

問1 インターネットでは、情報の安全なやり取りを実現するために暗号化技術が利用されている。

代表的な暗号化方式には、公開鍵暗号方式と共通鍵暗号方式がある。

(1) 公開鍵暗号方式

鍵を安全に通信相手に渡すことが容易であり、鍵の所有者が管理しなければならない鍵の数も通信相手の人数に関係なく1対であるが、処理速度が遅く、大量のデータ処理や高速処理には向いていない。

(2) 共通鍵暗号方式

データ処理速度も比較的速く、扱いやすいが、管理しなければならない鍵の数が通信相手の人数分だけ必要となり、鍵をどのように受け渡すかという大きな問題もある。例えば、通信相手が2人であれば管理しなければならない鍵は1個で済むが、3人であれば全部で3個、4人であれば全部で6個と、管理しなければならない鍵の数は増えていくことになる。

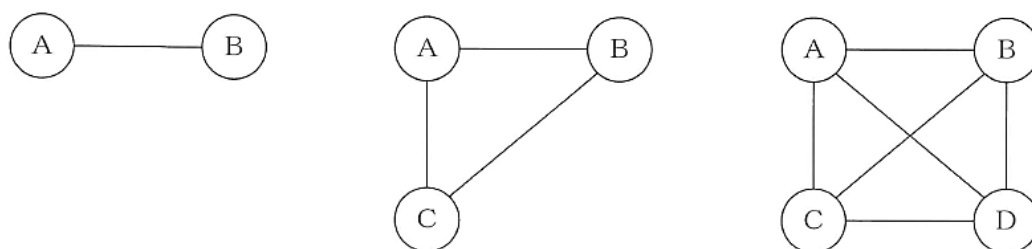
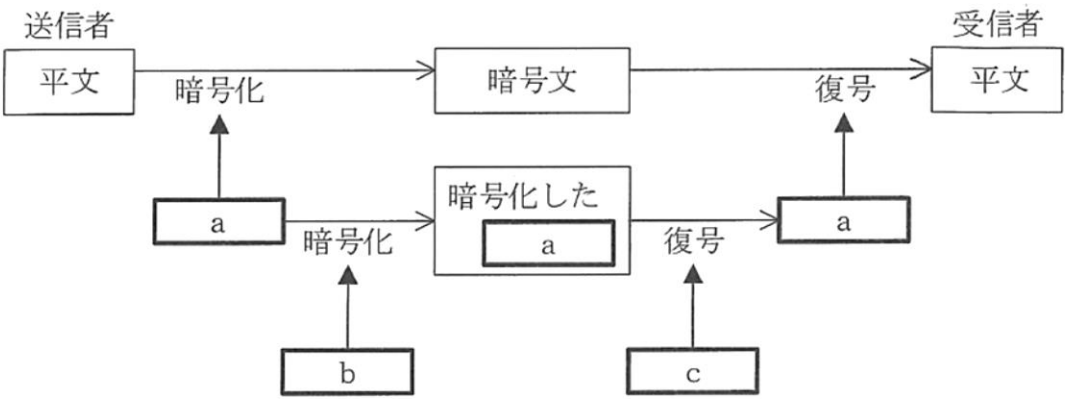


図1 通信相手の数と通信経路（管理しなければならない鍵の数）

このような双方の欠点を補い合う形で用いられている暗号方式に、セッション鍵暗号方式がある。セッション鍵暗号方式は、メール用暗号化のプログラムPGPや、暗号化・認証プロトコルSSLなどに採用されている。

設問 セッション鍵暗号方式の仕組みを表す図中の a ～ c に入れる鍵の組合せとして、適切なものを解答群の中から選べ。



解答群

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