情報関係基礎

学習指導要領（4）- 思・判・表 - ア
学習内容（4）- ア ネットワークの仕組みと構成要素

第 2 問 （必答問題） 次の文章を読み，後の問い(問 1 ～ 3)に答えよ。(配点 35)

ソリティア帝国が近年不穏な動きをみせている。これを警戒したシャッフル王国のシャッフル王は，国境の砦(とりで)と王都との間の通信文を暗号化することにした。

元の通信文を**平文**，平文を暗号化したものを**暗号文**と呼ぶ。シャッフル王国では♡，♠，♣，◇の 4 種類の文字を使っているのだが，文字を見間違えにくくするため，暗号文では♡と♠の 2 種類だけを使う。

問 1 次の文章を読み，空欄 ア ～ オ に入れるのに最も適当なものを，後の解答群のうちから一つずつ選べ。

シャッフル王国の暗号化では，次の表 1 のルールにしたがって，平文中の文字をそれぞれ対応する文字列に置き換える。例えば，♣♠♣という平文を暗号化すると♠♠♡♠♡♠♠♡という暗号文になり，♡♣◇♣という平文であれば ア という暗号文になる。また，♠♡♡♠♡という暗号文であれば イ という平文に，♠♠♠♠♠♡♠♡♠♡♡は ウ に，それぞれ復号できる。

表 1 シャッフル王国での暗号化のルール

平文中の文字	♡	♠	♣	◇
暗号文中での対応する文字列	♡	♠♡	♠♠♡	♠♠♠

このルールで平文を暗号化したとき，♠ 1 文字だけの暗号文になることや，エ という 4 文字の暗号文になることはない。また，平文を暗号化して オ が得られることもない。

ア の解答群

⓪ ♡♠♡♠♠♠♠♠♠♡　　① ♡♠♠♡♠♠♠♠♠♡

② ♡♠♠♠♡♠♡♠♠♠　　③ ♠♡♠♠♡♠♡♠♠♠

イ ・ ウ の解答群

⓪ ♡♣♡　　① ♠♡♠　　② ♠♠♡

③ ♠♡♠♡　　④ ♠◇♣♡　　⑤ ◇♠♠♣

⑥ ♡♠♠♣◇　　⑦ ♣◇♣♡♠　　⑧ ◇♣♠♠♡

エ の解答群

⓪ ♡♡♡♡　　① ♡♠♠♡

② ♡♠♠♠　　③ ♠♠♡♡

④ ♠♠♠♡　　⑤ ♠♠♠♠

オ の解答群

⓪ 文字数が奇数の文　　① 文字数が偶数の文

② ♡より♠を多く含む文　　③ ♠より♡を多く含む文

④ ♡♠で終わる文　　⑤ ♠♠で終わる文

情報関係基礎

問 2　次の文章を読み，空欄 カ ～ サ に入れるのに最も適当なものを，後の解答群のうちから一つずつ選べ。ただし，空欄 コ ・ サ の解答の順序は問わない。

国境近くには音楽といたずらが大好きな妖精が住んでいる。この妖精が暗号文を面白がり，その中の文字を魔法で♬に書き換えるいたずらを始めた。このせいで，砦から「♠♠♡♠♡」と送ったとしても，王都には「♠♬♡♠♡」が届いてしまうかもしれない。困ったシャッフル王は対策を検討し，次のように暗号文の末尾に「おまけ」を 1 文字書き加える方法を思いついた。

- 暗号文中の♡の数が偶数なら，おまけとして♡を文末に加える。
- 暗号文中の♡の数が奇数なら，おまけとして♠を文末に加える。

例えば，♠♡♠♡という暗号文であれば，♡を二つ含むのでおまけとして♡を加え，♠♡♠♡♡とする。また，♡♡♠♠♡という暗号文であれば，おまけとして カ を加える。

おまけを加えることで，いたずらで書き換えられた文字を復元しやすくなる。例えば，♡♡♠♬♠♡♡という文の「♬」は，おまけが「♡」であることから，キ だったとわかる。どんな暗号文でも，おまけを加えると必ず ク になる。このことを使えば，1 文字だけが♬になった文が届いた場合には，元の文字を必ず復元できる。 ケ が届いたのであれば♬を♡に，そうでなければ♬を♠に書き換えればよい。

おまけを加えても，2 文字以上が♬になってしまうと復元は難しい。例えば，♠♡♠♠♬♬♡♠という文の「♬♬」については，おまけが「♠」であることから，「♡♡」「♡♠」「♠♡」「♠♠」の 4 通りの可能性のうち コ か サ のどちらかだったことはわかる。しかし，そのどちらだったのかはわからない。

経験上，2 文字以上が♬に書き換えられたことはなかった。そこでシャッフル王はおまけを加えた暗号文を砦との通信に使うことにした。

カ ・ キ の解答群

⓪ ♡　① ♠　② ♣　③ ◇　④ ♬

ク ・ ケ の解答群

⓪ 文字数が奇数の文
① 文字数が偶数の文
② ♡の数が奇数の文
③ ♠の数が奇数の文
④ ♡の数が偶数の文
⑤ ♠の数が偶数の文

コ ・ サ の解答群

⓪ ♡♡　① ♡♠　② ♠♡　③ ♠♠

情報関係基礎

問 3　次の文章を読み，空欄 シ ～ ツ に入れるのに最も適当なものを，後の解答群のうちから一つずつ選べ。

ソリティア帝国には野心に燃える王子がおり，次期皇帝となるための大手柄を求めていた。シャッフル王国の暗号に目をつけた王子は，解読を目指してスパイを送り込み，次の情報を得た。

情報 1　平文中の♡，♠，♣，◇のどの 1 文字を暗号化しても，♡と♠だけを使った 1 ～ 3 文字のそれぞれ異なる文字列になる。

情報 2　平文中のある 1 文字を暗号化すると文字列 x，ほかの 1 文字を暗号化すると文字列 y になるとき，x の先頭から何文字を切り出しても y にはならない。例えば，平文中の♡を暗号化した結果が♡♠♠の 3 文字だとすると，♠，♣，◇のどの 1 文字を暗号化しても♡にも♡♠にもならない。

さらに，スパイに収集させた大量の平文と暗号文から，平文の文頭 1 文字と暗号文の文頭 3 文字の割合を集計し，次の表 2 と表 3 を得た。

表 2　平文の文頭 1 文字の割合

文頭 1 文字	♡	♠	♣	◇
割　合	40 %	30 %	20 %	10 %

表 3　暗号文の文頭 3 文字の割合

文頭 3 文字	♡♡♡	♡♡♠	♡♠♡	♡♠♠	♠♡♡	♠♡♠	♠♠♡	♠♠♠
割　合	10 %	10 %	10 %	10 %	10 %	20 %	20 %	10 %

王子は，「平文中の♡を暗号化すると♠ 1 文字になる」と仮定してみた。そうだとすると，**情報 2** をふまえれば，平文中の♠，♣，◇のどの 1 文字を暗号化した結果も シ はずなので，文頭が♠の暗号文はすべて文頭が♡の平文に対応する。しかし，表 3 によれば，文頭が♠の暗号文の割合は ス %であり，文頭が♡の平文の割合とは大きく異なる。よって「平文中の♡を暗号化すると♠ 1 文字になる」とは考えにくい。

次に王子は，「平文中の♡を暗号化すると♠♠の2文字になる」という可能性を検討した。しかし，♠♠が文頭の暗号文の割合は［セ］%なので，これも考えにくい。このように様々な可能性を検討し，最終的には「平文中の♡を暗号化すると♡1文字になる」と確信した。

さらに，平文中の♠を暗号化すると得られる文字列(以下zとする。)について考えた。「平文中の♡を暗号化すると♡1文字になる」ことから，zは［ソ］はずだ。しかも，zが文頭の暗号文の割合と文頭が♠の平文の割合が対応しなければならない。よって，zは♠♡か［タ］のどちらかだろう。

王子はこのような分析の末に，シャッフル王国の暗号化方法は次のどちらかだと結論づけた。

方法A　♡を♡，♠を♠♡，♣を♠♠♡，◇を♠♠♠に暗号化する。

方法B　♡を♡，♠を［タ］，♣を［チ］，◇を［ツ］に暗号化する。

王子は，どちらの方法なのかをはっきりさせるために，**方法A**で暗号文を復号してみることにした。——しかし王子は，暗号文には「おまけ」を加えてあり，そのままではうまく復号できないことを知らなかった。

［シ］，［ソ］の解答群

⓪	♠を2文字以上含む	①	♠を1文字以下しか含まない
②	♠から始まる	③	♠からは始まらない
④	♠で終わる	⑤	♠では終わらない

［ス］・［セ］の解答群

⓪ 0　① 10　② 20　③ 30　④ 40　⑤ 50　⑥ 60

［タ］～［ツ］の解答群

⓪	♡♡	①	♡♠	②	♠♡	③	♠♠
④	♡♡♡	⑤	♡♡♠	⑥	♡♠♡	⑦	♡♠♠
⑧	♠♡♡	⑨	♠♡♠	ⓐ	♠♠♡	ⓑ	♠♠♠