

情報部会研究委員会報告

「教材事例」、「教科『情報』と大学入試」、「アンケート結果報告」

今治北高等学校教諭	二宮 宏之
今治南高等学校教諭	安永 隆治
北条高等学校教諭	高智 英彰
松山東高等学校教諭	兵頭 道淳
松山北高等学校教諭	牟田口正虎
三間高等学校教諭	夏秋 従治

1 教材事例

- ・教室で行う実習事例・・・・・・・・・・・・・・・・・・高智 英彰
- ・携帯電話、スマートフォンのルール作り・・・・・・・・二宮 宏之
- ・基数変換、線形探索と二分探索・・・・・・・・・・安永 隆治
- ・回転式グリル暗号・・・・・・・・・・・・・・・・・・牟田口正虎
- ・ヴィジュネル暗号・・・・・・・・・・・・・・・・・・夏秋 従治
- ・RSA暗号・・・・・・・・・・・・・・・・・・・・・・・・二宮 宏之

2 教科「情報」と大学入試・・・・・・・・・・・・・・・・・・兵頭 道淳

- ・昨年度入試で情報を選択できた大学の紹介
- ・高知大学の出題例、解答例
- ・考察と総評

3 アンケート結果報告

- ・アンケート内容について
- ・各校における教科「情報」の実施状況について
- ・個人の校務分掌や業務の状況について

教室で行う実習事例

1 パラパラマンガを作成しよう（動画の表現）

- ・教科書の四隅の空白部分を利用してパラパラマンガを作成する。
- ・最初の図形やテーマを与えておくと取り掛かりやすい。

2 広告について話し合おう（情報の信憑性）

- ・広告やチラシを利用して、記載内容を吟味する。
- ・グラフや数値の扱いがどのようになっているか確認する。
- ・誇大な表現が使われていないかなど、班別で話し合う。

3 学校を改善しよう（問題解決）

- ・問題解決の実践として、学校の改善を考える。
- ・学校の施設や教室の環境、部活動や生徒会活動など、より良い学校生活を送るために何をどうようにすればよいか、思いつくまま考えさせる。

4 インタビューをしよう（コミュニケーション、情報の収集）

- ・笑顔であいさつ、本題に入る前に雑談、必要なところだけメモ、相手の顔を見る、話しを急かさな
い、時間はさりげなく確認などなど、対話によるコミュニケーションや情報の収集を行う。
- ・その人がよく知っていることを、上手に聞きだそう。

5 自分とメディアの関わり（メディアの特徴）

- ・各年齢において、どのようなメディアと関わってきたかを調べ、各メディアの特徴を調べる。
- ・グループ内で他の人と比較してみる。

年齢・学年	本	新聞	テレビ・ラジオ	ネット	その他
0～1歳	絵本		〇〇さんといっしょ		
1～2歳					
2～3歳					
年少	童話		〇〇戦隊		
年中					
年長					
小学1年	〇〇コロ		〇〇モン		
小学2年					
小学3年					
小学4年					
小学5年					
小学6年					
中学1年	〇〇ンブ		〇〇ボール	〇〇tube	携帯電話
中学2年					
中学3年					
高校1年	〇〇ジン	〇〇新聞	〇〇ピース	〇〇NE	スマートフォン
高校2年					
高校3年					

携帯電話・スマートフォンのルール作り

携帯電話・スマートフォンのルール作り 1年()組()番 氏名

・携帯電話を持っている人は今後のルール作りを「保護者と相談して」決めること。
持っていない人は今後もつことになった場合、どのようなことに気を付ける必要があるかを
考えて記入すること。

	ルールを作った理由 (保護者と話し合った内容)
1 利用時間帯について	
2 利用料金について	
3 メールの利用について	
4 SNS・掲示板等への書き込みについて	
5 利用場所について	
6 その他のルール	

以上のルールが守られなかった場合

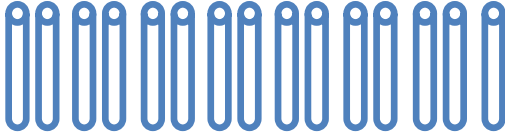
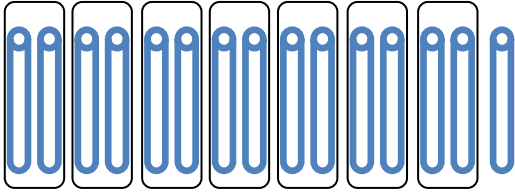
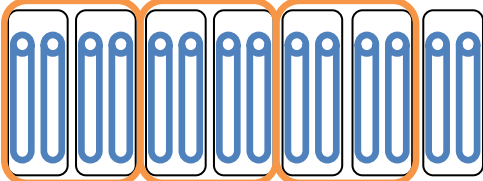
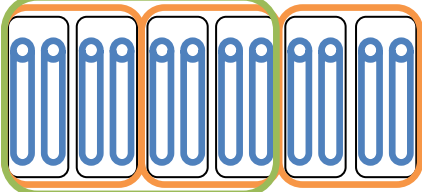
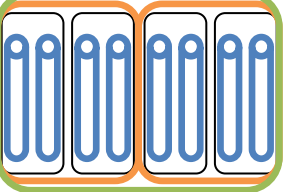
--

・保護者からの一言

--

10進数から2進数への変換実習

- ①チョークや爪楊枝などを使用し下図のようにずつのグループを作っていく。
- ②グループにまとめられないものは余り1とする。
- ③余りを右表の重みに記入していく。

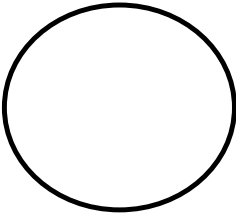

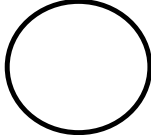

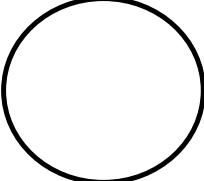
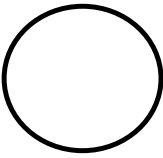
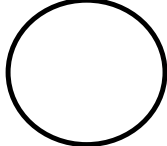

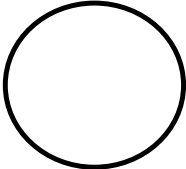
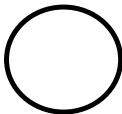
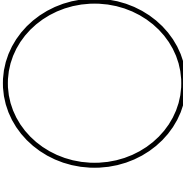
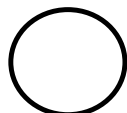
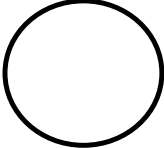
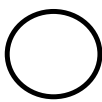
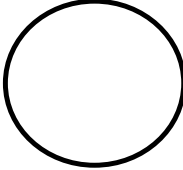
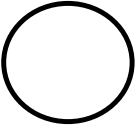
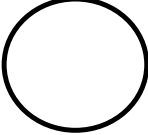
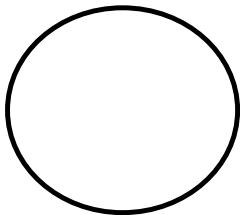
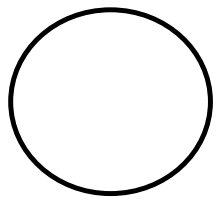
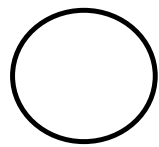
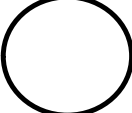
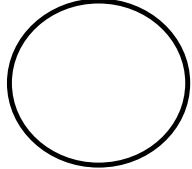

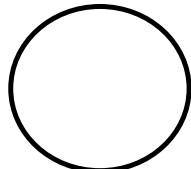
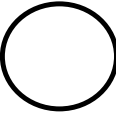
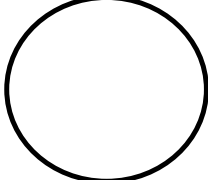
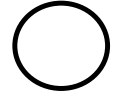
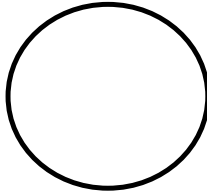
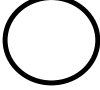
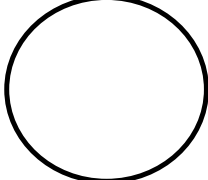
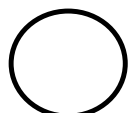
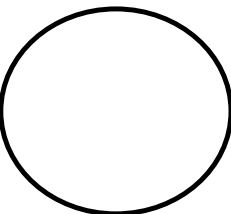

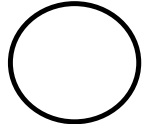
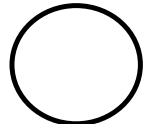
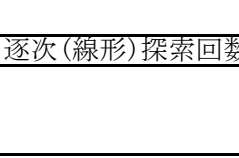
15	
グループの数	
7	
3	
1	
0	

余り	重み			
	2^3	2^2	2^1	2^0
1				1
1			1	
1		1		
1	1			

15の2進数	1	1	1	1
--------	---	---	---	---

逐次探索・二分探索実習ワークシート

- ① I～IVの列の中からペットボトルキャップと同じ大きさの○を上端から順に探し回数を記入しなさい。
- ② IVの列を二分探索でペットボトルキャップと同じ大きさの○を探し回数を記入しなさい。

I	II	III	IV	
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>
				逐次探索回数 <input style="width: 100%; height: 20px;" type="text"/>

逐次(線形)探索回数	逐次(線形)探索回数	逐次(線形)探索回数	逐次(線形)探索回数

回転式グリル暗号

1 目的

転置法に分類される暗号の中で、回転グリル暗号と呼ばれる暗号について、自分で簡単に作成でき、体験することで理解を深めさせる。

2 方法

作成、運用手順（下のような正方形のセットを配付する。）

- ① 4つのAから1つ選んで枠いっぱいに穴を開ける。B～Dについても同様にする。
- ② 正方形を切り出し、穴をあけた正方形をあいてない正方形の上に重ねる。
- ③ 穴を通して下側の正方形のマスを、A～Dの順にメッセージを記入する。
- ④ 上の正方形を回転の時計回りに90度回転させて、下の正方形とぴったり重ねる。
- ⑤ ③、④の手順を繰り返し、一周させる。
- ⑥ 上の正方形を取り除く。下の正方形に空きマスがあれば、ダミーの記号を記入する。
- ⑦ 周囲で交換し、暗号化、復号を確認する。（鍵は穴を開けた正方形だと確認する）

穴をあける正方形の例（鍵） 暗号メッセージの正方形の例（16文字以内）

A	B	C	A
C	D	D	B
B	D	D	C
A	C	B	A

R	U	E	R
A	Y	D	E
Z	L	M	R
O	A	E	I

メッセージが16文字を超える場合は2枚目の正方形に記入する。

網掛けは穴を開けるマス

A	B	C	A
C	D	D	B
B	D	D	C
A	C	B	A

網掛けは穴から見える文字

R	U	E	R
A	Y	D	E
Z	L	M	R
O	A	E	I

左の正方形を右の正方形の上に重ねる。穴から見える文字をA,B,C,Dの穴の順に読み取る。この例では、「R」「E」「A」「L」の順で読み取れる。

時計回りに90度回転

A	B	C	A
C	D	D	B
B	D	D	C
A	C	B	A

網掛けは穴から見える文字

R	U	E	R
A	Y	D	E
Z	L	M	R
O	A	E	I

同様の手順で、穴から見える文字をアルファベット順に読み取ると、「I」「Z」「E」「Y」が得られる。

90回転しても、文字の配置は変化

しない。穴の場所が変化する。

さらに 90 度回転

V	B	O	V
O	D	D	B
B	D	D	O
V	O	B	V

R	U	E	R
A	Y	D	E
Z	L	M	R
O	A	E	I

「O」「U」「R」「D」を得る。

最後の 90 度回転

A	B	C	A
C	D	D	B
B	D	D	C
A	C	B	A

R	U	E	R
A	Y	D	E
Z	L	M	R
O	A	E	I

「R」「E」「A」「M」を得る。

「Realize your dream」が復号されたメッセージである。

3 まとめ

手作業で、手軽に暗号を体験できるため、コンピュータ教室が使えない場合でも、普通教室で実習ができる。準備についても比較的負担が少なく教員側からも実施しやすい。

余裕があれば、数学と融合させ、暗号の組み合わせを考えさせることで、暗号の強度を考察することも可能である。4×4の正方形では穴をあける個数は4になることは容易に確認できるので、例えば、アルファベットで表現するならば、A,B,C,Dのように文字数が4であることが必然だと分かる。また、アルファベットの読む順番は4!通りである。穴をあける場合の数は、A,B,C,Dがそれぞれ4通りあるので、4⁴通りある。よって、回転グリル式暗号(4×4)の場合の数は、4!×4⁴=6144である。シーザー暗号と比較してみるのもよいと思う。

ヴィジュネル暗号を利用した簡単な暗号化・復号実習

1 ヴィジュネル暗号について

ヴィジュネル暗号とは、フランスの外交官ブレイズ・ド・ヴィジュネル（1523～1596年）によって16世紀に発表された暗号であり、図1、2のヴィジュネル方陣を使う。平文から暗号文への方陣と、暗号文から平文への方陣である。

図1 ヴィジュネル方陣(平文→暗号文)

		→平文																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓ 鍵	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

図2 ヴィジュネル方陣(暗号文→平文)

		→暗号文																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓ 鍵	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
	C	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	D	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	E	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	F	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	G	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	H	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	I	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	J	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	K	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	L	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	P	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	Q	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	R	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	S	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	T	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	U	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	V	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	W	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	X	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	Y	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	Z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

2 ヴィジュネル暗号を利用した実習例について

ヴィジュネル暗号の概要を説明した後、実際に暗号化・復号を体験させる。

例えば、「HUMAN」を鍵として、暗号化・復号させる。

(1) 「I like singing songs.」を暗号化させる。

① 平文から暗号文への方陣(図1)と図3, 4のような表を準備する。

図3

		→平文																										
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
↓ 鍵	H																											
	U																											
	M																											
	A																											
	N																											

図4

		→平文																
		I	L	I	K	E	S	I	N	G	I	N	G	S	O	N	G	S
↓ 鍵	H																	
	U																	
	M																	
	A																	
	N																	

② 図1の平文から暗号文への方陣の行(横)について「鍵」に従い、H, U, M, A, Nの順に取り出させ、図3の表に記入させる。

図5

		→平文																									
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓ 鍵	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

③ 図5の列(縦)について、暗号化する文章に従い、I, L, I, K, E, …の順に取り出させ、図4の表に記入させる。

図6

		→平文																
		I	L	I	K	E	S	I	N	G	I	N	G	S	O	N	G	S
↓ 鍵	H	P	S	P	R	L	Z	P	U	N	P	U	N	Z	V	U	N	Z
	U	C	F	C	E	Y	M	C	H	A	C	H	A	M	I	H	A	M
	M	U	X	U	W	Q	E	U	Z	S	U	Z	S	E	A	Z	S	E
	A	I	L	I	K	E	S	I	N	G	I	N	G	S	O	N	G	S
	N	V	Y	V	X	R	F	V	A	T	V	A	T	F	B	A	T	F

④ 図6を用いて、平文の1, 6, 11, 16番目の文字は鍵「H」の所の文字へ、2, 7, 12, 17番目の文字は鍵「U」の所の文字へ、…というように変換させていく。(図7では、必要でない文字を消しているが、あるいは、必要な文字に印を付けさせてもよい。)

図7

		→平文																
		I	L	I	K	E	S	I	N	G	I	N	G	S	O	N	G	S
↓ 鍵	H	P				Z											N	
	U		F				C					A						M
	M			U				Z					E					
	A				K				G						O			
	N					R				V						A		

⑤ 暗号化すると「PFUKRZCZGVUAEONM」

(2) 「SYFIGNI」を復号させる。

① 暗号文から平文への方陣(図2)と、図8, 9のような表を準備する。

図8

→暗号文

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	H																									
鍵	U																									
	M																									
	A																									
	N																									

図9

→暗号文

	S	Y	F	I	G	N	I
↓	H						
鍵	U						
	M						
	A						
	N						

② 図2の暗号文から平文への方陣の行(横)について「鍵」に従い、H, U, M, A, Nの順に取り出させ、図8の表に記入させる。

図10

→暗号文

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
↓	H	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
鍵	U	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

③ 図10の列(縦)について、復号する文章に従い、S, Y, F, I, …の順に取り出させ、図9の表に記入させる。

図11

→暗号文

	S	Y	F	I	G	N	I	
↓	H	L	R	Y	B	Z	G	B
鍵	U	Y	E	L	O	M	T	O
	M	G	M	T	W	U	B	W
	A	S	Y	F	I	G	N	I
	N	F	L	S	V	T	A	V

④ 図11を用いて、暗号文の1, 6番目の文字は鍵「H」の所の文字へ、2, 7番目の文字は鍵「U」の所の文字へ、…というように変換させていく。(図12では、必要でない文字を消しているが、あるいは、必要な文字に印を付けさせてもよい。)

図12

→暗号文

	S	Y	F	I	G	N	I
↓	H	L				G	
鍵	U		E				O
	M			T			
	A			I			
	N				T		

⑤ 復号すると「Let it go」

RSA 暗号

1 暗号化

共通鍵方式・・・暗号化と復号に同じ鍵をつかう。

(例) 鍵「五十音順で1文字後ろにずらす」

共通鍵方式の場合、ある文を秘密に伝えたいとき、まず先に鍵を秘密に伝えなければならない。

公開鍵方式・・・相手に配布した公開鍵で暗号化して、自分しか持っていない秘密鍵で復号する。

{ 鍵 A で暗号化したら → 公開鍵 A
 鍵 B でしか復号できない → 秘密鍵 B

{ 鍵 B で暗号化したら → 公開鍵 B
 鍵 A でしか復号できない → 秘密鍵 A

2 剰余演算

$$32 \div 10 = 3 \cdots 2$$

↓

$$32 \bmod 10 = 2 \quad (32 \text{ は } 10 \text{ を法として } 2 \text{ になる})$$

3 剰余演算の性質

素数 p を法として剰余演算を行うと、計算結果に規則性が現れ、ある数値 x の p 乗を p を法として計算すると x になる。

$$x^p \bmod p = x$$

が成り立つ。

(例)

2 のべき	1	2	3	4	5	6	7	8	9	10
通常計算	2	4	8	16	32	64	128	256	512	1024
5 を法として	2	4	3	1	2	4	3	1	2	4
7 を法として	2	4	1	2	4	1	2	4	1	2

3 のべき	1	2	3	4	5	6	7	8	9	10
通常計算	3	9	27	81	243	729	2187	6561	19683	59049
5 を法として	3	4	2	1	3	4	2	1	3	4

4 RSA 暗号

剰余演算の性質を利用して暗号化と復号を行う。

2つの素数 p, q を掛けた数値 $N(N=p \times q)$ を法とする。

ある数値 x の $n \times (p-1) \times (q-1) + 1$ 乗を N を法として計算すると x になる。(ただし、 n は任意の正の整数)

公開鍵「 N を法として、鍵を C として暗号化」が与えられたとき、ある数値 x の C 乗を N を法として計算して暗号化する。ここで、 C は $n \times (p-1) \times (q-1) + 1 = C \times D$ を満たす整数である。

この場合、秘密鍵は D となり、暗号化された数値の D 乗を N を法として計算すると復号される。

(例) 素数 $P=3, Q=11$ を選び、それらを掛けた $P \times Q = 33$ を法とする。

$n \times (p-1) \times (q-1) + 1$ より、21 が計算され、公開鍵は「33 を法として、鍵を 3 として暗号化」とする。

この場合、秘密鍵は 7 となる。

数値のべき乗を全て求めて表にすると、

復号

		べき乗数 →																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
数 値 ↓	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32
	3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12
	4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1
	5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23
	6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21
	7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10
	8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32
	9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12
	10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
	11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
	13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10
	14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23
	15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12
	16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1
	17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32
	18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21
	19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10
	20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23

べき乗する度に予想のつかない数に変わっていきながらも、全ての数は 21 乗するともとの数に戻っている。

よって、表より「248」は「83117」と暗号化され、暗号を 7 乗して 33 を法とすると復号できる。すなわち、暗号化において重要なのは、3 と 11 (P と Q) である。33 という数は公開するが、33 の素因数が 3 と 11 であることが分からなければ、秘密鍵 D は分からず、復号できない。

実際の暗号では、 N が

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

P と Q が

3490529510847650949147849619903898133417764638493387843990820577

32769132993266709549961988190834461413177642967992942539798288533

となっており、暗号のセキュリティーは因数分解が難しいという事実にかかっている。

公開鍵暗号実習

鍵

1. 下の②に右の鍵番号を記入しなさい。
2. 切り取り①で切り取り隣の席の生徒と交換しなさい。

ASCIIコード表

文字	10進	文字	10進	文字	10進	文字	10進
NUL	0	SP	32	@	64	`	96
SOH	1	!	33	A	65	a	97
STX	2	"	34	B	66	b	98
ETX	3	#	35	C	67	c	99
EOT	4	\$	36	D	68	d	100
ENQ	5	%	37	E	69	e	101
ACK	6	&	38	F	70	f	102
BEL	7	'	39	G	71	g	103
BS	8	(40	H	72	h	104
HT	9)	41	I	73	i	105
LF*	10	*	42	J	74	j	106
VT	11	+	43	K	75	k	107
FF*	12	,	44	L	76	l	108
CR	13	-	45	M	77	m	109
SO	14	.	46	N	78	n	110
SI	15	/	47	O	79	o	111
DLE	16	0	48	P	80	p	112
DC1	17	1	49	Q	81	q	113
DC2	18	2	50	R	82	r	114
DC3	19	3	51	S	83	s	115
DC4	20	4	52	T	84	t	116
NAK	21	5	53	U	85	u	117
SYN	22	6	54	V	86	v	118
ETB	23	7	55	W	87	w	119
CAN	24	8	56	X	88	x	120
EM	25	9	57	Y	89	y	121
SUB	26	:	58	Z	90	z	122
ESC	27	;	59	[91	{	123
FS	28	<	60	\	92		124
GS	29	=	61]	93	}	125
RS	30	>	62	^	94	~	126
US	31	?	63		95	DEL	127

切り取り①

- ① ASCIIコード表の大文字を使い5文字程度の単語を作り10進数で表しなさい。

単語

--	--	--	--	--

- ② ①で作成した単語を右に指定された鍵を基に暗号表を使い暗号変換しなさい。

鍵

変換後

--	--	--	--	--

- ③ ②で変換した暗号を下に記入し切り取り②で切り離し、隣の交換した生徒に渡しなさい。

切り取り②

暗号

--	--	--	--	--

- i 右の式を使い暗号文を平文に戻す鍵(秘密鍵)を作成します。
$$D = \frac{n \times (P - 1) \times (Q - 1) + 1}{A}$$

n: 任意の数値1でも良い P, Q: 暗号表を作成したときに使用した素数 A: 1. で指定した鍵

- ii iで作成した鍵(秘密鍵)を使用し暗号表を使い暗号文を平文に戻しなさい。

単語

--	--	--	--	--

Table with columns labeled 1 through 50 and a header labeled '番号' (Number). The table contains a grid of numerical values, likely representing a sequence or data set.

文字番号

Table with 50 columns and 100 rows of numerical data. The table contains a grid of numbers from 1 to 50 across the top and 100 rows of data below. The data appears to be a complex grid of integers.

文字番号

Table with 50 columns and 100 rows of numerical data. The columns are numbered 1-50 and the rows are numbered 1-100. The data consists of integers ranging from 1 to 100.

文字番号

教科「情報」と大学入試

1 2014年度入試で情報を選択することができた大学

区分	大学	学部	学科	入試区分	選択	試験範囲
国立	高知大	理	情報受験 コース	前期	必須	A・B・Cの共通範囲 とA・B・Cから1つ
私立	千歳科学技術大	総合光科		I期 II期	国数理外情から 2教科選択	情報C
	北海道情報大	経営情報	先端経営 システム情報	1期	下記4科目から2科目 ・国総 ・IB・政経・物I・化I・生Iから1 ・数IA・数I IAB・情報から1 ・英I II	A・B・Cの共通範囲
		医療情報	医療情報			
		情報メディア	情報メディア			
	青森大	ソフトウェア情報	ソフトウェア情報	A日程 B日程	数I必須 + 国・数II・英I II・情 から1科目選択	A・B・Cの共通範囲
	筑波学院大	経営情報	経営情報	A日程	国語必須 + 世B・IB・数IA・英I II・情 から1科目選択	情報A
	高崎商科大	商	商	A日程	国語必須 + 世B・IB・地B・現社・数IA・簿記・情・英I II から1科目選択	
	尚美学園大	芸術情報	情報表現	A日程 B日程	英I II必須 + 国数情から1教科選 択	情報ABC
	千葉経済大	経済	経済 経営	A日程	国語・英語必須 + 世B・IB・政経・数I IIA・簿記・情 から1科目選択	情報A
	中央学院大	商 法	商 法	1期3科目 B日程	国語・英語必須 + 世B・IB・地AB・現社・政経・数IA・簿記・情 から1科目選択	A・B・Cの共通範囲
1期1科目 B日程				国・世B・IB・地AB・現社・政経・数IA・簿記・情 から1科目選択	A・B・Cの共通範囲	
東京情報大	総合情報	総合情報	I期A方式	国・現社・数IA・英・情 から2科目選択	情報B	
明治大	情報コミュニケーション	情報コミュニケーション	B方式	数・英・情の3教科	A・B・Cの共通範囲	

区分	大学	学部	学科	入試区分	選択	試験範囲
私立	和光大	経済経営	経済 経営	前期 (学部方式)	国・世B・日B・政経・数IⅡAB・情・簿記会計・英 から2科目選択	情報ABC
	静岡産業大	経営	経営 スポーツ経営 心理経営	前期A方式	国・世B・日B・数I A・英IⅡ・情 から2教科2科目選択	
		情報	情報デザイン 国際情報			
	大阪国際大	グローバルビジネス	グローバルビジネス	A日程	国語・英語必須 + 世B・日B・数I A・情 から1科目選択	
		人間科学	心理コミュニケーション 人間健康科学 スポーツ行動	B日程		
		国際コミュニケーション	国際コミュニケーション			
	徳山大	経済	現代経済 ビジネス戦略	I期	国語必須 + 英IⅡ・情 から1科目選択	情報関係基礎
		福祉情報	人間コミュニケーション			
	九州情報大	経営情報	経営情報 情報ネットワーク	一期 二期	国・数IⅡ・英IⅡ・情・簿記会計 から2科目選択	情報関係基礎
	宮崎産業経営大	法	法律	総合・専門科生 選抜	国語必須 + 数I・簿記・情 から1科目選択	情報処理
経営		経営				

2 出題例 (2014年度 高知大学) ①と②は必答・③～⑤より1問選択

(掲載許諾済)

① 次の文章を読み、下の問に答えよ。(150点)

インターネットは、世界中の個人をはじめ、政府機関、教育機関、企業などが利用している。(ア)と契約することで、個人でもインターネットへ接続することができる。

コンピュータネットワークを用いてデータをやりとりするには、プロトコルと呼ばれる共通の規約が必要である。インターネットで主に使用されているプロトコルはTCP/IPである。これは、(イ)と(ウ)を組み合わせたものである。(イ)は、データをいくつかの(エ)に分けて、番号をつけて送るプロトコルである。(ウ)は指定された宛先のコンピュータまで(エ)を届けるためのプロトコルである。

インターネットには、様々なサービスを提供するコンピュータが接続されている。サービスを提供するコンピュータをサーバという。これに対してサービスを要求するコンピュータを(オ)という。サーバから(オ)へデータを転送することを(カ)という。また、(オ)からサーバへデータを転送することを(キ)という。

インターネット上の Web ページの情報を提供するためには、(ク) と呼ばれるサービスを利用する。その情報の閲覧には (ケ) と呼ばれる Web ページの閲覧ソフトウェアを使用する。Web ページの内容は (コ) で記述され、Web サーバと (ケ) との間で情報をやりとりするために TCP/IP に加えて (サ) というプロトコルが用いられる。また、Web ページのアドレスのことを (シ) という。

この他にも、インターネットの主なサービスとして電子メールサービスがある。電子メールの送信の際に使用するプロトコルは (ス) である。電子メールを受信するときに使用するプロトコルとして、(セ) または IMAP が用いられる。

インターネットには数多くのコンピュータが接続されている。Web ページの閲覧や電子メールのやりとりをするためには、各々のコンピュータを識別するための番号が必要である。これを、IP アドレスという。IP アドレスを指定することで、目的のコンピュータに接続することが可能である。しかし、IP アドレスは数字で表されるため、人間には覚えにくい。そこで、人間が覚えやすいように文字で表現した (ソ) を利用する。インターネット上には、IP アドレスと (ソ) を対応させ、これらを変換する DNS と呼ばれるシステムがある。

問 (ア) ~ (ソ) に入る適切な語句を、下記の語群から 1 つ選んで答えよ。

アップロード	インターネットサービスプロバイダ	クライアント			
ダウンロード	ドメインネーム	パケット	HTML	HTTP	IP
POP	SMTP	TCP	URL	WWW	Web ブラウザ

解答

(ア)インターネットサービスプロバイダ	(イ)TCP	(ウ)IP	(エ)パケット	(オ)クライアント	
(カ)ダウンロード	(キ)アップロード	(ク)WWW	(ケ)Web ブラウザ	(コ)HTML	(サ)HTTP
(シ)URL	(ス)SMTP	(セ)POP	(ソ)ドメインネーム		

2 次の文章を読み、下の問に答えよ。(150 点)

2 つの自然数 a 、 b の最大公約数 d を求める手続きをいくつか考えてみよう。簡単な手続きとしては次のようなものが考えられる：

手続き A_1

- ① $a < b$ ならば a と b の値を入れ替える。
- ② $d \leftarrow b$ とする。
- ③ a と b が共に d で割り切れれば d を出力し終了する。
- ④ $d \leftarrow d - 1$ とし、③へ戻る。

ただし、 \leftarrow は変数へ値を代入することを表す。

問 1 手続き A_1 が必ず終了する理由を述べよ。

問 2 例えば a と b の最大公約数が 1 である場合、手続き A が終了するまでに

$d=b, b-1, \dots, 1$ の b 通りの d の値に対して除算が実行される。しかし、 b の約数のうち b の次に大きいものは $\frac{b}{2}$ 以下であることに着目すると、このうちの約半数の除算は省略できる。手続き A_1 をどのように改良すれば良いか述べよ。

問3 最大公約数には次の性質がある：

定理 B $a > b$ のとき、 a と b の最大公約数は、 $a-b$ と b の最大公約数に等しい。

定理 B を繰り返し用いることにより、 $a=31$ と $b=11$ の最大公約数は次のように求めることができる。ただし、 a と b の最大公約数を (a, b) と表すこととする。

$$\begin{aligned} (31, 11) &= (31-11, 11) = (20, 11) \\ &= (20-11, 11) = (9, 11) = (11, 9) \\ &= (11-9, 9) = (2, 9) = (9, 2) \\ &= (9-2, 2) = (7, 2) = (7-2, 2) = (5, 2) \\ &= (5-2, 2) = (3, 2) = (3-2, 2) = (1, 2) = (2, 1) \\ &= 1 \end{aligned}$$

なお、この計算方法では、 $(a, b) = (b, a)$ であることと、 a が b で割り切れるとき、 $(a, b) = b$ であることを利用している。これにならって、 $a=11$ と $b=3$ の最大公約数を求める過程を示せ。

問4 問3のアイデアを用いると次のような手続きが考えられる：

手続き A_2

- ① $a < b$ ならば a と b の値を入れ替える。
- ② a が b で割り切れれば b を出力し終了する。
- ③ $a \leftarrow a-b$ とし、①へ戻る。

手続き A_2 にはさらに改良できる点がある。それはどのようなことか述べよ。

解答例

問1 d の値が $d=1$ まで変化すれば必ず a を割り切って終了条件を満たすので。

問2 ②の前に b が a を割り切るかどうか判定し、割り切らなければ②で設定する d の初期値を $(b/2$ の小数点以下切り捨て)にする。

問3 $(11, 3) = (11-3, 3) = (8, 3) = (8-3, 3) = (5, 3)$
 $= (5-3, 3) = (2, 3) = (3, 2) = (3-2, 2) = (1, 2) = (2, 1) = 1$

問4 a が b で割り切れなければ $a-b$ も b で割り切れないので、 $a < b$ となるまでループを繰り返す間の②の除算が無駄である。そこで③を

$a < b$ となるまで $a \leftarrow a-b$ を繰り返し、②へ戻る。

または

$a \leftarrow (a$ を b で割った剰余)とし、②へ戻る。

とすれば良い。

3 次の文章を読み、下の問に答えよ。(100点)

表1は、あるパーソナルコンピュータの仕様表の一部を抜粋したものである。この表のように、ハードディスクドライブ等の容量がSI接頭語(kmのkのようにSI単位の前に付ける接頭語)を用いて1GB=1,000,000,000Bとして換算され、仕様表やパッケージに表記されていることがある。しかし、慣例的にはバイト(B)の接頭語として用いる場合は、

1KB=(ア)B, 1MB=(ア)KB, 1GB=(ア)MB, 1TB=(ア)GB

として換算されている。これは、コンピュータにとっては10よりも2の累乗ごとにひとまとめにしたほうが切りがよく、2の累乗のうち1000に最も近い2の(イ)乗をひとまとめとしたからである。SI接頭語との混乱を防ぐために1KiB(キビバイト)=(ア)B等を代わりに使うようにIEC(国際電気標準会議)によって国際標準化されたが、まだ浸透はしていないようである。

表1 あるパーソナルコンピュータの仕様表の一部

CPU	動作周波数 3.00GHz
メインメモリ	8GB
ハードディスク容量	750GB
ディスプレイ (解像度/表示色)	1920×1200ドット/約1677万色
購入特典	USBフラッシュメモリ 8GB※

※1GB=1,000,000,000Bとして換算した場合。

問1 文中の空欄(ア)と(イ)にあてはまる数を答えよ。

問2 下記の語群のうち、表1に掲載されていないものを答えよ。

中央処理装置 主記憶装置 補助記憶装置 入力装置 出力装置

問3 一般に、ウェブページでは色をRGB表現で指定する際に、R、G、Bそれぞれ256段階ずつ計24ビットで表現する(24ビットカラーと呼ぶ)。表1のパーソナルコンピュータのディスプレイが、ウェブページで指定された色をすべて表示できるかどうかを、その理由とともに答えよ。

問4 A4サイズの全80ページからなる写真集を24ビットカラー、600dpiでスキャンしたい。スキャンしたデータをそのまま表1のUSBフラッシュメモリに保存することが可能かどうかを、その理由とともに答えよ。ただし、1インチ=2.54cm、A4サイズは21cm×29.7cmとする。

解答例

問1 (ア)1,024 (イ)10

問2 入力装置

問3 R、G、Bそれぞれ256段階ずつ計24ビットで表現できる色の総数は $256 \times 256 \times 256 =$

16,777,216 色である。表1によればこのディスプレイは約 1,677 万色表示できる。よって、このディスプレイは 24 ビットカラーに対応していると判断できる。したがってこのディスプレイはウェブページで指定された色をすべて表示できると言ってよい。

問4 A4 サイズ 21cm×29.7cm をインチに直すと 21/2.54 インチ×29.7/2.54 インチ。これを 600dpi でスキャンした時のドット数で表すと $(600 \times 21/2.54) \times (600 \times 29.7/2.54)$ ドットである。24ビットカラーなので1ドットあたり24ビット=3B のデータ量を要する。以上より、A4 サイズ 80 ページをスキャンしたときのデータ量 a は、

$$\begin{aligned} a &= (600 \times 21/2.54) \times (600 \times 29.7/2.54) \times 3 \times 80B \\ &= (6 \times 21/254) \times (6 \times 297/254) \times 3 \times 800,000,000B \quad \text{である。} \end{aligned}$$

一方、表1より、USB フラッシュメモリの容量 b は 8GB=8,000,000,000B である。

両者の大小関係を比較すると

$$\begin{aligned} a/b &= (6 \times 21/254) \times (6 \times 297/254) \times 3 \times 800,000,000/8,000,000,000 \\ &= (6 \times 21/254) \times (6 \times 297/254) \times 3 \times 1/10 = 673,596/645,160 > 1 \end{aligned}$$

よって、 $a > b$ であるから、保存できない。

4 次の文章を読み、下の問に答えよ。(100点)

情報検索の一つに、キーワード検索がある。知りたい情報のキーワードを入力して検索するものである。キーワードを一つだけ指定して検索するものを単純条件検索、二つ以上のキーワードを AND, OR, NOT の論理演算子でつないだ条件で検索するものを複合条件検索という。

問1 検索対象の情報の総件数を z 、キーワード A にヒットする情報の件数を a 、キーワード B にヒットする情報の件数を b 、「A または B」にヒットする情報の件数を e とするとき、以下の条件式にヒットする情報の件数を z 、 a 、 b 、 e を用いて表せ。

- (1) A AND B
- (2) A OR B
- (3) NOT A
- (4) A AND (NOT B)

問2 問1の設定に、新たにキーワード C を加え、キーワード C にヒットする情報の件数を c 、「B または C」にヒットする情報の件数を f 、「C または A」にヒットする情報の件数を g 、「A かつ B かつ C」にヒットする情報の件数を h とするとき、以下の条件式にヒットする情報の件数を z 、 a 、 b 、 c 、 e 、 f 、 g 、 h を用いて表せ。なお、(4) と (5) については、計算過程も含めて答えよ。

- (1) A AND B AND C
- (2) B AND C
- (3) C AND A
- (4) (A AND B) OR (B AND C) OR (C AND A)
- (5) A OR B OR C

解答例

問1 (1) $a+b-e$ (2) e (3) $z-a$ (4) $a-(a+b-e)=e-b$

問2 (1) h (2) $b+c-f$ (3) $c+a-g$

(4) 条件 X にヒットする件数を[X]で表すと, 求める値は

$$[A \text{ AND } B] + [B \text{ AND } C] + [C \text{ AND } A] - 2[A \text{ AND } B \text{ AND } C]$$

$$= (a+b-e) + (b+c-f) + (c+a-g) - 2h = 2(a+b+c-h) - e - f - g$$

(5) 求める値は

$$[A] + [B] + [C] - [A \text{ AND } B] - [B \text{ AND } C] - [C \text{ AND } A] + [A \text{ AND } B \text{ AND } C]$$

$$= a + b + c - (a+b-e) - (b+c-f) - (c+a-g) + h = e + f + g + h - a - b - c$$

5 次の文章を読み, 下の問に答えよ。(100点)

デジタル信号を送信したり保存したりする際にデータビットの0と1が反転する現象(ビット誤り)が生じることがある。その誤りを検出したり訂正したりするための技術が誤り訂正符号である。

データを表すビット列を情報ビットと言い, これに加えて検査ビットと呼ばれるビットをいくつか付加したビット列を符号語という。この検査ビットをうまく設計することにより誤りの検出・訂正を可能とするのである。

例えば, 2種類の情報AかBだけをデジタル信号で表現するには

$$A \rightarrow 0, \quad B \rightarrow 1$$

のように1ビットのビット列を用いればよい。しかし, このビット列にビット誤りが生じた場合, 誤りの検出・訂正は不可能である。そこで検査ビットとして同じビットをさらに2つ付加して

$$A \rightarrow 000, \quad B \rightarrow 111$$

という符号化を行うことにする。もし, 読み取った信号が010であれば, これは000でも111でもないので誤りが生じたことがわかる。さらに, 111の第1ビットと第3ビットの両方に誤りが生じるよりも000の第2ビットにだけ誤りが生じる方が確率が高いと考えられるので, 000へ復元することにする。すなわち, 「最も近い符号語に復元する」というのが誤り訂正の原理である。この原理に従って信号をデータに戻す操作

$$000 \rightarrow A, \quad 001 \rightarrow A, \quad 010 \rightarrow A, \quad 100 \rightarrow A$$

$$111 \rightarrow B, \quad 110 \rightarrow B, \quad 101 \rightarrow B, \quad 011 \rightarrow B$$

を復号化と言う。

A, Bからなる文字列の符号化は, 前から1文字ずつ処理をして

$$001 \ 111 \ 011 \ 010 \rightarrow ABBA$$

のように行う。

問1 4種類のデータA, K, N, Tをそれぞれ次のように符号化することとする:

$$A \rightarrow 00000, \quad K \rightarrow 01110, \quad N \rightarrow 10101, \quad T \rightarrow 11011$$

このとき文字列 TANAKA を符号化せよ。

問2 問1の符号化を行った文字列にビット誤りが生じて

11110 00000 11101 11111 10000 10101

という信号が受信されたとする。「最も近い符号語に復元する」という原理に従って復号化を行え。

問3 4種類のデータ A, K, N, T をそれぞれ次のように符号化することとする：

A → 00000, K → 01100, N → 10010, T → 11001

(1) A を符号化した符号語 00000 に 1 ビットのビット誤りを生じさせた信号は

10000, 01000, 00100, 00010, 00001

の 5 通りある。このうち、「最も近い符号語に復元する」という原理に従って誤りが正しく訂正できる信号をすべて答えよ。

(2) (1) の 5 つの信号のうち、誤りが正しく訂正できない信号をひとつ例に挙げ、正しく訂正できない理由を述べよ。

解答例

問1 11011 00000 10101 00000 01110 00000

問2 KANTAN

問3 (1) 00001

(2) 例えば 01000 という信号は、A の符号化である 00000 と第 2 ビットだけが異なり、また、K の符号化である 01100 と第 3 ビットだけが異なっていて、どちらに復元したら良いかが決められない。

3 考察

①はコンピュータネットワークに関する知識を問う問題である。基本的な問題であるが、知らない場合は考えることができないため、かなり厳しい。

②は手続きに関する思考力を問う問題である。アルゴリズムに関連するが、ユークリッドの互除法など、整数の性質に関する知識が必要である。

③はコンピュータを主体的に活用するための基礎知識を問う問題である。基本的な知識だけで対応できるが、問 4 においては計算に工夫が必要である。

④は条件検索に関する基礎的知識と理解度を問う問題である。数学における集合の要素の個数を理解していれば容易な問題であるが、変数が多いため注意が必要である。

⑤はデジタル信号に関する思考力を問う問題である。原理に関する説明が丁寧にされているため、誘導に従って考えていけば容易である。

総評として国立大学の 2 次試験としては容易な問題が多く、平均点は高いと思われる。そのため、センター試験の得点が低いものが 2 次での逆転を狙うのは厳しいであろう。また、記述が必要な問題があるため、論理的に説明する国語力も求められる。

情報の授業等に関するアンケート集計結果（55校）

（学科やコースにより教育課程が異なる学校があるため、合計が55校を超えている項目あり）

1 情報の授業の実施状況について

社会と情報（45校）

1年2単位（40校）

2年2単位（3校）

TT主副（11校）

情報の科学（9校）※TTなし

1年2単位（8校）

2年2単位（1校）

両方実施（1校）

学年無し2単位【通信制】TTなし

専門科目で代替え（11校）

情報（1校） 1年2単位 TT主副

情報A（1校） 3年1～3単位

2 情報の免許を持っている教員、情報の授業を担当している教員の人数

授業 免許	0人	1人	2人	3人	4人	5人	10人	12人
0人		1※1	1※2					
1人	1	7	2※3	1※1		1	1	
2人		8	6		1※4			
3人			1	3	1			
4人			3	3	3			
5人			2	3	1			
6人				1				1
7人						2		
9人			1					

※1 詳細未記入 ※2 免許外申請で実施

※3 TT（主副） 主：免許あり1名 副：免許なし1名

※4 TT（主副） 主：免許あり2名 副：免許なし2名

太字斜体は、専門科目で代替え

3 コンピュータ教室で行う授業数（週の割り当て）

1時間（2校） 2時間（34校） 3時間以上（16校）

年間8時間（1校） 年間30時間（1校） 年間0時間（1校） 随時（1校）

4 実習の割合（教室での実習も含む）

20%未満（5校）	20%～40%（6校）	40%～60%（21校）
60%～80%（13校）	80%以上（10校）	回答なし（1校）

5 補助教材を使用

準拠ノート・モラル・リテラシー（2校）

準拠ノート・モラル（6校）

準拠ノート・リテラシー・検定用問題集（1校）

準拠ノート・リテラシー（7校）

準拠ノートのみ（16校）

モラルのみ（6校）

検定用問題集のみ（3校）

自作教材のみ（5校）

未記入等（3校）

教科書で十分、必要としていない、補助教材は利用できる内容が少ない（各1校）

6 自作教材

- ・ 2時間連続の授業において、座学（前半1時間）の内容を実習（後半1時間）で行う。そのための補助資料を自作している。
- ・ 見やすく分かりやすく（視覚的支援）するため、説明用の補助教材を作成している。
- ・ 暗号化の実習
- ・ パワーポイントを利用して、視覚的に授業を行っている。
- ・ HTML、エクセル、暗号
- ・ Word、Excel、PowerPointの実習用
- ・ Word、Excelの実習用
- ・ 補充プリント
- ・ 自作授業プリント（全授業）
- ・ n進法の計算、電子掲示板、PHPで作成したWebアプリケーション
- ・ 文字入力用文章、学校周辺地図
- ・ 内容をまとめたパワーポイント、エクセルの実習用
- ・ 2進数から16進数への変換、加法混色・減法混色、内容をまとめたパワーポイント
- ・ コンピュータ利用の基礎知識（設定等）、Word利用の基礎
- ・ ビジネス文書実務検定の問題をベースとした、入力方法や周辺機器に関すること、モラルや文書作成の方法に関するテスト対策プリントを作成・配布
- ・ 自作プリント
- ・ 指導書を参考にしたプリント
- ・ 自作のサブノート
- ・ 時事問題をとりあげたプリント
- ・ 流れ図の解説用プリント、プログラミング（C言語）演習用プリント、CADシステム活用操作マニュアル

7 ICT活用教育支援ツールの利用（複数選択可）

教材配布（47校） 教材回収（33校） 教材提示（44校） 作業確認（35校）

出席確認（13校） アンケート回収（12校） 付属ソフトの利用（9校）

その他の利用 教師用画面送信（1校）、モニタリングしながら支援（1校）

利用無し（4校）

購入していない（2校）

コンピュータシステムが更新されず、以前の支援システム・ツールが利用不可能

（1校）

教育支援ツールが何か分からない（1校）

8 資格試験

全員に受けさせている（6校）※4校は専門科目で代替え

日検情報処理技能 日検文書デザイン 日検プレゼンテーション作成

全商情報処理検定 P検 情報技術検定

希望者に受けさせている（9校）※3校は専門科目で代替え

全商ビジネス文書実務検定試験 全商情報処理検定 情報技術検定

パソコン利用技術検定 ITパスポートなど

9 評価規準の提示

生徒・保護者（10校） 生徒だけ（20校） 保護者だけ（0校）

提示していない（9校） HPで一般に公開している（12校） 無回答（3校）

10 コンピュータ教室の日々のメンテナンス

アップデートについて

業者（2校）

定期的を実施

自動（11校）

週一（2校）、その都度（1校） など

担当者（32校）

定期的・月1・その都度（19校）、不定期（3校）、放課後・授業時間以外

（2校）

学期毎（1校）、長期休業中（1校）、テスト期間中（1校）、毎日（1校）

2～3か月に1度（1校）、教育センターから連絡があったとき（1校）

手動（4校）、自動更新で緊急時は手動（3校）、自動（3校）

WindowsUpdateを一括処理（2校） など ※アップデートしていない

（1校）

バックアップについて

業者（1校）

その都度、業者任せ

自動（8校）

その都度（3校）、週1（2校） など

担当者（18校）

その都度（6校）、年度末（3校）、年末（1校）、学期毎（1校） など
バックアップしていない（16校）

ハードのトラブル

業者（12校）、担当者（11校）、担当者と業者（21校） など

ソフトのトラブル

業者（11校）、担当者（14校）、担当者と業者（17校） など

その他のトラブル

業者（3校）、担当者（9校）、担当者と業者（2校） など

個人の業務等に関するアンケート集計結果（159名）

1 情報関係の校務分掌であるか

はい（17名） 別の分掌と掛け持ち（34名） いいえ（95名） 無答（13名）

各業務の月間作業時間

作業時間(時間) 作業項目	0.5	1	2~5	6~10	11~20	21以上	最高
サーバ管理	1	9	14	6	0	2	60時間
ホームページ管理	1	4	8	12	3	5	30時間
情報機器整備	1	8	22	5	3	1	30時間
情報機器貸出	1	12	5	2	0	0	10時間
各種調査集計	3	15	5	3	0	0	10時間
情報モラル指導	1	9	8	1	0	0	10時間
その他	1	3	2	0	1	0	20時間

2 授業以外の業務において、負担に感じていること（複数選択可）

サーバー管理（22名） ホームページ管理（23名） 情報機器整備（34名）
 情報機器貸出（7名） 各種調査集計（12名）
 情報モラルの指導（教員・保護者対象など）（6名） なし（82名）
 その他

IPアドレスの管理

パソコン教室の管理

ソフトウェアの使用法を教員に指導

プリンタのトラブル（紙詰まり、用紙切れ）まで呼び出される

各種調査集計の担当者が質問によくくる

教師は自分で挑戦してみるという手間を省いて、情報機器全般の仕事を教科情報へ依頼するケースが多いので負担になっている

成績管理、入試における成績等管理のシステムを個人（教務課長）が作成・運用しているので、不具合が出たときの対応に追われる

会議 部活動 校外の業務 校務分掌以外の業務 事務とのやりとり・調整

3 情報と他教科の授業時数（総合的な学習の時間、HRは除く）

情報の授業数	数学	理科	家庭	農業	工業	商業	その他	人数
0	11 14(2) 15 17(2) 18	13 14 15(3) 16 19	14 17	5 17(2) 18 19(2) 20 21	14 15 16(5) 17 18 19	2 3 3 19 15(2) 19	国語17 数学7・工業6 理科5・特別支援16 商業6・水産8 福祉15 未記入等(11)	55
2	10 11 12(3) 13(2) 14(2) 15(3)	2 8 10(2) 11(2) 13(2) 14 15	8 11	16		9 10 12 13 14(2) 15 16	数学7・特別支援12 理科4・特別支援11 他教科0 未記入等(2)	38
3							数学2・特別支援10	1
4	3 7 8 9 10(2) 11 12(3) 13(2) 14(3) 15	8 10(3) 11 12	12(2)	14(2)		4 7 8(2) 12 13(3)	高大連携9	35
6	10(2)	8(2) 9 10(3) 11 11	10	6			現社4・政経2	13
8	4 7 8	6(2) 8	7			2		8
10		4				2(2)	国語7	4
12							他教科0	1
13							現社6	1
14							他教科0	1
16							他教科0(2)	2
人数	40	35	8	12	10	24	30	159

() 内の数字は2名以上の人数