7

5.21

We continue with the coin tossing scenario from Example 5.23, so our experiment consists in tossing a fair coin ten times. Compute the probabilities of the following events.

a

The first and last tosses are both heads.

Answer

$(0.5)(0.5) = 0.25$

b

Either the first toss or the last toss (or both) are heads.

Answer

$0.5 + 0.5(0.5) = 0.75$

c

Either the first toss or the last toss (but not both) are heads.

Answer

$(0.5)(0.5) + (0.5)(0.5) = 0.5$

d

There are exactly k heads and 10 − k tails. Compute the probability for each value of k between 0 and 10. (Hint. To save time, note that the probability of exactly k heads is the same as the probability of exactly k tails.)

Answer

x	P(x)
0	0.00098
1	0.00977

x	P(x)
2	0.04395
3	0.11719
4	0.20508
5	0.24609
6	0.20508
7	0.11719
8	0.04395
9	0.00977
10	0.00098

e

There is an even number of heads.

✓ **Answer**
The sum of all the even numbers

0.50002 (possible rounding error)

f

There is an odd number of heads.

✓ **Answer**
0.50001 (another possible rounding error)

Entropy

Consider a cryptosystem with $M = \{a, b, c\}$, $K = \{K1, K2, K3\}$, and $C = \{1, 2, 3, 4\}$.

Suppose the encryption rules are as follows:

	a	b	c
K1	1	2	3
K2	2	3	4
K3	3	4	1

Assume the keys are equiprobable, and the plaintext probabilities are:

$P(a) = 1/2$, $P(b) = 1/3$, and $P(c) = 1/6$.

1

$H(M)$

✓ **Answer**

$H(M) = -\left(\frac{1}{2}\log_2\left(\frac{1}{2}\right) + \frac{1}{3}\log_2\left(\frac{1}{3}\right) + \frac{1}{6}\log_2\left(\frac{1}{6}\right)\right)$
$= 1.46 \text{ bits}$

2

$H(K)$

✓ **Answer**

$\log_2(3) = 1.58 \text{ bits}$

3

$H(C)$

✓ **Answer**

$P(C = 1) = \frac{2}{9}$
$P(C = 2) = \frac{5}{18}$
$P(C = 3) = \frac{1}{3}$
$P(C = 4) = \frac{1}{6}$

$H(C) = 1.87 \text{ bits}$

4

$H(K|C)$

✓ **Answer**

$P(C\|\|K)$	**K1**	**K2**	**K3**
1	1/2	0	1/6
2	1/3	1/2	0
3	1/6	1/3	1/2
4	0	1/6	1/3

$P(K\|C)$	**K1**	**K2**	**K3**	$H(K\|C)$
1	3/4	0	1/4	0.8113
2	2/5	3/5	0	0.9710
3	1/6	1/3	1/2	1.4591
4	0	1/3	2/3	0.9183

$$\frac{2}{9} \cdot 0.8113 + \frac{5}{18} \cdot 0.9710 + \frac{1}{3} \cdot 1.4591 + \frac{1}{6} 0.9183$$
$$= 1.089 \text{ bits}$$

5

$H(M|C)$

✓ Answer

$$H(M|C) = H(M) + H(K) - H(C)$$
$$= 1.17 \text{ bits}$$