

1. 以下の文章を読み、下の設問に答えなさい。

社内の機密情報をケンジに伝えるために、ユキは暗号通信を用いることにした。現在用いられている暗号方式には、DES などの (あ) 暗号と、(い)、(う) などの (え) 暗号に大きく分けることができる。

(あ) 暗号は、シーザ暗号以来約 2000 年に渡る長い歴史を有するが、重大な問題点が内在している。それは (お) と呼ばれる問題である。(え) 暗号は、この (お) を解決した暗号方式である。しかし、(え) 暗号は、(あ) 暗号と比べると演算が複雑で、計算に時間がかかるなどの欠点を有するため、実際のアプリケーションでは、(か) と呼ばれる方式が用いられる。

(え) 暗号の一方式である (い) は、MIT の 3 人の研究者 Rivest, Shamir, Adleman により提案された方式であり、(き) の困難さにその安全性の根拠をおく暗号である。一方、(う) は、<sup>(1)</sup>離散対数問題 の困難さにその安全性の根拠をおいている。離散対数問題の困難さを用いるという考え方自体は、(え) 暗号のアイデアを提案した Diffie と Hellmann も着目していた。実際、Diffie と Hellmann が (え) 暗号のアイデアを提案した 1976 年の論文には、離散対数問題の困難さを用いた (く) も提案されている。

(い) は、暗号化だけでなく、デジタル (け) にも容易に適用できるので、ユキは、ケンジへの通信に (い) を用いることにした。(い) を用いた場合のユキの公開鍵を  $(n_Y, e_Y)$ 、秘密鍵を  $d_Y$ 、ケンジの公開鍵を  $(n_K, e_K)$ 、秘密鍵を  $d_K$  とする。ユキがケンジに通信内容を暗号化して送信する場合、(こ) を用いて暗号化し、暗号文を受信したケンジは、(さ) を用いて復号する。具体的には、暗号化対象となる平文  $M$  は

(2)

により暗号文  $C$  へと変換される。一方、受信された暗号文  $C$  は

(3)

により平文  $M$  に変換される。

問 1 (あ)、(い)、(う)、(え)、(お) に適する語句を記しなさい (各 4 点)。

- (あ) 秘密鍵 [対称鍵でも可]。
- (い) RSA 暗号
- (う) エルガマル暗号 (など)
- (え) 公開鍵暗号 [非対称鍵でも可]。
- (お) 鍵配送問題

問 2 (か) に適する語句を記し (4 点)、その内容を簡単に説明しなさい (6 点)。

- (か) ハイブリッド方式
  - 通信内容そのものを公開鍵暗号で送るのは、計算量の観点から望ましくないので、通信内容は秘密鍵暗号方式で暗号化することにし、秘密鍵暗号方式の鍵を公開鍵暗号方式で暗号化して送信する。
  - \* 両者の長所を組み合わせるなどの解答は全て不可。

問 3 (き)、(く)、(け) に適する語句を記しなさい (各 4 点)。

- (き) 素因数分解
- (く) 鍵共有法
- (け) 署名

問4 (こ), (さ) に適する記号を記しなさい (各4点) .

(こ)  $(n_K, e_K) e_K$  だけでも良い .

(さ)  $(n_K, d_K) d_K$  だけでも良い .

問5 下線部 (1) に関する以下の文章を完成させなさい . 解答用紙には , 答えのみ記入すれば良い (各4点) .

『離散対数問題とは ,  $(\text{し})$   $p$  に対して ,  $y = g^x \pmod{p}$  なる関係があるときに ,  $(\text{す})$  ,  $(\text{せ})$  ,  $(\text{そ})$  より  $(\text{た})$  を求める問題である 』

(し) 素数

(す),(せ),(そ)  $y, g, p$

(そ)  $x$

問6 (2),(3) に適する数式を記しなさい (各5点) .

(2)  $C \equiv M^{e_K} \pmod{n_K}$

(3)  $M \equiv C^{d_K} \pmod{n_K}$

\* この部分は , RSA 署名までは要求していない .

\* そこまで正しく書いていれば正解とした .

問7 ユキの公開鍵 , 秘密鍵の決定に関する以下の文章を完成させなさい . 解答用紙には , 答えのみ記入すれば良い (各4点) .

『ユキの公開鍵の一つ  $n_Y$  を計算するためには , あらかじめ大きな素数を二つ選ぶ必要がある . これらを  $p_Y, q_Y$  とすると ,  $n_Y = (\text{ち})$  となる . 同時に , オイラー数  $\phi(n_Y) = (\text{つ})$  を求めておく .  $\phi(n_Y)$  と互いに素となる整数を  $e_Y$  とすれば ,  $(\text{て})$  を満たす  $d_Y$  が秘密鍵になる 』

(ち)  $p_Y q_Y$

(つ)  $(p_Y - 1)(q_Y - 1)$

(て)  $e_Y d_Y \equiv 1 \pmod{\phi(n_Y)}$

2. 以下を計算しなさい (各4点) .

問8  $24^{23} \pmod{77} = 19$

問9  $\log_7 4 \pmod{11} = 6$

– 答えがあっていれば OK .

– 地道に計算する .

– 問9で , 離散対数問題の意味を理解していない解答が多かった . ー , 残念!