RSA Revisited

Please read through the following articles from Duo and answer the proceeding questions:

**Duo:SHA-1 ‘Fully and Practically Broken by New Collision**

**Duo:Flaw in Crypto library causes revocation of SSH keys for GIT services**

**Task 1:** Using an example from one of the readings, what are the potential vulnerabilities of using broken encryption schemes like SHA-1?

**Pass condition:** Students could point to a place in the text where their answer stemmed from or briefly explain their answers from the text.

**Examples:** Potential vulnerabilities of using broken encryption schemes like SHA-1:

- “Currently, the concrete impact is mostly for people who use the PGP web of trust. If they trust SHA-1 signatures, an attacker could impersonate their contacts,” (Article 1)
- The end result is that those keys could be guessed relatively easily and an attacker could then decrypt sensitive data or gain access to a victim’s account. (Article 2)
- “Our work show that SHA-1 is now fully and practically broken for use in digital signatures. GPU technology improvements and general computation cost decrease will quickly render our attack even cheaper, making it basically possible for any ill-intentioned attacker in the very near future” (Article 1)

Now read this article from Microsoft about their decisions to remove windows updates that use SHA-1. While you read think about the responsibility technology companies have to their users to ensure their privacy.

**Task 2:** What have tech companies done to prevent more vulnerabilities from SHA-1? Reference one strategy used by tech company’s mentioned in the article.

**Pass condition:** Again, students should point to a place in the text where their answer stemmed from or briefly explain their answers from the text.

**Examples:**
• Microsoft will retire content that is Windows-signed for Secure Hash Algorithm 1 (SHA-1) from the Microsoft Download Center on August 3, 2020,

• Switching away from SHA-1 has been in the works for a long time. Major browsers started blocking websites using certificates signed with SHA-1 in 2017.

• Apple removed SHA-1 from iOS 13 and macOS Catalina. OpenSSH deprecated SHA-1 for its login process earlier this year. After Microsoft stopped using SHA-1 to sign and authenticate updates, it stopped updating devices without SHA-2 support.

• As a result, GitHub recommends that organizations check any SSH keys linked to their GitHub accounts—or any other service that uses a potentially vulnerable key—and rotate any keys that were generated using a vulnerable version of the library.

• "Using the SHA-1 hashing algorithm in digital certificates could allow an attacker to spoof content, perform phishing attacks, or perform man-in-the-middle attacks.

Counting Arguments

A counting argument shows that the LHS (lefthand side) and the RHS (righthand side) of some equation count the same thing. Instead of using algebraic manipulation, we explain why both sides enumerate the elements of some set, just in different ways.

For instance, consider the following identity.

\[
\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}
\]

Let \( S \) be a set with \( n \) elements.

• The LHS counts the number of ways to form a subset of \( S \) size \( k \).

• The RHS also counts the number of subsets of size \( k \). It partitions it into two parts:
  
  – \( k \)-sized subsets \textbf{with} a fixed element \( x \). Since we already know \( x \) is in the subset, so we just want to pick \( k - 1 \) more elements from the \( n - 1 \) remaining elements.

  – \( k \)-sized subsets \textbf{without} \( x \). We know we can’t pick \( x \) for our subsets, so we just choose \( k \) elements from \( n - 1 \) other elements in \( S \).
Task 3

Below is a table of counting problems involving putting \( k \) balls in \( n \) distinct bins, and seven expressions. Match each problem with its solution.

<table>
<thead>
<tr>
<th></th>
<th>No restrictions</th>
<th>At most 1 ball per bin</th>
<th>At least 1 ball per bin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>assume ( k \leq n )</td>
<td>assume ( k \geq n )</td>
<td></td>
</tr>
<tr>
<td>Identical balls</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Distinct balls</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
A & \left( \frac{n}{k} \right) n^k & B & \binom{k-1}{n-1} & C & \frac{n!}{(n-k)!} & D & \binom{k+n-1}{k} & E & n^k - \sum_{i=1}^{n-1} \binom{n}{i} (n-i)^k (-1)^{i+1} & F & n! \binom{k}{n} n^{k-n} \\
\end{align*}
\]

1. This is stars and bars, so it’s E.

2. Each of the \( k \) balls have \( n \) options, so it’s B.

3. We have \( n \) bins and \( k \) of them will have 1 ball in them. There is a bijection between this situation and \( n \)-bit binary strings with \( k \) ones and \( n-k \) zeros. So, this is choosing which digits will have 1s, which is A.

4. For each of the options from question 3, which is \( \binom{n}{k} \), there are \( k! \) ways of scrambling the balls in sequence. So we have \( \frac{n!}{k!(n-k)!} k! \), which cancels out to D. Note this is also the permutation \( P(n, k) \).

5. This can be reduced to stars and bars, but we pre-distribute \( n \) balls to the \( n \) bins to make sure there’s 1 in each bin. Then, with the \( k-n \) balls left, we distribute it into \( k \) bins, which is \( \binom{k-n+n-1}{n-1} = \binom{k-1}{n-1} \), which is C.

6. We’ll count the ways there is a bin with no balls, using inclusion-exclusion, and find the complement of that. Let \( E_j \) be the event that the \( j \)-th bin is empty, and we want to find \( |E_1 \cup \cdots \cup E_n| \). Each \( E_j \) is of size \( (n-1)^k \), since the \( k \) balls can go to any of the \( n-1 \) other bins. Then we take out the pairwise intersections, each of which are of size \( (n-2)^k \), and so on to \( (n-i)^k \) generally. The number of \( i \)-way intersections is \( \binom{n}{i} \), which we also have to multiply by. To include all of this in a summation, along with using \( (-1)^{i+1} \) to simulate the alternating addition/subtraction. Note that the last term, \( i = n \), is always zero (why?). This is expression F.
Note: This is equivalent to asking how many surjective functions there are from a domain of size \( k \) to a codomain of size \( n \).

Checkpoint 1 - Call a TA over!
Inclusion/Exclusion

Say we have two sets, $A$ and $B$, and we want to know how many elements there are in their union, $A \cup B$. If $A$ and $B$ have no elements in common, we can compute this just by adding the cardinality of each, $|A| + |B|$. However, this approach will not work in general.

For instance, if $A = \{1, 2\}$ and $B = \{1, 3\}$, then $A \cup B = \{1, 2, 3\}$. $|A \cup B| = 3$, but $|A| + |B| = 2 + 2 = 4$. The problem is that we’ve double counted the elements that are in both $A$ and $B$, that is, element 1. To fix this problem, we should subtract $|A \cap B|$.

The resulting Inclusion/Exclusion property for two sets is:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$ 

Let’s try generalizing this idea to three sets, $A$, $B$, and $C$!
If we tried adding $|A| + |B| + |C|$, which regions would we double count? Which regions would we triple count?

$w, x, y$ get double counted and $z$ gets triple counted.

As it turns out, the final formula for $|A \cup B \cup C|$ is the following. Convince yourself that it works!

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|.$$ 

Going further, we can repeat this process for any number of sets, alternating between adding and subtracting the sizes of sets.

**Task 4**

a. Let $S = \{1, 2, 3, 4, 5\}$.

i. How many permutations of $S$ contain the sequence 24?

   Treat 24 as a single units, so we’re left with permuting $\{1, 3, 5, 24\}$. There are $4!$ permutations.

   ii. How many permutations of $S$ contain the sequence 52?

   Same as above, $4!$.

   iii. How many permutations of $S$ contain the sequence 24 or 52?

   Let $A$ be the set of permutations where 24 appears and $B$ be the set of permutations where 52 appears. $A \cap B$ will be the set of permutations where 524 appears. If we treat this as a unit, we permute 3 elements, $|A \cap B| = 3!$. Thus, $|A \cup B| = |A| + |B| - |A \cap B| = 4! + 4! - 3! = 42$.

b. Let $X$ and $Y$ be sets such that $|X| = 8$ and $Y = \{a, b, c\}$.

i. How many functions from $X \to Y$ do not map to $a$?

   Each of the 8 elements in $X$ have two options of where to map to: $b$ or $c$. So, it’s $2^8 = 256$.

ii. How many functions from $X \to Y$ do not map to $a$ and also do not map to $b$?
iii. How many functions from $X \to Y$ are not surjective?

**Hint:** A function is not surjective if nothing maps to $a$, nothing maps to $b$, or nothing maps to $c$.

Let the set of functions not mapping to $a$ be $A$, not mapping to $b$ be $B$, and not mapping to $c$ be $C$.

$|A| = |B| = |C| = 2^8$, as established above, since the argument for $i$ can be made to all three sets.

$|A \cap B| = |B \cap C| = |A \cap C| = 1$, as the argument for $ii$ can also be generalized.

$A \cap B \cap C$ is functions from $X$ to $\{\}$, which is no functions.

The total number of non-surjective functions is $|A \cup B \cup C| = 3 \cdot 2^8 - 3 \cdot 1 + 0 = 765$.

---

**The Pigeonhole Principle**

Let’s say we have $n$ pigeons who are trying to fit in $n - 1$ holes.

It isn’t possible for each pigeon to get its own hole: at least two of them are going to have to share. It could be the case that they are all in the same hole, or, like the picture above, all but 2 pigeons get their own hole, or anything in between.
This is the Pigeonhole Principle: in general, if we are assigning \( n \) objects to \( m \) categories, where \( n > m \), there is at least one category that has more than one object assigned to it.

Solve the following problems using the Pigeonhole Principle:

**Task 5**

a. Celeste is pulling socks out of her drawer. She only has four types of socks: solid, striped, polka-dotted, and ones with coffee mugs on them. What is the minimum number of socks Celeste should pull out to ensure she has a pair?

We are asking what the size of the domain of a function needs to be, where the function is from socks to types, such that there is some style with at least 2 socks that map to it. The answer is therefore 5.

b. There are \( n > 2 \) astronauts having a party on Mars. Throughout the night, they dance with each other in pairs.

i. The minimum number of total dance partners someone can have is 0 (they didn’t dance with anyone). What is the maximum number of dance partners one can have?

\[ n - 1, \text{ dancing with everyone else} \]

ii. Prove that at least 2 astronauts have the same number of dance partners by the end of the night. (Come back to this question later if you get stuck.)

The possible number of dance partners are \([0, n - 1]\). Trying to apply the pigeonhole principle directly doesn’t work, since it seems like all \( n \) astronauts could have all \( n \) possible numbers of partners. But, if someone has 0 dance partners, then no one can have \( n - 1 \). So, the choices are either \([1, n - 1]\) or \([0, n - 2]\), each of which results in \( n - 1 \) possible options for the number of dance partners. Since we have \( n \) astronauts, two people must have the same number of partners.

c. Optional: Given any 5 points inside a square with side length 2, there is always a pair whose distance apart is at most square root of 2.

Partition the square into 4 unit squares. Then, there is a square with two dots. The maximum distance between two points within a unit square is square root of 2.

**Checkpoint 2 - Call over a TA**
Probability

A finite discrete probability space is a pair \((S, \Pr)\) for some finite set \(S\) and some function \(\Pr: S \rightarrow \mathbb{R}\), where, for all \(x \in S\), \(\Pr(x) > 0\), and \(\sum_{x \in S} \Pr(x) = 1\). The set \(S\) is called the sample space, and the elements of \(S\) are called outcomes. The function \(\Pr\) is called the probability distribution function.

Where do these definitions come from? It’s all about predictions. The sample space \(S\) is supposed to represent a set of atomic outcomes—that is, the set of all things that can happen. All these outcomes are mutually exclusive.

An event is a subset of the sample space \(S\), containing some atomic outcomes. For example, if I flip a coin 3 times, the outcomes are HHH, TTT, \ldots, so the sample space is \(S = \{\text{HHH, TTT, TTH, \ldots}\}\), with \(2^3 = 8\) outcomes. An event can be: We see exactly 1 H, which we view as a set of outcomes \(\{\text{HTT, THT, TTH}\}\). An event can also be the empty set: for example, the event We see 4 Hs is the empty set, since it is not a possible outcome (it does not correspond to anything in the sample space). Similarly, the event We see an elephant is the empty set for this probability space.

How many different events can the above sample space have? Since each event is a subset of the sample space, the number of events is equal to the number of possible subsets, which here is \(2^8\) (since the sample space has 8 elements).

To understand the probability distribution function, let’s think about our sample space as a box of area 1. Then, each outcome occupies a certain amount of area within the sample space. That is, the area is distributed among the outcomes according to the probability distribution function! The larger the area, the more likely the outcome is.

<table>
<thead>
<tr>
<th>It rains</th>
<th>It doesn’t rain</th>
</tr>
</thead>
</table>

In this example, we have that each outcome occupies the same amount of area in the box—each is equally likely. Because we have 2 outcomes, we have that the probability of each outcome is \(\frac{1}{2}\).
Let’s take a look at another way we could divide up the area of the box among the outcomes.

<table>
<thead>
<tr>
<th>It rains</th>
<th>It doesn’t rain</th>
</tr>
</thead>
</table>

Here, the probability of it raining is $\frac{3}{4}$, so this outcome takes up $\frac{3}{4}$ of the area within the box. The remaining amount of area is $\frac{1}{4}$, which becomes the probability that it doesn’t rain.

**Task 6**

a. If we have $n$ outcomes in $S$, and Pr assigns each outcome an equal amount of area within our box, what is the probability of a particular outcome?

   **Note:** Such a division of the space is called a **uniform distribution**!

   $\frac{1}{n}$

b. Consider $S = \{\text{It’s sunny, It’s raining}\}$, where the probability distribution is 0.8 and 0.2, respectively. Under what constraints on the world is this sample space reasonable?

   If the world is only sunny or raining, then the sample space is fine. But, in the real world, we can have cloudy weather and snowy weather, too. A sample space should be **exhaustive** and also **mutually exclusive**, that is, exactly one of the outcomes has to happen each time we do the experiment.

c. Is the following probability distribution valid? Experiment: flipping a biased coin. $S = \{H, T\}$, $\Pr(H) = 1/3$, $\Pr(T) = 1/3$.

   No, because the probability of all outcomes must add up to 1.
The Relationship Between Counting and Probability

Questions about probability are often closely tied to questions about counting. Often, we need to count two things—the set of outcomes in our event, and the set of total possible outcomes. In a uniform distribution, the probability of getting an event $E$ is simply $\Pr(E) = |E|/|S|$.

Task 7

a. Suppose $S$ is the set of all binary strings of length $n$, and $\Pr$ is a uniform distribution. What is the probability of getting a string with $k$ ones (where $0 \leq k \leq n$)?

There are $\binom{n}{k}$ strings with $k$ ones, and $2^n$ total strings, so the answer is $\binom{n}{k}/2^n$.

b. For what value(s) of $k$ is the probability of getting a string with $k$ ones the largest? Try it out for some values and see if you find a pattern.

When is $\binom{n}{k}$ largest? When $k$ is closest to $\frac{n}{2}$

c. Explain how we can use $n$-ary (not just binary) strings to help us with other problems that involve, say, flipping a fair coin $m$ times, or rolling a die $m$ times.

We can form bijections to count things! For example, let 0 denote tail, head denote 1. Then, there is a bijection between the possible binary strings and the possible outcomes of $m$ coin flips. If we were using dice instead, though, we can use a senary (6 valued) string.

Conditional Probability and Independence

We sometimes want to know what the probability of something is, given that we know an outcome from certain subset of outcomes has happened (that is, no outcome outside that subset can happen).

Prof. Lewis has 2 coins: one fair, and one double heads. He picks one uniformly at random (that is, each coin has probability of $1/2$ of being picked), but he doesn’t tell us which one he picks. Prof. Lewis then flips the coin he picks, and he then shouts out the result.

Suppose Prof. Lewis shouts out “Heads.” What is the probability he flipped the fair coin, given that we know the coin flip resulted in heads ($H$)?

*Hint*: How many ways can the coin flip result in heads, and how many of them start with the fair coin?
We can generalize our work here. Given two events \( A, B \subseteq S \) (the sample space) where \( \Pr(B) > 0 \), we define the conditional probability of \( A \) given \( B \) as

\[
\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)}.
\]

We know that the only possible outcomes are those in \( B \) (since \( B \) is supposed to have happened). We therefore make \( \Pr(B) \) our denominator to renormalize our universe.

Looking at this formula, we also get a general definition for \( \Pr(A \cap B) \):

\[
\Pr(A \cap B) = \Pr(A) \Pr(B \mid A) = \Pr(B) \Pr(A \mid B)
\]

This is a derivation of Bayes' Theorem, and it will be your friend in the probability unit.

There are certain special situations where \( \Pr(B \mid A) = \Pr(B) \); that is, where the fact that \( A \) happened does not affect the probability of \( B \) happening. We have a name for this situation.

**Definition:** Two events \( A, B \subseteq S \) are (pairwise) independent if

\[
\Pr(A \mid B) = \Pr(A)
\]

If \( \Pr(B) = 0 \), \( B \) and any other event are independent.

Equivalently, \( A \) and \( B \) are independent if

\[
\Pr(A \cap B) = \Pr(A) \Pr(B).
\]

Note that these two definitions are equivalent—try to convince yourself by substituting the definition of conditional probability!

**Task 8**

a. If two events \( A \) and \( B \) have an empty intersection, what is the probability of \( A \) AND \( B \)?

\[
0
\]

b. For each of the following pairs of events \( A \) and \( B \), identify whether they are independent, and justify why or why not.

i. Suppose we roll a fair die, and suppose \( A \) = rolling an even number, and \( B \) = rolling a number greater than three.
Not independent: \( \Pr(A) = \frac{1}{2}, \Pr(B) = \frac{1}{2} \). \( A \cap B = \{4, 6\} \), so \( \Pr(A \cap B) = \frac{1}{3} \), but \( \frac{1}{2} \times \frac{1}{2} = \frac{1}{4} \).

ii. Optional: Suppose we flip a fair coin three times, and suppose \( A = \) the last coin is a tails, and \( B = \) there is a run of exactly two tails (that is, two, but not three, tails are flipped in a row).

\[ \begin{align*}
\text{Independent: } & \Pr(A) = \frac{1}{2}, \text{ and } B = \{TTH, HTT\} \text{ so } \Pr(B) = \frac{2}{8} = \frac{1}{4}. \\
& A \cap B = \{HTT\} \text{ so } \Pr(A \cap B) = \frac{1}{8} \text{ which is } \frac{1}{2} \times \frac{1}{4}.
\end{align*} \]

c. Optional: If two events \( A \) and \( B \) are \textit{mutually exclusive}, are they \textit{independent}? You can assume \( \Pr(A) \) and \( \Pr(B) \) are nonzero.

\[ \begin{align*}
\text{No. By definition, } & \Pr(A \cap B) = 0, \text{ so if the probability of each individual event occurring is nonzero, then } \Pr(A \cap B) \neq \Pr(A) \Pr(B).
\end{align*} \]

Checkoff — call over a TA!