第3問　暗号化に関する次の記述を読んで、設問1，2に答えよ。

JAB社はeビジネス市場の拡大や電子政府の実現、電子署名法の施行に伴い、PKI（Public Key Infrastructure）の重要性が確実に高まっていることを踏まえて、情報を伝送する場合のセキュリティの確保や情報を閲覧する者の本人確認、資格や属性の認証の実現手段を見直すことにした。

インターネットを介しての通信には、共通かぎ方式を採用している。

設問1　B（受信者）がA（送信者）の認証を、公開かぎ方式で行う場合の手順を図1に示す。図1中の空欄(a)，(b)に入れるべき適切な字句を解答群の中から選べ。

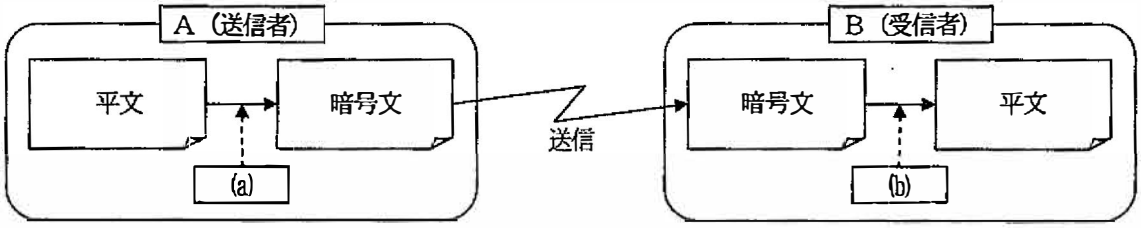


図1　ディジタル署名

解答群

ア　A（送信者）の公開かぎ　　イ　A（送信者）の秘密かぎ
ウ　B（受信者）の公開かぎ　　エ　B（受信者）の秘密かぎ

設問2　図1の手順を応用してメッセージの交換を行う場合の手順を図2に示す。図2中の空欄(c)～(e)に入れるべき適切な字句を解答群の中から選べ。なお、空欄(a)，(b)には図1と同じ字句が入るものとする。また、解答は重複して選んでもよい。

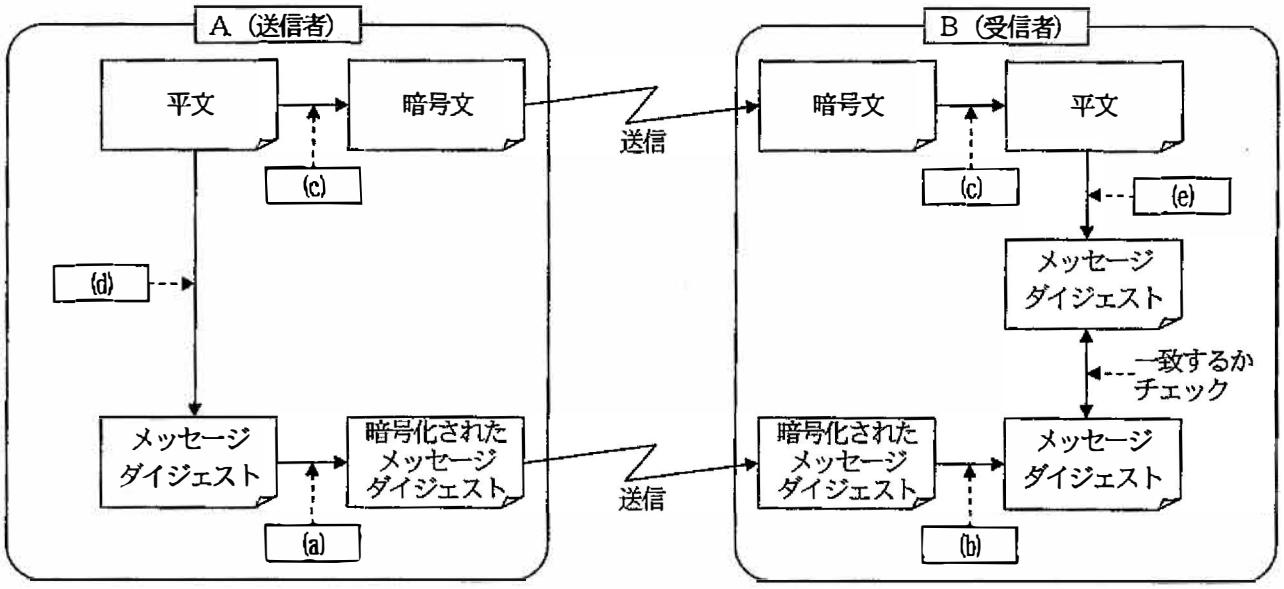


図2　メッセージ交換

解答群

ア　A（送信者）の公開かぎ　　イ　A（送信者）の秘密かぎ
ウ　B（受信者）の公開かぎ　　エ　B（受信者）の秘密かぎ
オ　共通かぎ　　カ　ハッシュ関数