問040003解説

◆解答

設問　a　オ　　b　キ　　c　ア

◆解説

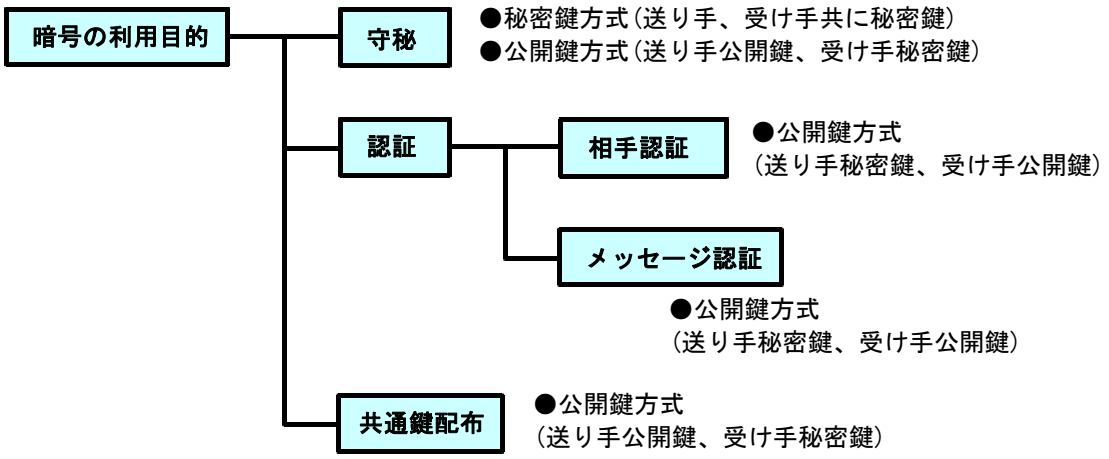
共通鍵暗号方式に関する問題である。

暗号化の利用目的

鍵を利用することによって、情報が保証されるのは送り手なのか受け手なのかを十分に考慮して検討する必要がある。特に、公開鍵を利用する場合、秘密鍵を利用するのは保証される必要がある人であり、公開鍵は秘密鍵を用いる人のものが利用される。

署名やメッセージ認証の場合、他の送り手の「なりすまし」による悪用を避けるために、送り手が自分の秘密鍵を使用して署名やメッセージの暗号文を作成し、送り手の公開鍵で受け手が暗号文から平文を作成させることになる。この方法を利用することによって、送り手が唯一になり、送り手の保証が可能となる。署名もメッセージも保証された送り手のみが送信したものになる。

秘密鍵を配布する場合、受け手に安全に秘密鍵を届けるためには、送り手は受け手の公開鍵で暗号化し、受け手のみが自分の秘密鍵で復号できると、安全に鍵を配布することができる。



利用者Ａと利用者Ｂが共通鍵Ｋを共有するまでの手順

① 素数ｐとｐより小さい任意の自然数αが公開されている。ｐ＝７、α＝５

② 利用者Ａは任意の自然数X_Aを秘密鍵として保持する。式$Y_A=\alpha^{X_A} \bmod p$から公開鍵を求め、利用者Ｂに送る。$Y_A=6$

③ 利用者Ｂは任意の自然数X_Bを秘密鍵として保持する。式$Y_B=\alpha^{X_B} \bmod p$から公開鍵を求め、利用者Ａに送る。$Y_B=3$

④ 利用者Ａは、利用者Ｂの公開鍵Y_Bを使って、$K=Y_B^{X_A} \bmod p$から共通鍵Ｋを求める。

⑤ 利用者Ｂは、利用者Ａの公開鍵Y_Aを使って、$K=Y_A^{X_B} \bmod p$から共通鍵Ｋを求める。

以上の①～⑤の手順を利用すると、公開鍵Ｋを求めることができる。ここでは、ｐ、αは公開されている値であり、Y_A、Y_Bは保持している値であるから、逆算して、X_A、X_Bを求めることができる。X_A、X_Bが分かるとＫを計算することが可能になる。

設問１

aはＤＨ法の目的で、秘密の共通鍵を安全に共有する方式である。答は秘密の共通鍵の共有で、求める答はオである。

bは次の要領で計算する。

①　$６＝５^{X_A} \bmod ７$ の式からX_Aを求めると、$１２５ \bmod ７＝６$となり、$X_A＝３$。

②　$３＝５^{X_B} \bmod ７$ の式からX_Bを求めると、$３１２５ \bmod ７＝３$となり、$X_B＝５$。

③　$K＝３^{３} \bmod ７＝２７－２１＝６$、$K＝６^{５} \bmod ７＝７７７６－７７７０＝６$

④　共通鍵Ｋは６となる。求める答はキとなる。

cは利用者Ａ、Ｂが任意の自然数X_A、X_Bを選び替えすることによって、共通鍵Ｋの更新が可能であるから、共通鍵Ｋの更新間隔の短縮が有効となる。求める答はアとなる。