

【No. 49】 ある暗号文を解読するためには、公開されている正の整数 m , n と $s^2 = m(\text{mod } n)$ を満たす秘密の正の整数 s を知っている必要がある。ボブは、アリスが s を知っているかどうかを、 s の値を直接尋ねずに確かめたい。ここでボブは、次の手順で生成される x と y を報告するようアリスに依頼した。

手順1. ランダムな正の整数 r を生成する。

手順2. r をもとにして $x = r^2 (\text{mod } n)$ と $y = r \cdot s (\text{mod } n)$ を計算する。

このようにして生成された x と y は、 $y^2 = r^2 \cdot s^2 = x \cdot m (\text{mod } n)$ を常に満たすので、ボブはアリスの報告した x と y が $y^2 = x \cdot m (\text{mod } n)$ を満たせば、アリスが s を知っているかと判定する。

いま、アリスは実際には s を知らないが、あらかじめ用意した x と y を報告することで、自分が s を知っているかとボブに信用させたい。 $m = 12$, $n = 33$ であり、アリスの用意した x と y のうち y が 24 であるとき x として最も妥当なのはどれか。

ただし、 $\text{mod } n$ は n を法とする剰余類を表す。

1. 0 2. 5 3. 10 4. 15 5. 20

面白い設定のような気がしますが、これだけ数字が限られていて、しかも選択肢があるため、選択肢をしらみつぶしで容易に解けてしまうと思うのですが、どうでしょうか。

解答

$$y^2 = 24^2 = 576 \equiv 15 (\text{mod } 33)$$

であるので、こうなるものを選択肢から選べばよい。明らかに x は 0 ではなく、他について、

$$5 \cdot 12 = 60 \equiv 27 (\text{mod } 33)$$

$$10 \cdot 12 = 120 \equiv 54 \equiv 21 (\text{mod } 33)$$

$$15 \cdot 12 = 180 \equiv 81 \equiv 15 (\text{mod } 33)$$

$$20 \cdot 12 = 240 \equiv 42 \equiv 9 (\text{mod } 33)$$

であるので、 x としては 15 が適している。