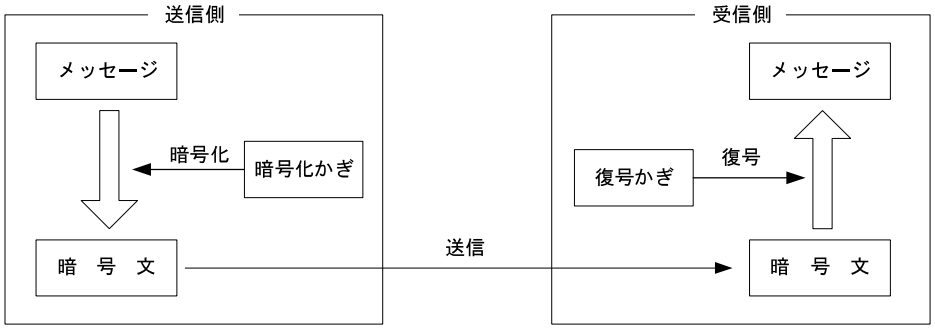

図１　［　(1)　］暗号方式によるデータの送信

２．［　(2)　］暗号方式

暗号化かぎと復号かぎは一方が分かっても他方を推測することはできない。したがって，かぎの管理は一方を厳重に管理していればよい。

この方式を用いて機密通信を行う場合，送信側は［　(3)　］を利用して暗号文を作り送信する。受信側は［　(4)　］を利用して復号する。

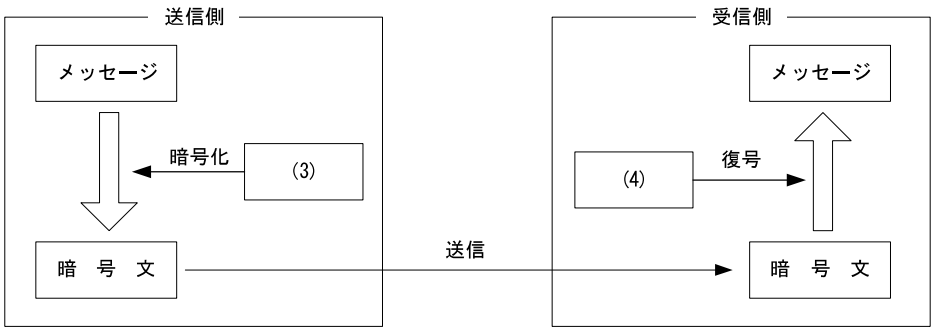

図２　［　(2)　］暗号方式による機密通信

(1)，(2) の解答群

ア．S/MIME　　イ．SSL
ウ．共通かぎ　　エ．公開かぎ
オ．電子かぎ　　カ．秘密かぎ

(3)，(4) の解答群

ア．受信側の公開かぎ　　イ．受信側の秘密かぎ
ウ．送信側の公開かぎ　　エ．送信側の秘密かぎ

＜設問２＞　次のディジタル署名に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ディジタル署名は，［　(2)　］暗号方式の技術を利用したもので，文書の改ざんの検出やなりすましを防止することができる。

ディジタル署名は，メッセージからハッシュ関数により生成されたダイジェストを暗号化し，元のメッセージとともに送信する。このとき暗号化に使われるかぎは［　(5)　］である。

受信側は，受け取ったディジタル署名を［　(6)　］を使って復号する。さらに，一緒に送られてきたメッセージを送信側と同じハッシュ関数を用いてダイジェストを作成し,復号して得たダイジェストと照合して,改ざんやなりすましの有無を判断する。

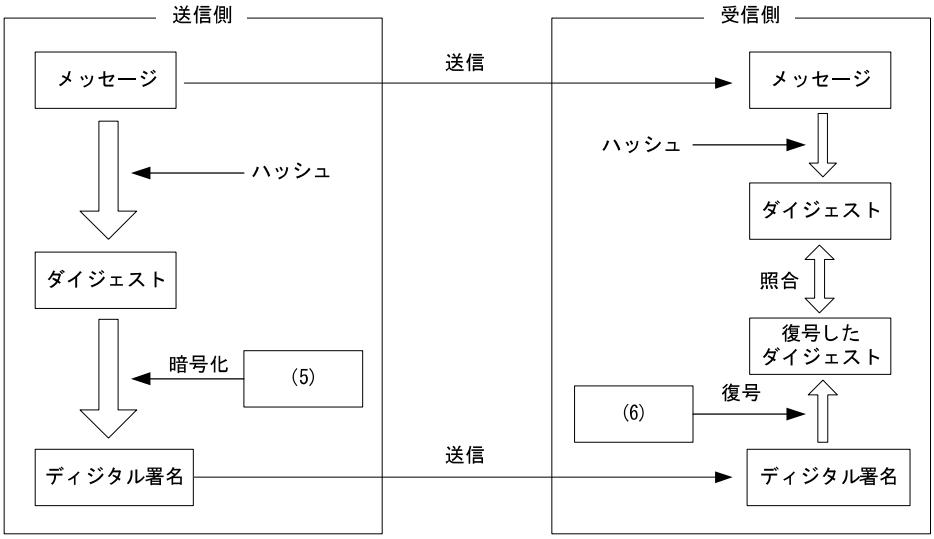

図３　ディジタル署名

(5)，(6) の解答群

ア．受信側の公開かぎ　　イ．受信側の秘密かぎ
ウ．送信側の公開かぎ　　エ．送信側の秘密かぎ

＜設問３＞　次のユーザ認証に関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

インターネットを利用した取引の場合，第三者が他人になりすまして不正にデータを搾取することがある。このようなりすましを防止するのがユーザ認証である。

インターネット上でユーザ認証を実現するには，［(7)］と呼ばれる組織と［(8)］と呼ばれる仕組みが必要になる。インターネット上のショッピングサイトを例にすると，次のようになる。

① ショッピングサイトの運営者は［(7)］に申請を行う。

② ［(7)］は，申請内容を審議し，合格した場合［(9)］を発行する。

③ インターネット利用者がショッピングサイトに接続すると，［(9)］が利用者に送られる。［(9)］に添付されている［(10)］を［(7)］の公開かぎで正しく復号できれば，このショッピングサイトは信頼できることになる。

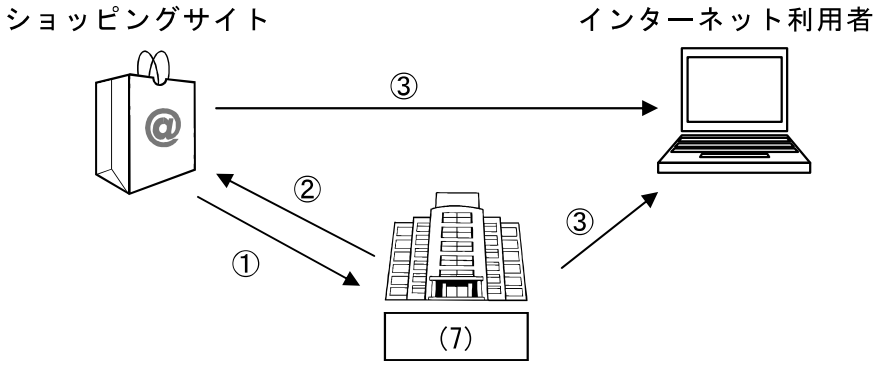

図４　ショッピングサイトの認証

(7)，(8) の解答群

ア．CA(Certification Authority)　　イ．DES(Data Encryption Standard)
ウ．MD(Message Digest)　　エ．PKI(Public Key Infrastructure)
オ．SHA(Secure Hash Algorithm)　　カ．RSA(Rivest, Sharmir, Adleman)

(9)，(10) の解答群

ア．ディジタルコンテンツ　　イ．ディジタルデバイド
ウ．ディジタル証明書　　エ．ディジタル書籍
オ．ディジタル署名　　カ．ディジタル認証