

第3問 暗号化に関する記述を読んで、設問1、2に答えよ。

I社は、インターネットのグローバルエリアを利用して情報の共有や、機密情報のやり取りを行っている。  
下記の表にある共通鍵暗号方式の長所と、公開鍵暗号方式の長所の両方を生かして、情報のやり取りを行えないか検討することにした。

共通鍵暗号方式	長所	・処理が比較的高速である。
	短所	・鍵の受渡し方法を別に考える必要がある。 ・複数の相手とやり取りする際、鍵の数が増える。
公開鍵暗号方式	長所	・鍵の配布が容易である。 ・鍵の管理が容易である。
	短所	・暗号化や復号の処理に時間がかかる。 ・大量のデータ処理には向いていない。

設問1 暗号技術に関する次の記述を読んで、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。

暗号技術には、暗号化に利用する鍵と復号に利用する鍵に同じ鍵を利用する共通鍵暗号方式と、暗号化と復号で異なる鍵を利用する公開鍵暗号方式がある。

自分を含め100人の間で送受信すると、共通鍵暗号方式では、全体で  種類の鍵が必要であり、公開鍵暗号方式では、全体で  種類の鍵が必要である。

解答群

ア 50	イ 99	ウ 100	エ 200
オ 4,950	カ 5,000	キ 9,900	ク 10,000

設問2 I社は検討の結果、共通鍵暗号方式の処理が高速という長所と公開鍵暗号方式の鍵の管理、配布が容易というそれぞれの長所を組み合わせた、ハイブリッド暗号方式を導入することになった。次の図の空欄（c）～（e）に入れるべき適切な字句を、解答群の中から選べ。

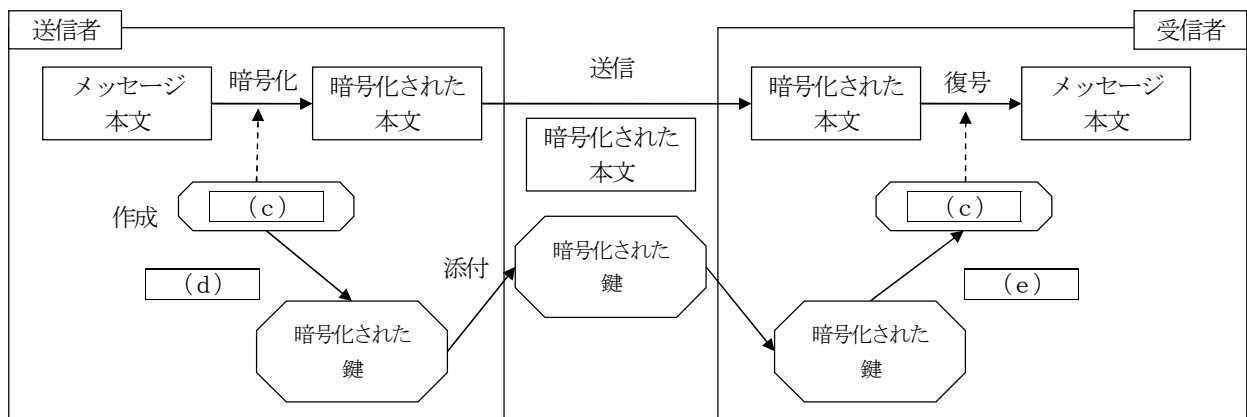


図 ハイブリッド暗号方式

解答群

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