MTH6115 **Cryptography**

Solutions 5

---

1 The Vigenère square is not self-adjugate unless $n = 2$. This is because for $n > 2$ it is not true that for every i and j, $i - j \equiv i + j \pmod{n}$. The Vigenère square is self-transpose because $j + i \equiv i + j \pmod{n}$. For the last part of the problem see Exercise Sheet 2, Problem 8(iii).

2 We have to show that for every $a, b \in \mathbb{Z}_n$, we have $a \oplus b = a \ominus b$. By definition $a \ominus b = c$, where c is the unique element in $\mathbb{Z}_n$ such that $c \oplus b = a$, that is $b - c = a$ in $\mathbb{Z}_n$. Solving this for c, we find that $c = b - a = a \oplus b$. So $a \ominus b = a \oplus b$.

3 a) (**Optional.**) The corresponding orthogonal array is

$$\begin{pmatrix} a & a & a & a & b & b & b & b & c & c & c & c & d & d & d & d \\ a & b & c & d & a & b & c & d & a & b & c & d & a & b & c & d \\ b & c & a & d & c & d & b & a & d & a & c & b & a & b & d & c \end{pmatrix}$$

b) The adjugate is

d	c	a	b
a	d	b	c
b	a	c	d
c	b	d	a

The transpose is

b	c	d	a
c	d	a	b
a	b	c	d
d	a	b	c

c) It is the same as the adjugate; see part (b).

4 Let us do the final two questions together. We note that Shannon's Theorem does not apply since the substitution table is not a Latin square. For all possible strings P_0, we must calculate $\mathrm{P}(p = P_0 \mid z = 23030)$. Firstly we calculate

$$\mathrm{P}(z = 23030 \mid p = P_0) = \frac{1}{4^5} \times \#\{\,\text{keys } K_0 \text{ such that } P_0 \oplus K_0 = 23030\,\}.$$

The ones we shall need are:

$$\mathrm{P}(z = 23030 \mid p = 21312) = \tfrac{12}{1024}; \qquad \mathrm{P}(z = 23030 \mid p = 20310) = 0;$$
$$\mathrm{P}(z = 23030 \mid p = 30312) = \tfrac{36}{1024}.$$

(The numerators of these are calculated as $1 \cdot 2 \cdot 1 \cdot 2 \cdot 3$, $1 \cdot 2 \cdot 1 \cdot 2 \cdot 0$ and $3 \cdot 2 \cdot 1 \cdot 2 \cdot 3$ respectively.) The Theorem of Total Probability now gives:

$$\mathrm{P}(z = 23030) = \sum_{P_0} \mathrm{P}(z = 23030 \mid p = P_0).\mathrm{P}(p = P_0).$$

We thus get $\mathrm{P}(z = 23030) = \frac{12}{1024} \cdot a + 0 \cdot b + \frac{36}{1024} \cdot c = \frac{12}{1024}(a + 3c)$, where we have excluded from our sum those P_0 for which $\mathrm{P}(p = P_0) = 0$. (Of course, in lowest terms we have $\frac{12}{1024} = \frac{3}{256}$ and $\frac{36}{1024} = \frac{9}{256}$, but for what we to do here, and problems like it, it is probably easier *not* to put the fractions in their lowest terms.) Finally, we apply Bayes's Theorem, which here states that

$$\mathrm{P}(p = P_0 \mid z = 23030) = \frac{\mathrm{P}(z = 23030 \mid p = P_0).\mathrm{P}(p = P_0)}{\mathrm{P}(z = 23030)},$$

at least when $\mathrm{P}(z = 23030) \neq 0$. We thus find new probabilities

$$\begin{aligned} \mathrm{P}(p = 21312 \mid z = 23030) &= \tfrac{a}{a+3c}, \\ \mathrm{P}(p = 20310 \mid z = 23030) &= 0, \\ \mathrm{P}(p = 30312 \mid z = 23030) &= \tfrac{3c}{a+3c}. \end{aligned}$$

Of course, we have $\mathrm{P}(p = P_0 \mid z = 23030) = 0$ for $P_0 \neq 21312$, 20310 or 30312. Specialising to $(a, b, c) = (\frac{1}{5}, \frac{3}{10}, \frac{1}{2})$ gives the new probabilities for Question 4 as being $\frac{2}{17}$, 0 and $\frac{15}{17}$ respectively.

Note that in the above we need $a+3c \neq 0$, which will be the case unless $b = 1$ and $a = c = 0$. In any other case, the new probabilities lie between 0 and 1 (inclusive) and sum to 1. However if $(a, b, c) = (0, 1, 0)$ then we get $\mathrm{P}(z = 23030) = 0$, which means that the ciphertext cannot be 23030 (unless one or more of the P_0 with $\mathrm{P}(p = P_0) = 0$ can actually occur), so some sort of contradiction has (almost certainly) arisen here. In some contexts, events with probability 0 *can* happen. For example, if one tosses a fair coin countably infinitely often it can come up heads every time, but this event has probability 0.

5 See previous question.