CSCI-4116
Assignment 5

Anas Alhadi

B00895875

February 24, 2025

Question 1

Let $a = 15$ and $b = 18$, so $gcd(15, 18) = 3$.

Now $\varphi(15 \times 18) = \varphi(270)$:

$$\begin{aligned}
\varphi(270) &= 270 \times \prod_{p|270}(1 - \tfrac{1}{p}) \qquad \text{where } p \in \mathbb{P} \\
&= 270 \times (1 - \tfrac{1}{2}) \times (1 - \tfrac{1}{3}) \times (1 - \tfrac{1}{5}) \\
&= 270 \times \tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{4}{5} \\
&= 72
\end{aligned}$$

While $\varphi(15) \times \varphi(18)$

$$\begin{aligned}
\varphi(15) &= 15 \times \tfrac{2}{3} \times \tfrac{3}{5} \\
&= 8
\end{aligned}$$

$$\begin{aligned}
\varphi(18) &= 18 \times \tfrac{1}{2} \times \tfrac{2}{3} \\
&= 6
\end{aligned}$$

And $72 \neq 48$

Question 2

$$\begin{aligned}
S &= \{HH, HT, TH, TT\} \\
p(HH) &= \tfrac{1}{4} \\
p(HT) &= \tfrac{1}{4} \\
p(TH) &= \tfrac{1}{4} \\
p(TT) &= \tfrac{1}{4}
\end{aligned}$$

The event of flipping at least 1 tail, is the subset $e = \{HT, TH, TT\}$. Which is equivelent to the event of not getting 2 Heads. So $e = S \setminus \{HH\}$

$$\begin{aligned}
p(e) &= p(S) - p(HH) \\
&= 1 - \tfrac{1}{4} \\
&= \tfrac{3}{4}
\end{aligned}$$

Question 3

Let $R = \{1, 2, 3, 4, 5, 6\}$. Then the sample space of rolling 2 dice is $S = R^2$.

The question describes 2 events in S:

$$\begin{aligned}
e_1 &= \{(a, b) \in S, \text{where } a \neq b\} \\
e_2 &= \{(a, b) \in S, \text{where } 2|(a + b)\}
\end{aligned}$$

And asks for the probability that e_1 occurs given e_2. So $p(e_1|e_2)$, which is equivelent to the probability of event e_1 occuring when the sample space is restricted to the set e_2

Now observe that e_2 is the event in which a and b have the same parity. Thus:

$$\begin{aligned}
e_2 = \{&(1, 1), (1, 3), (1, 5), \\
&(2, 2), (2, 4), (2, 6), \\
&(3, 1), (3, 3), (3, 5), \\
&(4, 2), (4, 4), (4, 6), \\
&(5, 1), (5, 3), (5, 5), \\
&(6, 2), (6, 4), (6, 6)\}
\end{aligned}$$

We know that S follows a uniform distribution, so the probabilty of each elementary event is $\frac{1}{|S|}$. Since e_2 is a subset of S this means that the elements in e_2 are also uniformally distributed, that is the probability of each elementary event in e_2 is $\frac{1}{|e_2|}$

Finally, the probablity of $a \neq b$ in e_2 is equal to $1-$ (probability that $a = b$).

So:

$$\begin{aligned}
p(e_1|e_2) &= 1 - \tfrac{6}{|e_2|} \\
&= 1 - \tfrac{6}{18} \\
&= \tfrac{2}{3}
\end{aligned}$$

Question 4

Part a)

We know that the probability q of no two people having the same birthday is:

$q \quad \leq \quad exp(-\frac{k(k-1)}{2n})$

The probability p of two people having the same birthday is then $p = 1 - q$. In our case we solve for $p \geq 0.9$ and $n = 365$

So:

$$q \leq exp(\frac{-k^2 + k}{720}) \leq 0.1$$

$$ln(0.1) \geq \frac{-k^2 + k}{720}$$

Rearranging the inequality:

$$k^2 - k + 720(ln(0.1)) \geq 0$$

Solving for k:

$$k = \frac{1 \pm \sqrt{1 - 4 \times (720 \times ln(0.1))}}{2}$$

Giving the value: $k = 41.2199...$
Since we cant have fractional values of k we have it that $k = 42$

So the number of people needed, k, such that the probability of at least 2 having the same birthday is $p \geq \frac{9}{10}$ is $k \geq 42$

Part B)

Since the PIN cannot start with 0 we have it that there are 9×10^3 possible 4 digit combinations. So $n = 9 \times 10^3$.

And we want the probability of at least 2 people having the same PIN to be, $p \geq 0.5$ (so $q \leq 0.5$).

We now repeat the same steps in part A). So:

$$q \leq exp(\frac{-k^2 + k}{18 \times 10^3}) \leq 0.5$$

$$ln(0.5) \geq \frac{-k^2 + k}{18 \times 10^3}$$

Rearranging:

$$k^2 - k + ln(0.5) \times 18 \times 10^3 \geq 0$$

Solving for k:

$$k = \frac{1 \pm \sqrt{1 - 4(ln(0.5) \times 18 \times 10^3)}}{2}$$

Giving the value: $k = 112.2...$
So there must be $k \geq 113$ people to have the probability of at least 2 sharing the same PIN be $p \geq 0.5$

Question 5

First we define the cryptosystem:

$$\begin{aligned} \mathcal{P} &= \mathbb{Z}_{26} \\ \mathcal{C} &= \mathbb{Z}_{26} \\ \mathcal{K} &= \mathbb{Z}_{26} \end{aligned}$$

Using the definition of perfect secrecy

$$p(w|c) = p(w), \quad w \in \mathcal{P} \text{ and } c \in \mathcal{C}$$

Then by Bayes Theorem:

$$p(w|c) = \frac{p(w)p(c|w)}{p(c)}$$

Observe that:

1. Only one key in the Key space has a $p(k) > 0$, which is $k = 3$
2. We know that the

   $$p(c) = \sum p(w) \times p(k_{w,c}) \quad \forall w \in \mathcal{P}, \text{ and } k_{w,c} = \{k \in \mathcal{K} \mid E_k(w) \mapsto c\}$$

   Then since there is only one key, we have it that the probability of the ciphertext being c is equal to the probability $p(w_c)$ where $E_k(w_c) = c$
3. $p(c|w)$ asks for the probability that the encryption of the plaintext w results in c, so the probability that $E_k(w) \mapsto c$. Given that there is only one key, we know that w will either always be mapped to c or never, so $p(c|w) = 1$ or 0

It follows then that:

$$p(w|c) = \frac{p(w_c) \times 1}{p(w_c)} \quad OR \quad \frac{p(w) \times 0}{p(w_c)}$$
$$p(w|c) = 1 \quad OR \quad 0$$

Thus we do not have perfect secrecy.

Using Shannon's Theorem

Shannon's Theorem requires that $\mathcal{K}$ follows a uniform distribution. Notice however that in caesar cipher only one key has a non-zero probability. So keys are not uniformly distributed, violating the requiement. Thus the cryptosystem does not have perfect secrecy