

# Cryptographic Secret Sharing

## ANSWER KEY

Girls Talk Math

### 1 Probability and Randomness

#### Answer 1.1

(a) Sample space:

$$\{A\Diamond, 2\Diamond, 3\Diamond, \dots, K\Diamond, A\heartsuit, \dots, K\heartsuit, A\spadesuit, \dots, K\spadesuit, A\clubsuit, \dots, K\clubsuit\}$$

Probability distribution:

$$\left\{ \frac{1}{52}, \dots, \frac{1}{52} \right\}$$

(where  $\frac{1}{52}$  is repeated 52 times).

(b) Sample space:

$$\{\text{registered}, \text{not registered}\}$$

Probability distribution:

$$\{0.95, 0.05\}$$

#### Answer 1.2

- (a) **Uniform.** The deck is shuffled, so a card is equally likely to be in any one place in the deck.
- (b) **Not uniform.** You are more likely to draw a lower card if you draw from the beginning of the deck instead of the end.

- (c) **Not uniform.** Though it fluctuates, weather generally follows large-scale patterns that depend on the season, latitude and longitude, the air masses present, and so on. This is called climate. The reason meteorologists can predict the weather is precisely because it is not a uniformly random variable.
- (d) **Uniform.** Every number is equally likely to be rolled.
- (e) **Not uniform.** In fact, some birthdays are more likely to occur than others. Summer birthdays are slightly more common, for instance.<sup>1</sup>

**Answer 1.3**  $d \leftarrow_{\$} \{1, 2, 3, 4, 5, 6\}$ . (You could have chosen any name for the variable in the place of  $d$ .)

**Answer 1.4** To find  $\Pr[B \mid A]$ , we simply switch the places of  $A$  and  $B$  in the formula:

$$\Pr[B \mid A] = \frac{\Pr[A \text{ and } B]}{\Pr[A]}$$

- (a) 0;  $B$  takes up none of  $A$ 's space.
- (b)  $\frac{1}{16} \div \frac{1}{8} = \frac{1}{2}$ ;  $B$  overlaps with half of  $A$ .
- (c)  $\frac{1}{8} \div \frac{1}{8} = 1$ ;  $B$  fully encompasses  $A$ , so if our outcome is in  $A$ , it is certainly in  $B$ .

**Answer 1.5** Let  $c_1$  and  $c_2$  be random variables representing the first and second coin toss, respectively. Since the coin tosses are independent,

$$\begin{aligned} & \Pr[c_1 = H \text{ and } c_2 = H] \\ &= \Pr[c_1 = H] \cdot \Pr[c_2 = H] \\ &= \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \end{aligned}$$

---

<sup>1</sup>You can see a visualization of the probability of each birthday here: <http://thedailyviz.com/2016/09/17/how-common-is-your-birthday-dailyviz/>.

**Answer 1.6** There are two ways of getting one heads outcome: (1) the first toss is heads ( $c_1 = H$ ), and we don't do another coin toss, or (2) the first toss comes up tails, and the second one comes up heads ( $c_1 = T$  and  $c_2 = H$ ).

$$\begin{aligned}
 & \Pr[c_1 = H] + \Pr[c_1 = T \text{ and } c_2 = H] \\
 &= \Pr[c_1 = H] + \Pr[c_2 = H] \cdot \Pr[c_1 = T] \\
 & \hspace{10em} (\text{coin tosses are independent events}) \\
 &= \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \\
 &= \frac{1}{2} + \frac{1}{4} \\
 &= \frac{3}{4}
 \end{aligned}$$

**Answer 1.7**

- (a) Rolling an even number means rolling 2, 4, **or** 6, each of which happen with probability  $\frac{1}{6}$ , so the probability of rolling an even number is  $\frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$ .

Another way to see this is that our roll has to land in the set  $\{2, 4, 6\}$  and not in  $\{1, 3, 5\}$ . Because even number happens with equal probability and the sets are of equal size, the dice roll lands in each of the two sets with equal probability. So landing in one set happens with probability  $\frac{1}{2}$ .

- (b) This happens if the first roll is a 1 **and** the second roll is a 2. Each of those occurs with probability  $\frac{1}{6}$ , so the answer is  $\frac{1}{6} \cdot \frac{1}{6} = \frac{1}{6 \cdot 6} = \frac{1}{36}$ .

- (c) This can be broken down into cases based on the first roll:

$$\begin{aligned}
 & \Pr[\text{roll} > 1 \mid \text{first roll is 1}] \cdot \Pr[\text{first roll is 1}] \\
 &+ \Pr[\text{roll} > 2 \mid \text{first roll is 2}] \cdot \Pr[\text{first roll is 2}] \\
 &+ \Pr[\text{roll} > 3 \mid \text{first roll is 3}] \cdot \Pr[\text{first roll is 3}] \\
 &+ \Pr[\text{roll} > 4 \mid \text{first roll is 4}] \cdot \Pr[\text{first roll is 4}] \\
 &+ \Pr[\text{roll} > 5 \mid \text{first roll is 5}] \cdot \Pr[\text{first roll is 5}] \\
 &+ \Pr[\text{roll} > 6 \mid \text{first roll is 6}] \cdot \Pr[\text{first roll is 6}]
 \end{aligned}$$

$$\begin{aligned}
&= \Pr[\text{roll} > 1] \cdot \frac{1}{6} + \Pr[\text{roll} > 2] \cdot \frac{1}{6} \\
&\quad + \Pr[\text{roll} > 3] \cdot \frac{1}{6} + \Pr[\text{roll} > 4] \cdot \frac{1}{6} \\
&\quad + \Pr[\text{roll} > 5] \cdot \frac{1}{6} + \Pr[\text{roll} > 6] \cdot \frac{1}{6} \\
&= \frac{1}{6} \left( \frac{5}{6} + \frac{4}{6} + \frac{3}{6} + \frac{2}{6} + \frac{1}{6} + 0 \right) \\
&= \frac{1}{6} \left( \frac{15}{6} \right) \\
&= \frac{1}{6} \cdot \frac{5}{2} = \frac{5}{12}
\end{aligned}$$

- (d) Either I roll a 5 or 6 on my first roll, or I roll a 1 and my second roll is a 5 or 6:

$$\begin{aligned}
&\Pr[\text{first roll is 5}] + \Pr[\text{first roll is 6}] \\
&\quad + (\Pr[\text{second roll is 5} \mid \text{first roll is 1}] + \Pr[\text{second roll is 6} \mid \text{first roll is 1}]) \\
&\quad \cdot \Pr[\text{first roll is 1}] \\
&= \frac{1}{6} + \frac{1}{6} + \left( \frac{1}{6} + \frac{1}{6} \right) \frac{1}{6} \\
&= \frac{1}{3} + \left( \frac{1}{3} \right) \frac{1}{6} \\
&= \frac{1}{3} + \frac{1}{18} \\
&= \frac{7}{18}
\end{aligned}$$

### Answer 1.8

- (a) **indistinguishable:** both  $\left\{ \frac{1}{2}, \frac{1}{2} \right\}$
- (b) **not indistinguishable:** the uniform distribution with all probabilities equal to  $\frac{1}{52}$  is not the same as the uniform distribution with all probabilities  $\frac{1}{6} \left( \frac{1}{2} \right)^3 = \frac{1}{48}$ .
- (c) **indistinguishable:**  $\left\{ \frac{1}{4}, 3 \left( \frac{1}{4} \right) \right\} = \left\{ \frac{13}{52}, \frac{39}{52} \right\} = \left\{ \frac{1}{4}, \frac{3}{4} \right\}$

## 2 Secret Sharing

### 2.1 A simple secret sharing

**Sample Answer 2.1** Note that for any secret  $s$  there are many possible answers based on the randomness  $s_1$  that's used.

An example application of **Share** with  $s = 42$  follows. First,  $s_1$  is chosen at random. Say  $s_1 = 18$ . Then **Share** outputs  $(18, 42 - 18) = (18, 24)$ .

$s_1$  could also be larger than  $s$ , e.g.  $s_1 = 321$ . In this case, **Share** outputs  $(321, 42 - 321) = (42, -279)$ .

**Answer 2.2** Reconstruction simply adds the shares together:

- (a)  $2 + 6 = 8$
- (b)  $4 + 1 = 5$
- (c)  $10 + 2 = 12$
- (d)  $115 + (-103) = 12$
- (e)  $559 + (-544) = 15$

**Answer 2.3** Additive secret sharing with 3 shares:

<u>Share(<math>s</math>)</u>	<u>Rec(<math>s_1, s_2, s_3</math>)</u>
$s_1, s_2 \leftarrow_{\$} \{1, \dots, 2^\lambda\}$ $s_3 = s - (s_1 + s_2)$ <b>return</b> $(s_1, s_2, s_3)$	<b>return</b> $s_1 + s_2 + s_3$

In fact, the additive secret sharing scheme can be adapted to share the secret  $s$  into any natural number  $n$  of shares:

<u>Share(<math>s</math>)</u>	<u>Rec(<math>s_1, \dots, s_n</math>)</u>
$s_1, \dots, s_{n-1} \leftarrow_{\$} \{1, \dots, 2^\lambda\}$ $s_n = s - (s_1 + \dots + s_{n-1})$ <b>return</b> $(s_1, \dots, s_n)$	<b>return</b> $s_1 + \dots + s_n$

(Where if **Rec** is run on the incorrect number of shares—anything except 3 and  $n$ , respectively—the algorithms return  $\perp$ .)

## 2.2 Formal Definitions\*

**Sample Answer 2.4** The adversary should only be able to win about half the time. This is because  $s_i$  looks random to the adversary. The key part of the scheme is that  $s_1$  is chosen uniformly at random, thereby making both  $s_1$  and  $s_2$  uniformly distributed and independent of  $s$ .

**Answer 2.5** No. There is an adversary  $\mathcal{A}$  whose advantage in the privacy game is not small.

$\mathcal{A}$  works as follows: it chooses values  $x_0, x_1$  such that  $x_0$  is even and  $x_1$  is odd (the opposite works too) and lets  $i = 1$ . When the game sends it the share  $s_1$ ,  $\mathcal{A}$  checks if  $s_1 < 2^\lambda/2$ . If so, it outputs  $b' = 0$ ; otherwise, it outputs  $b' = 1$ .

$\mathcal{A}$  wins the game with probability  $3/4$ :

$$\begin{aligned}\Pr[\text{SS-priv}_{\mathcal{A},\mathcal{S}}(t, n) = 1] &= \Pr[b' = b \mid b = 0] + \Pr[b' = b \mid b = 1] \\ &= \frac{1}{2}(1) + \frac{1}{2}\left(\frac{1}{2}\right) \\ &= \frac{1}{2} + \frac{1}{4} = \frac{3}{4}\end{aligned}$$

So  $\mathcal{A}$ 's advantage is  $\frac{3}{4} - \frac{1}{2} = \frac{1}{4}$ , which is not small.

## 3 Shamir's Secret Sharing

### 3.1 Polynomials

#### Answer 3.1

- (a) degree: 2,  $y$ -intercept: -1
- (b) degree: 2,  $y$ -intercept: 11
- (c) degree: 3,  $y$ -intercept: 0
- (d) degree: 5,  $y$ -intercept: -15
- (e) degree: 3 ( $= 2 + 1$ ),  $y$ -intercept: -3 ( $= -1 \cdot 3$ )
- (f) degree: 3 ( $= 1 + 1 + 1$ ),  $y$ -intercept: 120 ( $= 2 \cdot -6 \cdot 2 \cdot -5$ )
- (g) degree: 4 ( $= 3 + 1$ ),  $y$ -intercept: 32 ( $= 2 \cdot 16$ )

#### Answer 3.2

- (a) 3
- (b) 3
- (c) 4
- (d) 6
- (e) 4
- (f) 4
- (g) 5

#### 3.1.2 Lagrange Interpolation\*

#### Answer 3.3

- (a)  $2(1)+2(2)+2(3)+2(4)+2(5) = 2(1+2+3+4+5) = 2(15) = 30$
- (b)  $1 + 1 + 1 + 1 + 1 = 5(1) = 5$
- (c)  $1 + 5 + (-3) + 0 + 8 = 11$
- (d)  $1 + 5 + (-3) = 3$

**Answer 3.4**

(a)  $2(1) \cdot 2(2) \cdot 2(3) \cdot 2(4) \cdot 2(5) = 2^5 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 32 \cdot 120 = 3840$

(b)  $1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 = 1$

(c)  $1 \cdot 5 \cdot (-3) \cdot 0 \cdot 8 = 0$

(d)  $1 \cdot 5 \cdot (-3) = -15$

**Answer 3.5**  $3x^2 + 7x - 12$

**Answer 3.6** N/A

**Answer 3.7** N/A