

筑波大学 情報学群 情報メディア創成学類

平成31年度 個別学力検査（後期日程）

小論文問題

【注意事項】

1. 試験開始の合図があるまで、この問題冊子の中を見たり、解答用紙に記入したりしてはいけません。
2. この問題冊子は、表紙と白紙を除いて全部で8ページです。
3. 解答用紙は、罫紙2枚とマス目紙2枚の計4枚です。
4. 解答用紙の定められた欄に、氏名、受験番号を記入しなさい。
5. 問題はⅠとⅡの2題で、問題Ⅰには設問1～8、問題Ⅱには設問9～11が含まれます。
設問1～5の解答を1枚目の罫紙、設問6～8の解答を2枚目の罫紙、設問9～10の解答を3枚目のマス目紙、設問11の解答を4枚目のマス目紙に記入しなさい。
6. 解答用紙上部の 欄には設問番号をそれぞれ「1～5」、「6～8」、「9～10」、「11」と記入しなさい。
7. 解答用紙左側の余白に設問番号を記入すること。
8. 解答は各解答用紙の表側の面だけに記入し、裏面には記入しないこと。
9. 解答用紙は、記入の有無にかかわらず、持ち帰ってはいけません。
10. この問題冊子と下書き用紙は持ち帰ること。

I 以下の【解説】と【英文】を読み，5 ページの【設問】1～8 に答えなさい。なお，波線のついた語句は4 ページの【注】を参考にすること。

【解説】 暗号と鍵

暗号とは，セキュア通信の手法の種類で，第三者が通信文を見ても特別な知識なしでは読めないように変換する，というような手法をおおまかには指す。いわゆる通信に限らず，記録媒体への保存などにも適用できる。「鍵」(key) は，暗号化する際に，同じ暗号方式を使用しながら利用者毎に暗号化の手順を異なるものにするために使用される。暗号方式と「平文」(plaintext) が同じであっても，鍵が違えば生成される「暗号文」(ciphertext) は異なるものになる。暗号文を復号する際にも，暗号化に使用した鍵に対応する鍵が使用される。復号の際には暗号化で使った鍵と同じ鍵か，または対応する（暗号化用とは別の）鍵が必要で，失うと復号できなくなる（または難しい）。例えば，シーザー暗号ではアルファベットをずらす数を変えることによって違う暗号文が生成される。この数が鍵である。実際のシーザーが用いたものはこの数（鍵）が3であった。

（出典 ウィキペディアの「暗号」と「鍵（暗号）」より抜粋，一部変更して引用）

【英文】

Figure 1.1: A sequence of 1000 random bits, represented as a long horizontal bar with a repeating pattern of small circles.

Figure 1.2: A sequence of 1000 random bits, represented as a long horizontal bar with a repeating pattern of small circles.

Figure 1.3: A sequence of 1000 random bits, represented as a long horizontal bar with a repeating pattern of small circles.

Figure 1.4: A sequence of 1000 random bits, represented as a long horizontal bar with a repeating pattern of small circles.

Figure 1.5: A sequence of 1000 random bits, represented as a long horizontal bar with a repeating pattern of small circles.

Figure 1.6: A sequence of 1000 random bits, represented as a long horizontal bar with a repeating pattern of small circles.

(出典 Susan Loepp and William K. Wootters 著, 「Protecting Information: From Classical Error Correction to Quantum Cryptography」 Cambridge University Press (2006) より一部

変更して引用)

【注】 語句（【英文】 への出現順）

cipher	暗号
cryptography	暗号法
scheme	枠組み, 仕組み
cryptanalysis	暗号解読
foil	阻む, 打ち負かす
encryption	暗号化
crack	(暗号を) 解読する, (暗号文を) 解く
code	暗号
cryptology	暗号学
substitution cipher	換字暗号 (平文の各文字を別の文字に置換する原理の暗号)
Caesar cipher	シーザー暗号
Julius Caesar	ジュリアス・シーザー (人名)
plaintext	平文
ciphertext	暗号文
remainder	余り (剰余)
adept at	～に熟達している
integer	整数
joke punchline	冗談の落ち (聞かせ所)
permutation	置換
frequency	頻度
cryptanalyst	暗号解読者
decrypt	復号 (解読) する
Giovan Battista Bellaso	ジョヴァン・バッティスタ・ベラソ (人名)
Blaise de Vigenère	ブレーズ・ド・ヴィジュネル (人名)
key	(暗号に用いる) 鍵
recipient	受信者
subtract	引く (減ずる)
straightforward	直接的な, ありのままの

【設問】

設問3～7では、【英文】中で述べられている A, B, \dots, Y, Z の26文字のみからなる英語テキストの平文を暗号化する場合について、答えなさい。

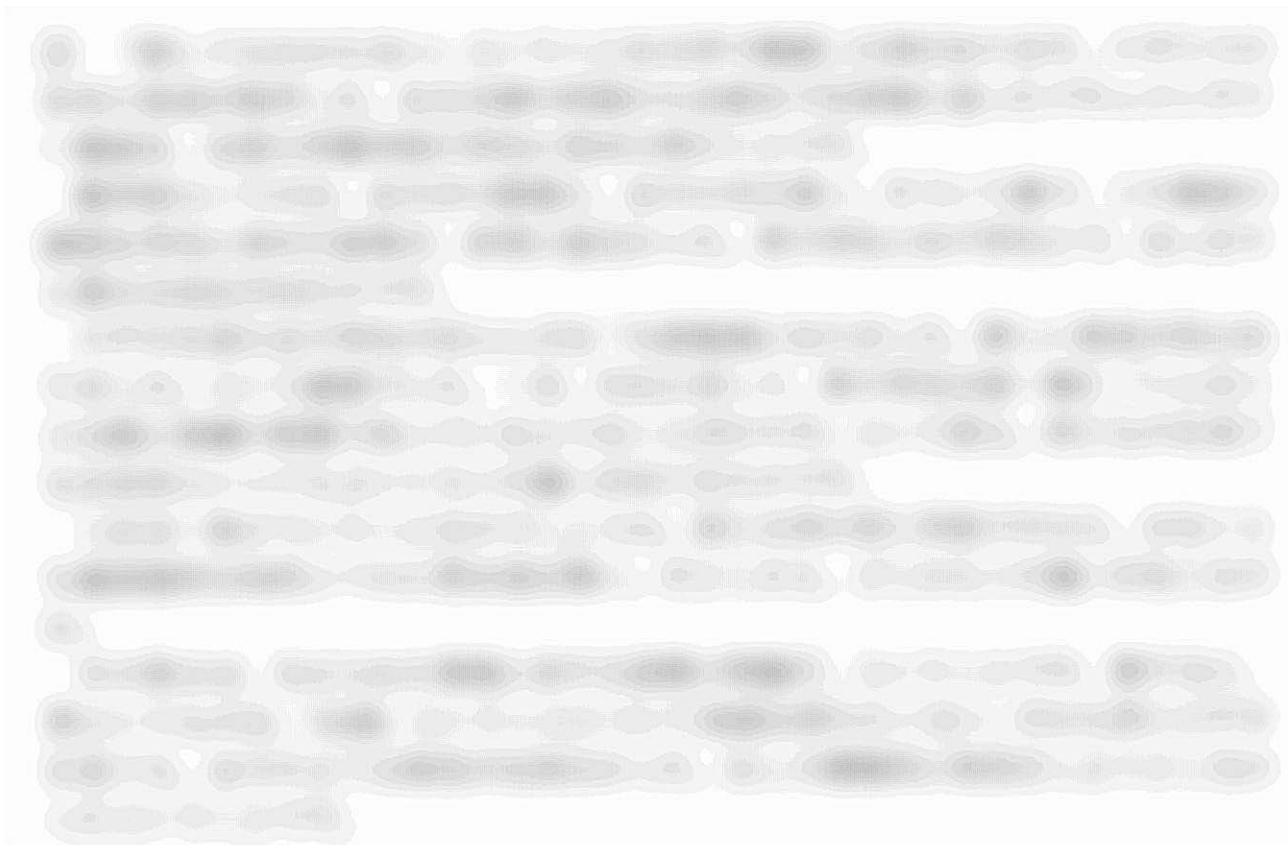
1. 下線部(c)を英訳しなさい。
2. 下線部(d)を和訳しなさい。
3. 次式で表される換字暗号(substitution cipher)を用いて平文 *FLOWER* を暗号化した暗号文を求めなさい。

$$y = x + 10 \pmod{26}$$

4. 鍵が *BOY* であるヴィジュネル(Vigenère)暗号を用いて平文 *FLOWER* を暗号化した暗号文を求めなさい。
5. 式(1)で表される換字暗号を用いて暗号化した暗号文を、逆に y から x を求め平文に復号する数式を mod 演算を用いて書きなさい。
6. 下線部(b)に関して、頻度分析(frequency analysis)とはどのような暗号の解読方法か、150字程度で述べなさい。
7. 式(2)で表される換字暗号を考える。下線部(a)に関して、 $a=2, b=1$ を用いると暗号文から平文が一つに定まらず正しく復号できない問題が発生する。何故この問題が発生するか、具体例を示して述べなさい。
8. 換字暗号を設計する際に安全性の面で重要と思われることを、その理由とともに100字程度で述べなさい。

Ⅱ

次の三つの文章（①、②、③）を読んで、8ページの【設問】9～11に答えなさい。





(出典 ①および②: 養老孟司著「バカの壁」 新潮社 (2003) より一部変更して引用、
③: 西垣通著「こころの情報学」 筑摩書房 (1999) より一部変更して引用)

【設問】

9. ①、②、③それぞれの主旨を述べなさい。ただし、①と②の主旨は40字以内、③の主旨は80字以内とする。
10. ③の「機械的な情報量」と「非機械的・意味内容的な情報量」の視点から、①が述べる「話してもわからない」とはどのようなことかを150字以内で述べなさい。
11. ①と②のそれぞれが示す人と情報に関する論点を基礎として、人と人のコミュニケーションにおいて起こりがちな問題とそれを避けるための工夫について、例をあげて300字以内で述べなさい。