学籍番号：

2005 年 6 月 13 日

情報工学序説　　名前：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　得点：＿＿＿＿＿＿/4

小テスト

リエからヒデへ通信をおこなうときに関する問いである．

1. 以下の記述は，それぞれどういう意味があるか，あるいは不可能か，適切な解答を次の 3 つから選んで，書き込みなさい：暗号文の送付，電子署名の認証，不可能．

   a. リエは，自分の秘密鍵でメッセージ M を暗号化してヒデに送り，
   ヒデにはリエの公開鍵で復号してもらうことを要請する．　電子署名の認証

   b. リエは，ヒデの秘密鍵でメッセージ M を暗号化してヒデに送り，
   ヒデにはヒデの公開鍵で復号してもらうことを要請する．　不可能

   c. リエは，リエの公開鍵でメッセージ M を暗号化してヒデに送り，
   ヒデにはヒデの秘密鍵で復号してもらうことを要請する．　不可能

   d. リエは，ヒデの公開鍵でメッセージ M を暗号化してヒデに送り，
   ヒデにはヒデの秘密鍵で復号してもらうことを要請する．　暗号文の送付

2. リエからヒデへ，メッセージ M をヒデの公開鍵 $(e = 3, n = 55)$ で暗号化して送ってもらった値 C が 9 であった．ヒデの秘密鍵 $(d = 7)$ を使って復号化した値 $M = C^d \bmod n$ を求めよ．必要であれば $26^2 \bmod 55 = 16$，$26^3 \bmod 55 = 31$ を使ってよい．

$$
\begin{aligned}
M &= 9^7 \bmod 55 \\
&= 9^{1+2+4} \bmod 55 \\
&= (9 \bmod 55) \times (9^2 \bmod 55) \times (9^4 \bmod 55) \\
&= (9 \bmod 55) \times (9^2 \bmod 55) \times (9^2 \bmod 55) \times (9^2 \bmod 55) \\
&= 9 \times 26 \times 26 \times 26 \bmod 55 \\
&= 9 \times 31 \bmod 55 \\
&= 279 \bmod 55 \\
&= 4
\end{aligned}
$$