## 問題５　次のセキュリティ技術に関する各設問に答えよ。

＜設問１＞　次の暗号化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。

データを暗号化して通信を行う方法の代表的なものとして共通鍵暗号方式と公開鍵暗号方式がある。

共通鍵暗号方式は暗号化と復号に同じ鍵を使い，公開鍵暗号方式は暗号化と復号で異なる一組の鍵を使用し，一方を一般に公開するので公開鍵と呼び，もう一方の鍵は作成した本人だけが使用するので秘密鍵と呼ぶ。この二つの方式を，暗号化と復号に要する時間で比較すると，［(1)］。

また，図１のように５台のコンピュータが相互に暗号化したデータを送受信する場合，共通鍵暗号方式のみで行う場合に必要になる鍵の数は［(2)］個になり，公開鍵暗号方式のみで行う場合に必要になる鍵の組数は［(3)］組である。通信相手が多くなるほど鍵の数や鍵の漏えいに対する点から［(4)］の方が鍵の管理が容易である。

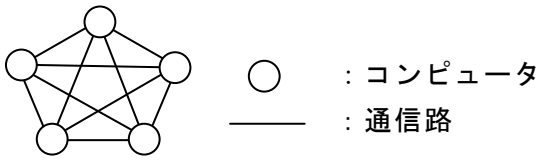


**図１　ネットワークの図**

**(1) の解答群**

ア．共通鍵暗号方式の方が長い
イ．共通鍵暗号方式の方が短い
ウ．どちらも同じである

**(2) ～ (4) の解答群**

ア．1　　イ．4　　ウ．5　　エ．10　　オ．20
カ．共通鍵暗号方式　　キ．公開鍵暗号方式

＜設問２＞　次のメッセージダイジェストに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ハッシュ関数は，任意の長さの入力データに対して固定長のハッシュ値を返すものである。また，ハッシュ値から元の入力データに戻すことができないという性質を持っている。

メッセージダイジェストとは，送信データ(平文のメッセージ)にハッシュ関数を施して得られるハッシュ値のことである。メッセージダイジェストを利用した通信を行うことで通信の途中で改ざんが行われていないことを証明できる(図２)。送信者は，平文のメッセージとメッセージダイジェストを一緒に送信し，受信者は，平文のメッセージに同じハッシュ関数を施してメッセージダイジェストを生成し，受信したメッセージダイジェストと照合して一致すれば平文のメッセージが改ざんされていないことを確認できる。

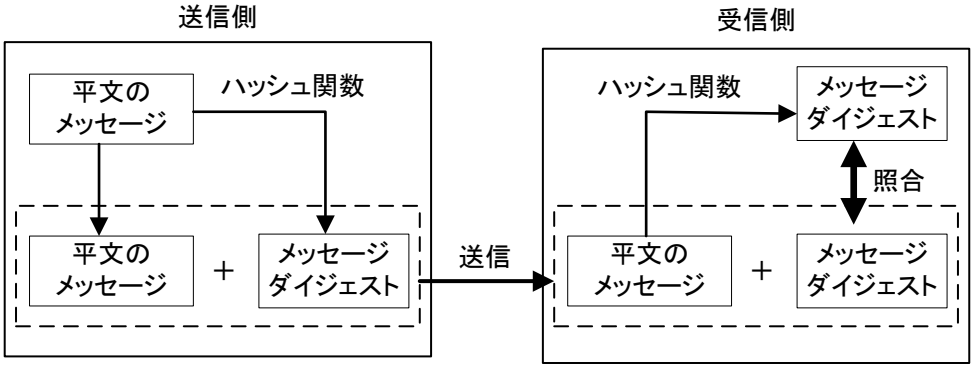


**図２　メッセージダイジェストを利用した通信**

また．送信者の正当性を受信者が確認する技術に，公開鍵暗号化方式を利用した［　(5)　］がある。これは任意の文字列を［　(6)　］で暗号化したものをデータに添付して送信し，受信者は添付された任意の文字列を［　(7)　］で復号するものである。この任意の文字列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改ざんの有無も確認できる。ただし，これだけでは鍵の正当性が確認できないので，［　(8)　］が発行するディジタル証明書を利用することで，より送信者の正当性が保証される。

**(5)，(8) の解答群**

ア．検証局　　イ．セッションキー
ウ．チャレンジ／レスポンス　　エ．ディジタル署名
オ．認証局　　カ．プリシェアードキー

**(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