Cryptographic Secret Sharing
ANSWER KEY

Girls Talk Math

1 Probability and Randomness

Answer 1.1

(a) Sample space:

$\{A\diamondsuit, 2\diamondsuit, 3\diamondsuit, \ldots, K\diamondsuit, A\heartsuit, \ldots, K\heartsuit, A\spadesuit, \ldots, K\spadesuit, A\clubsuit, \ldots, K\clubsuit\}$

Probability distribution:

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

(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 any card is equally likely to be at the top of the deck.

(b) **Not uniform.** Since the deck has only one correct ”order”, the first card to be drawn will always be the same.

(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 meteoroligists can predict the weather is precisely because it is not a uniformly random variable: each day, certain outcomes are more likely than others (in the summer, for instance, it is very likely that the weather will be sunny, while snow has a near 0% chance of occurring).

(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.[1]

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.

[1] 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 1.5 Let c_1 and c_2 be random variables representing the first and second coin toss, respectively. Since the coin tosses are independent,

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

Answer 1.6 There are two ways of getting heads once: (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 $c_2 = H$).

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

You might also have realized that the only way *not* to get heads once was to get tails twice (TT). In that case you could have calculated the probability as $1 - \Pr[TT] = 3/4$.

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 and 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 every 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 the even 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:

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

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

(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:

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

Answer 1.8

(a) **not perfectly indistinguishable:** the uniform distribution with all probabilities equal to $\frac{1}{52}$ is not the same as the uniform distribution with all probabilities $\frac{1}{6}\left(\frac{1}{2}\right)^3 = \frac{1}{48}$. The sample spaces are also different.

(b) **perfectly indistinguishable:** $D_1 = \left\{3\left(\frac{1}{4}\right), \frac{1}{4}\right\}$ over the sample space $\{\text{yes}, \text{no}\}$ and $D_2 = \left\{\frac{39}{52}, \frac{13}{52}\right\}$ over the same sample space. Since the sample spaces are the same and both of the probability distributions simplify to $\left\{\frac{3}{4}, \frac{1}{4}\right\}$, D_1 and D_2 are perfectly indistinguishable.

(c) **not perfectly indistinguishable:** both distributions are $\left\{\frac{1}{2}, \frac{1}{2}\right\}$, but D_1 is over the sample space $\{\text{even}, \text{odd}\}$ while D_2's sample space is $\{H, T\}$.

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 $(18, 42 - 18 \mod 1024) = (18, 24 \mod 1024) = \mathbf{(18{,}24)}$.

s_1 could also be larger than s, e.g. $s_1 = 321$. In this case, Share outputs $(321, 42-321 \mod 1024) = (321, -279 \mod 1024) = (321, 1024 - 279) = \mathbf{(321{,}745)}$.

Answer 2.2 Reconstruction simply adds the shares together (reducing modulo 1024):

(a) $2 + 6 \mod 1024 = 8 \mod 1024 = \mathbf{8}$

(b) $4 + 1 \mod 1024 = 5 \mod 1024 = \mathbf{5}$

(c) $10 + 2 \mod 1024 = 12 \mod 1024 = \mathbf{12}$

(d) $115 + 921 \mod 1024 = 1036 \mod 1024 = 1036 - 1024 = \mathbf{12}$

(e) $559 + 480 \mod 1024 = 1039 \mod 1024 = 1039 - 1024 = \mathbf{15}$

Answer 2.3 Additive secret sharing with 3 shares:

```
Share($s$)
    $s_1, s_2 \leftarrow_\$ \{0, \ldots, 2^\lambda - 1\}$
    $s_3 = s - (s_1 + s_2) \mod 2^\lambda$
    return $(s_1, s_2, s_3)$

Rec($s_1, s_2, s_3$)
    return $s_1 + s_2 + s_3 \mod 2^\lambda$
```

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

```
Share($s$)
$s_1, \ldots, s_{n-1} \leftarrow_\$ \{1, \ldots, 2^\lambda\}$
$s_n = s - (s_1 + \ldots + s_{n-1}) \mod 2^\lambda$
return $(s_1, \ldots, s_n)$
```

```
Rec($s_1, \ldots, s_n$)
return $s_1 + \ldots + s_n \mod 2^\lambda$
```

(Where if Rec is run on the incorrect number of shares—anything except n—the algorithm returns $\perp$.)

2.2 Formal Definitions*

Sample Answer 2.4 The person playing the role of 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:

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

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

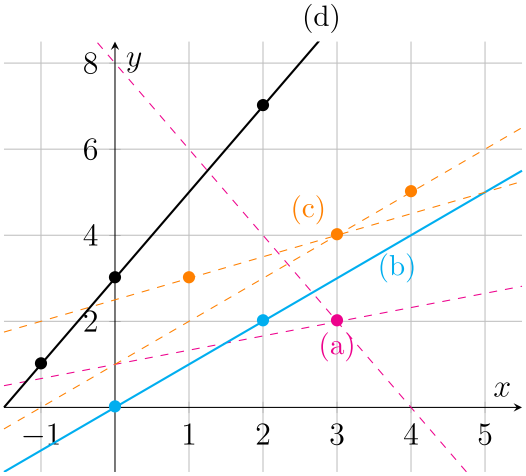
(d) 6

(e) 4

(f) 4

(g) 5

Answer 3.3



(a) No; there are not enough points to define a *unique* degree-1 polynomial, and in fact there are infinitely many degree-1 polynomials passing through this point. (In pink above.)

(b) Yes; these points uniquely define the polynomial $f(x) = x$. (In light blue above.)

(c) No; there is no degree-1 polynomial passing through these points because they are not properly aligned. However, they do define a unique degree-2 polynomial. (In orange above.)

(d) Yes; these points uniquely define the polynomial $f(x) = 2x + 3$. (In black above.)

3.1.2 Lagrange Interpolation*

Answer 3.4

(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 3.5

(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 3.6

(a) $x_0 = 0$:

$$\begin{aligned}
\ell_0(0) &= \frac{(0-1)(0-4)}{4} = \frac{(-1)(-4)}{4} &&= 1 \\
\ell_1(0) &= \frac{0(0-4)}{-3} = \frac{0(-4)}{-3} &&= 0 \\
\ell_2(0) &= \frac{0(0-1)}{12} = \frac{0(-1)}{12} &&= 0
\end{aligned}$$

(b) $x_1 = 1$:

$$\begin{aligned}
\ell_0(1) &= \frac{(1-1)(1-4)}{4} = \frac{(0)(-3)}{4} &&= 0 \\
\ell_1(1) &= \frac{1(1-4)}{-3} = \frac{1(-3)}{-3} &&= 1 \\
\ell_2(1) &= \frac{1(1-1)}{12} = \frac{1(0)}{12} &&= 0
\end{aligned}$$

(c) $x_2 = 4$:

$$\begin{aligned}
\ell_0(4) &= \frac{(4-1)(4-4)}{4} = \frac{(3)(0)}{4} &&= 0 \\
\ell_1(4) &= \frac{4(4-4)}{-3} = \frac{4(0)}{-3} &&= 0 \\
\ell_2(4) &= \frac{4(4-1)}{12} = \frac{4(3)}{12} &&= 1
\end{aligned}$$

Answer 3.7 $3x^2 + 7x - 12$

Answer 3.8 N/A

Answer 3.9 N/A