第3問　ディジタル署名に関する次の記述を読んで、設問1～5に答えよ。

インターネット経由で取引先などとデータ（以下メッセージという）の交換を行う場合、メッセージの本文を暗号化するだけではセキュリティ面で安全とは言えないため、メッセージの交換相手の認証も行う必要がある。

この相手の認証を行うに当たって、暗号化と復号を各個人が所有する秘密鍵と公開鍵で行う公開鍵暗号方式の暗号化アルゴリズムを用いて、次の手順で送受信を行うことにした。

(1) 送信者Aは、メッセージ本文を、送信者Aと受信者Bが共有している共通鍵を使って、秘密鍵暗号方式で暗号化してBへ送る。

(2) 認証を行うために、送信者Aと受信者Bが共有しているハッシュ関数を用いて、送信者Aはメッセージダイジェストを生成し、生成したメッセージダイジェストを公開鍵暗号方式で暗号化して受信者Bへ送る。

(3) 受信者Bは、受け取ったメッセージダイジェストを公開鍵暗号方式で復号する。さらに、メッセージ本文を共通鍵で復号し、復号した本文からハッシュ関数を使ってメッセージダイジェストを作る。

(4) 受信者Bは、送信者Aから受け取って復号したメッセージダイジェストと、自分でメッセージ本文から生成したメッセージダイジェストが一致しているかどうかをチェックすることによって、相手を認証する。

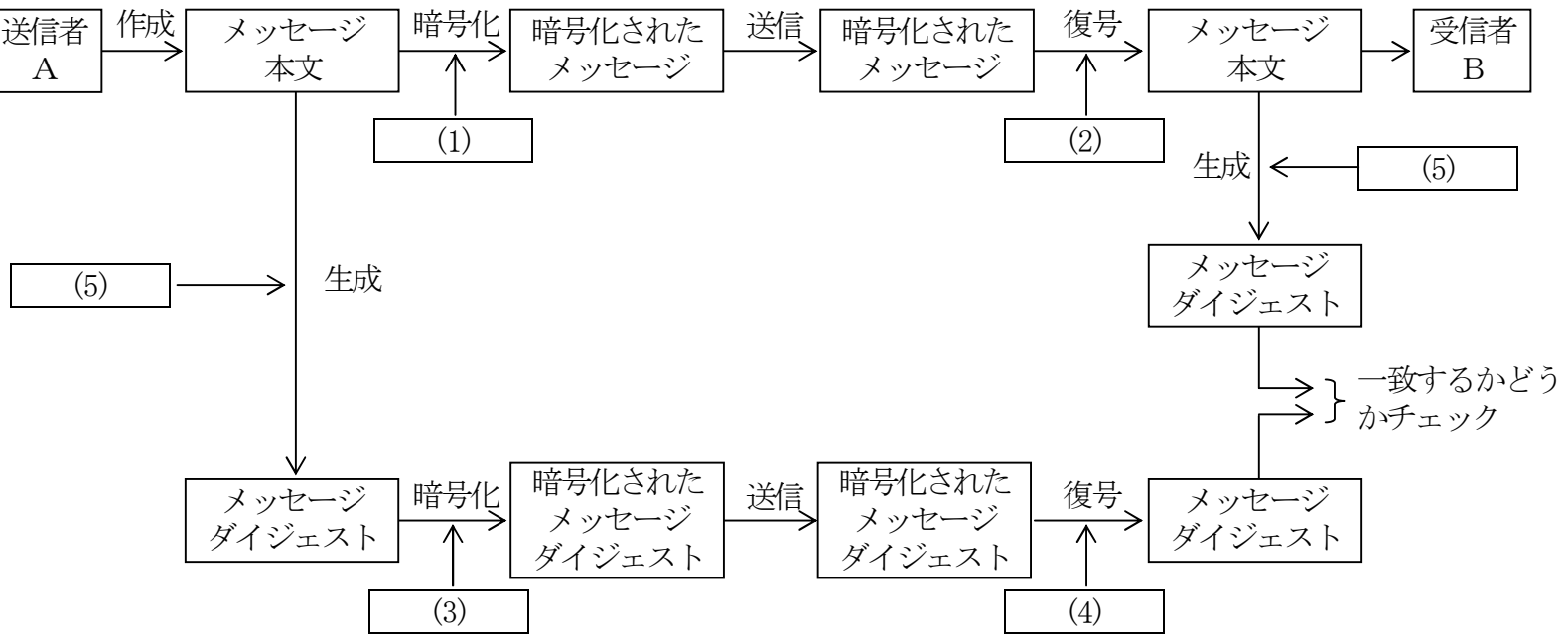

図　認証を可能にしたメッセージ送受信の手順

設問１　メッセージの漏えいを防止するために、図中の空欄(1)と(2)に入れる字句の組合せとして適切なものを解答群の中から選び(a)に答えよ。

解答群

	(1)	(2)
ア	送信者Aの公開鍵	送信者Aの秘密鍵
イ	送信者Aの秘密鍵	送信者Aの公開鍵
ウ	送信者Aと受信者Bの共通鍵	送信者Aと受信者Bの共通鍵
エ	受信者Bの公開鍵	受信者Bの秘密鍵
オ	受信者Bの秘密鍵	受信者Bの公開鍵

設問２　送信者のなりすましを防止するために、図中の空欄(3)と(4)に入れる字句の組合せとして適切なものを解答群の中から選び(b)に答えよ。

解答群

	(3)	(4)
ア	送信者Aの公開鍵	送信者Aの秘密鍵
イ	送信者Aの秘密鍵	送信者Aの公開鍵
ウ	送信者Aと受信者Bの共通鍵	送信者Aと受信者Bの共通鍵
エ	受信者Bの公開鍵	受信者Bの秘密鍵
オ	受信者Bの秘密鍵	受信者Bの公開鍵

設問３　図中の空欄(5)に入れる適切な字句を解答群の中から選び(c)に答えよ。

解答群

ア　PIN　　イ　セション鍵　　ウ　チャレンジコード　　エ　トリプルDES
オ　ハッシュ関数　　カ　楕円曲線暗号

設問４　図の方式を採用して通信を行った場合、設問１，２の二つの効果を得ることの他に得られる効果として適切なものを、解答群の中から選び(d)に答えよ。

解答群

ア　送信者の秘密鍵の漏えい防止　　イ　受信者の公開鍵の漏えい防止
ウ　送信メッセージの改ざんの防止　　エ　受信者の受信したことの否認の防止
オ　送信メッセージの窃取の防止　　カ　受信者のなりすましの防止

設問５　この方式を採用して通信を行う場合、相手の公開鍵が真に本人のものである必要がある。公開鍵の正当性を証明するために公開鍵の電子署名を作成する機関として適切なものを、解答群の中から選び(e)に答えよ。

解答群

ア　CRL　　イ　RADIUS　　ウ　検証局　　エ　認証局　　オ　登録局