問040003問題

暗号通信に関する次の記述を読んで，設問に答えよ。

安全でない通信経路を利用する２者が，秘密の共通かぎを安全に共有する方式としてDiffie-Hellman法(以下，ＤＨ法という)が知られている。ＤＨ法で利用者Ａと利用者Ｂが共通かぎＫを共有するまでの手順は，次のとおりである。

（１） 素数ｐと，ｐよりも小さいある自然数αが公開されていて，利用者Ａと利用者Ｂがともに知ることができる。

（２） 利用者Ａは，ｐよりも小さい任意の自然数X_Aを選び，秘密かぎとして保持するとともに，次の式で得られる公開かぎY_Aを利用者Ｂに送る。

$$Y_A = \alpha^{X_A} \bmod p$$

ここで，ｘｍｏｄｙは整数ｘを整数ｙで割った余り(剰余)である。

（３） 利用者Ｂは，ｐよりも小さい任意の自然数X_Bを選び，秘密かぎとして保持するとともに，次の式で得られる公開かぎY_Bを利用者Ａに送る。

$$Y_B = \alpha^{X_B} \bmod p$$

（４） 利用者Ａは，利用者Ｂの公開かぎY_Bを使って，次の式によって共通かぎＫを得る。

$$K = Y_B^{X_A} \bmod p$$

（５） 利用者Ｂは，利用者Ａの公開かぎY_Aを使って，次の式によって利用者Ａと同じ共通かぎＫを得る。

$$K = Y_A^{X_B} \bmod p$$

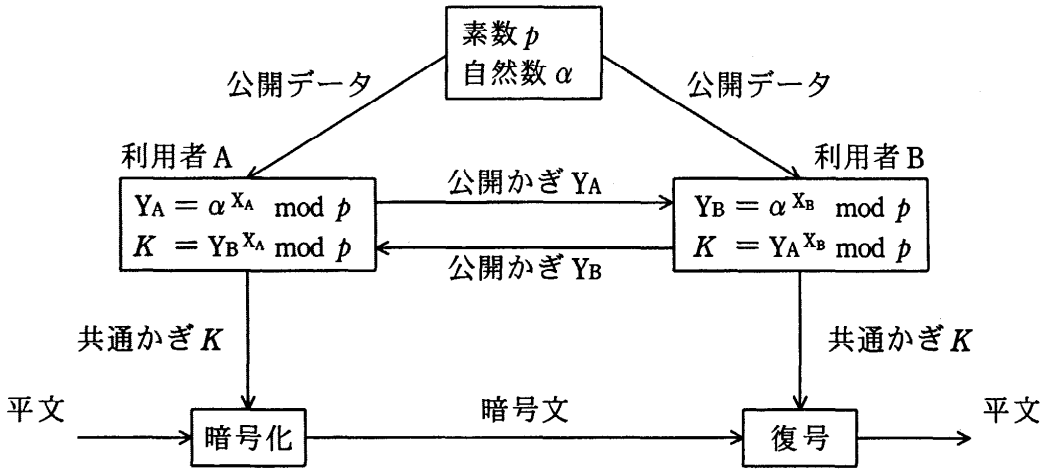

図　DH 法を使った機密情報の通信

ＤＨ法によるかぎ共有を利用して，図に示すように，安全でない通信経路を利用する２者間で機密情報を送信する仕組みを作る。まず，利用者Ａと利用者ＢはＤＨ法を使って，共通かぎＫを共有する。次に，利用者Ａは平文を共通かぎＫを使って暗号化して送信する。利用者Ｂは受信した暗号文を共通かぎＫを使って復号して，元の平文を得ることができる。

設問 次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

ＤＨ法は，目的が［　ａ　］に限定されたアルゴリズムであるが，この方式の安全性はほかの公開かぎ暗号と同じく計算の一方向性に基づいている。すなわち，ＤＨ法において，素数ｐの値が十分に大きい場合，秘密かぎから公開かぎを求めるのは容易であるが，公開かぎから秘密かぎを求めるのは非常に困難である。

反対に，素数ｐの値が小さい場合には，かぎの値が小さくなるので公開かぎから秘密かぎを短時間で求めることも可能であり，安全性に問題がある。例えば，利用者Ａと利用者Ｂが使う通信経路上に通信を傍受している第三者Ｃがいて，公開されている素数ｐが７，αが５であることに加え，利用者Ａが送った公開かぎY_Aが６，利用者Ｂが送った公開かぎY_Bが３であることを知ったとする。このとき，共通かぎＫの値は，［　ｂ　］であることが容易に分かる。

また，ＤＨ法は，通信経路上の第三者Ｃが，利用者Ａから送られる情報を，にせの情報にすりかえて利用者Ｂに送信する中間者攻撃に対して，弱いことが知られている。中間者攻撃を防ぐためには公開かぎに信頼できる第三者によるディジタル署名をつけるなどの対策が必要である。さらに，第三者Ｃが暗号文を傍受してそれを手掛かりとして共通かぎＫを見つけるリスクもあるので，継続的な通信の安全性を高めるための対策として，共通かぎＫの値が十分に大きいものを使うだけでなく，［　ｃ　］も有効である。

ａ，ｃに関する解答群

ア　共通かぎＫの更新間隔の短縮
イ　公開かぎY_A，Y_Bの交換回数の削減
ウ　公開かぎの交換
エ　秘密かぎによる情報の復号
オ　秘密の共通かぎの共有
カ　より大きな値の素数ｐの使用

ｂに関する解答群

ア　０　　イ　１　　ウ　２　　エ　３
オ　４　　カ　５　　キ　６