Caesar Cipher

Keyspace $\mathcal{K}$: $\{0, 1, \ldots, 25\}$
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Caesar Cipher

Keyspace $\mathcal{K}$: $\{0, 1, \ldots, 25\}$
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.

Caesar Cipher

Keyspace $\mathcal{K}$: $\{0, 1, \ldots, 25\}$
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
$\mathrm{Enc}(k, m_1 m_2 \cdots m_\ell)$: $c_i = k + m_i \mod 26$

Caesar Cipher

Keyspace $\mathcal{K}$: $\{0, 1, \ldots, 25\}$
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
$\mathrm{Enc}(k, m_1 m_2 \cdots m_\ell)$: $c_i = k + m_i \mod 26$
$\mathrm{Dec}(k, c_1 c_2 \cdots c_\ell)$: $m_i = c_i - k \mod 26$

Caesar Cipher

Keyspace $\mathcal{K}$: $\{0, 1, \ldots, 25\}$
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
$\mathrm{Enc}(k, m_1 m_2 \cdots m_\ell)$: $c_i = k + m_i \mod 26$
$\mathrm{Dec}(k, c_1 c_2 \cdots c_\ell)$: $m_i = c_i - k \mod 26$

Example:
3 $\leftarrow$Gen
$\mathrm{Enc}(3, \text{“}DOG\text{”}) = \text{“}GRJ\text{”}$
$\mathrm{Enc}(3, \text{“}ZOO\text{”}) = \text{“}CRR\text{”}$

Caesar Cipher

Keyspace $\mathcal{K}$: $\{0, 1, \ldots, 25\}$
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
$\mathrm{Enc}(k, m_1 m_2 \cdots m_\ell)$: $c_i = k + m_i \mod 26$
$\mathrm{Dec}(k, c_1 c_2 \cdots c_\ell)$: $m_i = c_i - k \mod 26$

Suppose you see a ciphertext:
$c =$"FCJJMUMPJB"
Dec(0, c) = "FCJJMUMPJB".
Dec(1, c) = "EBIILTLOIA".
Dec(2, c) = "DAHHKSKNHZ".
⋮
Dec(24, c) = "HELLOWORLD"
Dec(25, c) = "GDKKNVNQKC"

Substitution Cipher

Keyspace $\mathcal{K}$: { Permutations on $\{0, \ldots, 25\}$ }
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.

Substitution Cipher

Keyspace $\mathcal{K}$: { Permutations on $\{0, \ldots, 25\}$ }
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
Enc$(k, m_1 m_2 \cdots m_\ell)$: $c_i = \pi(m_i)$

Substitution Cipher

Keyspace $\mathcal{K}$: { Permutations on $\{0, \ldots, 25\}$ }
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
$\mathrm{Enc}(k, m_1 m_2 \cdots m_\ell)$: $c_i = \pi(m_i)$
$\mathrm{Dec}(k, c_1 c_2 \cdots c_\ell)$: $m_i = \pi^{-1}(c_i)$

Substitution Cipher

Keyspace $\mathcal{K}$: { Permutations on $\{0, \ldots, 25\}$ }
Message space $\mathcal{M}$: $\{0, 1, \ldots, 25\}^*$
Ciphertext space $\mathcal{C}$: $\{0, 1, \ldots, 25\}^*$
(Note $\{0, \ldots, 25\}$ is in 1-1 correspondence with $\{A, \ldots, Z\}$)

Gen: Sample $k \leftarrow \mathcal{K}$.
Enc$(k, m_1 m_2 \cdots m_\ell)$: $c_i = \pi(m_i)$
Dec$(k, c_1 c_2 \cdots c_\ell)$: $m_i = \pi^{-1}(c_i)$

Example:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	C	E	P	S	I	M	K	Q	V	R	O	D	Z	N	F	B	L	T	W	J	A	Y	X	U	H

$= k \leftarrow$Gen

Enc$(k,$ "DOG" $) =$ "PNM"
Enc$(k,$ "ZOO" $) =$ "HNN"
Enc$(k,$ "BEE" $) =$ "CSS"

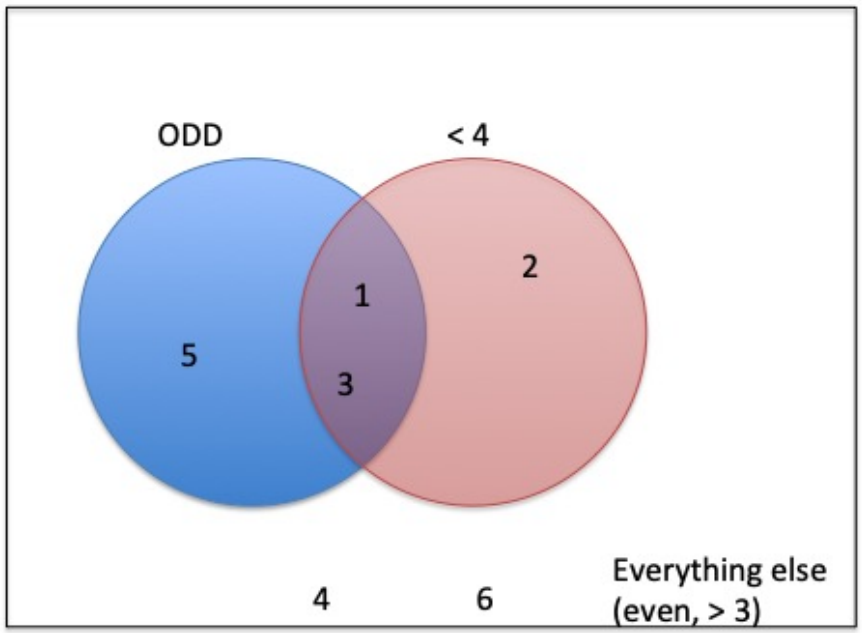
Probability Theory (refresher)

Let E_1 and E_2 be events that might be the result of some randomized process.
$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$.

Probability Theory (refresher)

Let E_1 and E_2 be events that might be the result of some randomized process.
$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$.

Example:

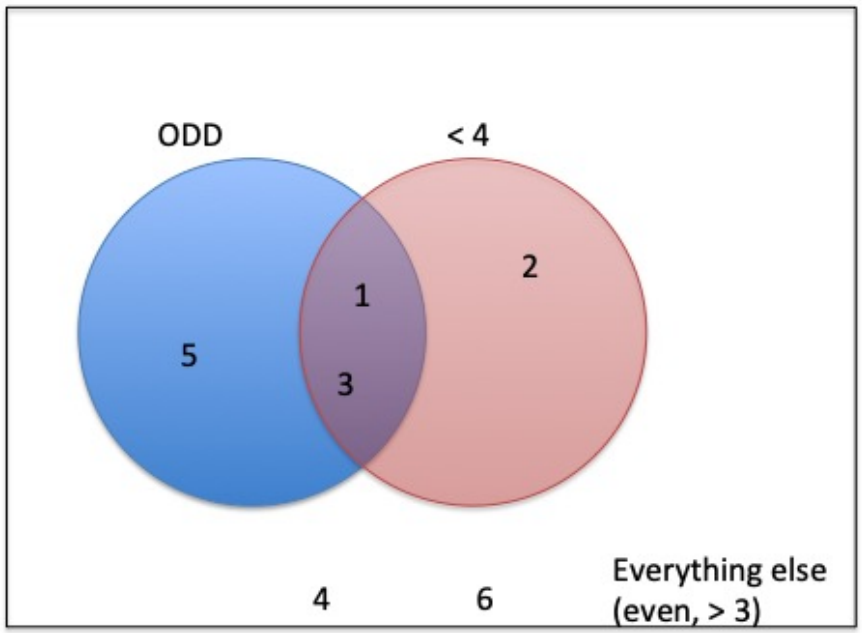


E_1 is the event that the roll of a die comes up odd.
E_2 is the event that the roll of a dies comes < 4.

Probability Theory (refresher)

Let E_1 and E_2 be events that might be the result of some randomized process.
$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$.

Example:



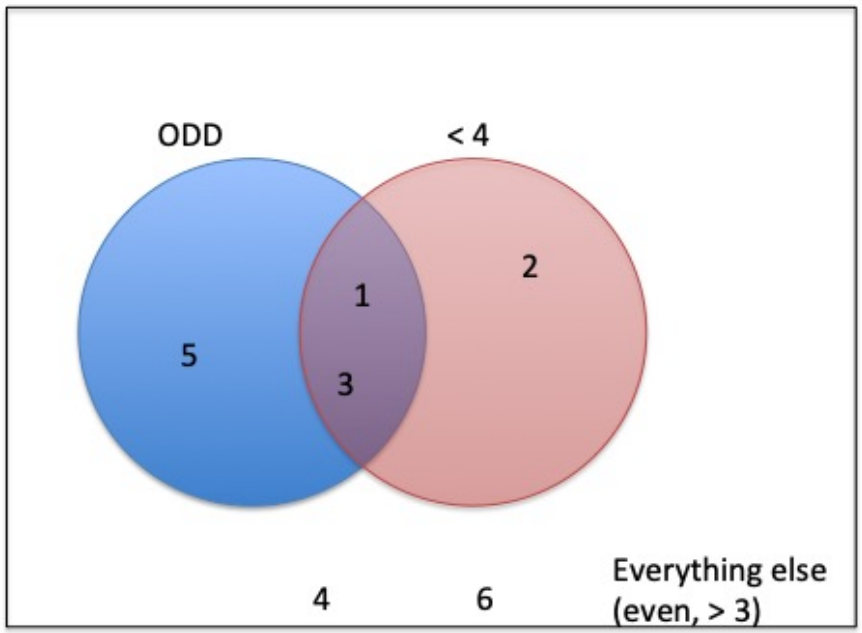
E_1 is the event that the roll of a die comes up odd.
E_2 is the event that the roll of a dies comes < 4.

$\Pr[E_1 \mid E_2]$:
Given that the value is in the pink circle, what is the probability that it is *also* in the blue circle?

Probability Theory (refresher)

Let E_1 and E_2 be events that might be the result of some randomized process.
$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$.

Example:



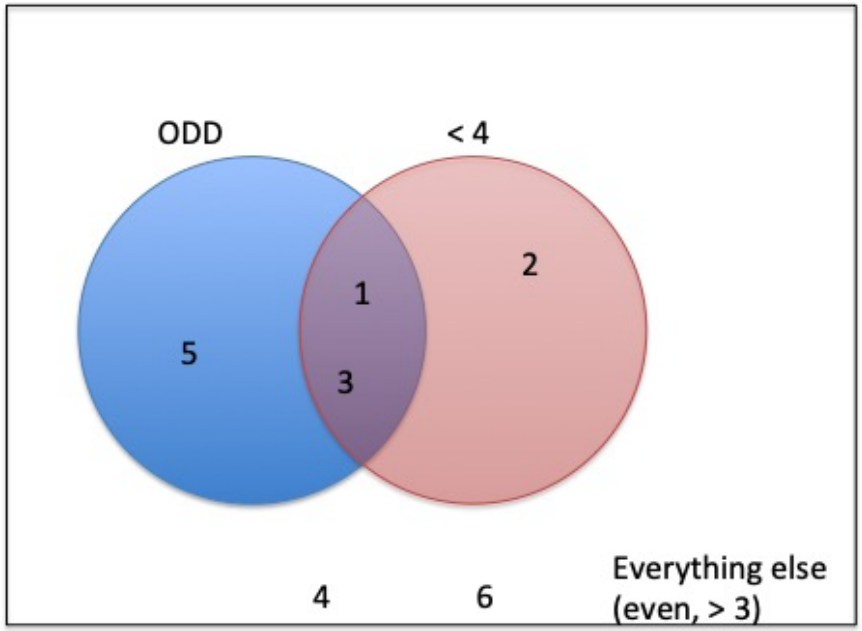
E_1 is the event that the roll of a die comes up odd.
E_2 is the event that the roll of a dies comes < 4.

$\Pr[E_1 \mid E_2]$:
Given that the value is in the pink circle, what is the probability that it is *also* in the blue circle?
What fraction of the pink circle overlaps with the blue?

Probability Theory (refresher)

Let E_1 and E_2 be events that might be the result of some randomized process.
$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$.

Example:



E_1 is the event that the roll of a die comes up odd.
E_2 is the event that the roll of a dies comes < 4.

$\Pr[E_1 \mid E_2]$:
Given that the value is in the pink circle, what is the probability that it is *also* in the blue circle?
What fraction of the pink circle overlaps with the blue?
$\frac{2}{6}$ of the outcomes are in the intersection, and $\frac{3}{6}$ of the outcomes are in the pink circle.

Probability Theory (refresher)

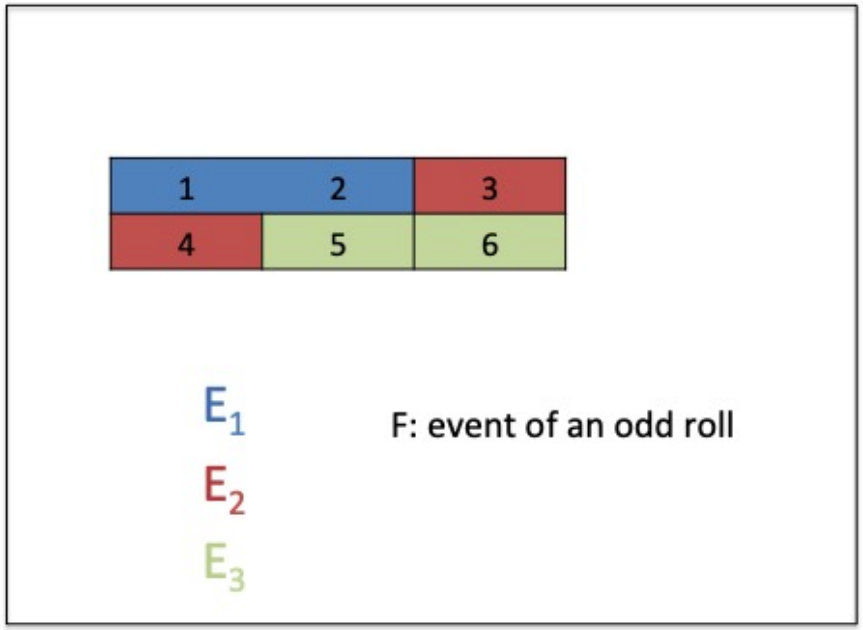
Let E_1 and E_2 be events that might be the result of some randomized process.
$\Pr[E_1 \mid E_2] = \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$.

Bayes's Theorem:

$$\Pr[E_1 \mid E_2] \Pr[E_2] = \Pr[E_1 \wedge E_2] = \Pr[E_2 \mid E_1] \Pr[E_1]$$

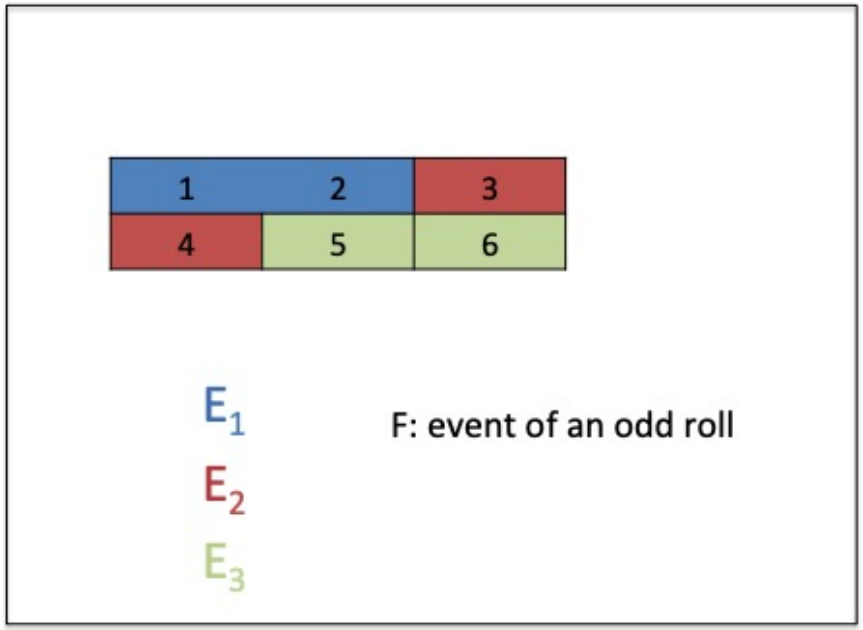
$$\Rightarrow \Pr[E_1 \mid E_2] = \frac{\Pr[E_2 \mid E_1] \Pr[E_1]}{\Pr[E_2]}$$

Probability Theory (refresher)



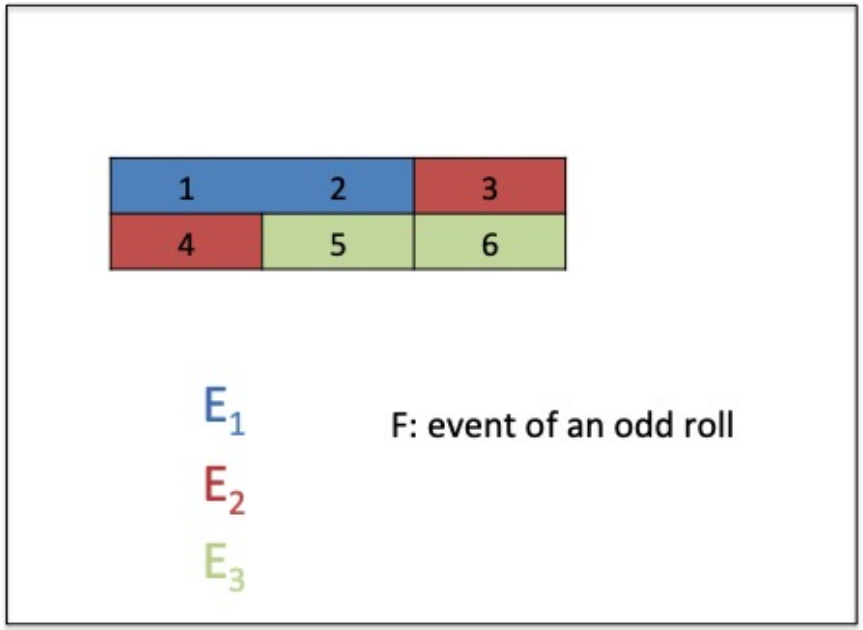
Let E_i be independent events that sum to 1.

Probability Theory (refresher)



Let E_i be independent events that sum to 1.
Formally: $\forall i, j : \Pr[E_i \wedge E_j] = 0$ and $\sum_i \Pr[E_i] = 1$

Probability Theory (refresher)

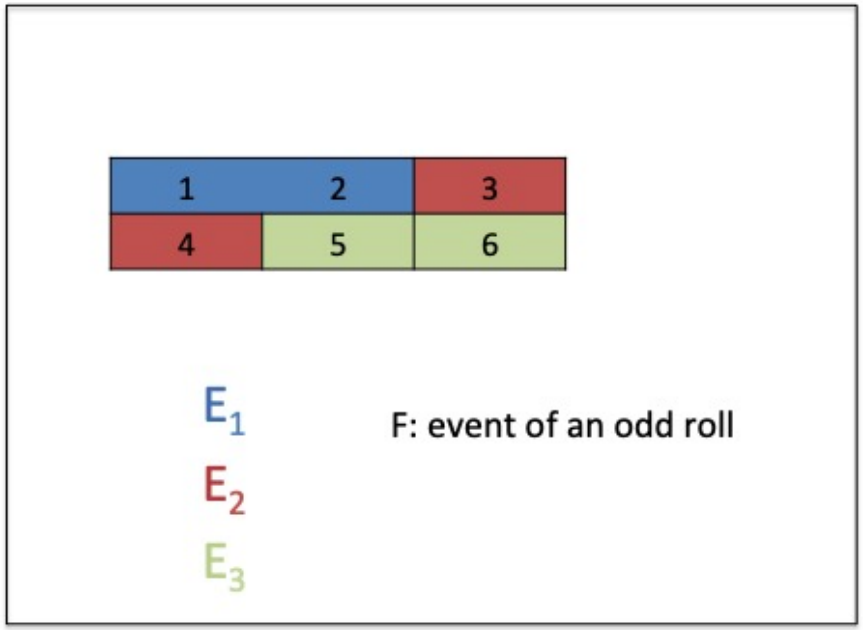


Let E_i be independent events that sum to 1.
Formally: $\forall i, j : \Pr[E_i \wedge E_j] = 0$ and $\sum_i \Pr[E_i] = 1$

For any event F,

$$\Pr[F] = \sum_i \Pr[E_i \wedge F]$$

Probability Theory (refresher)



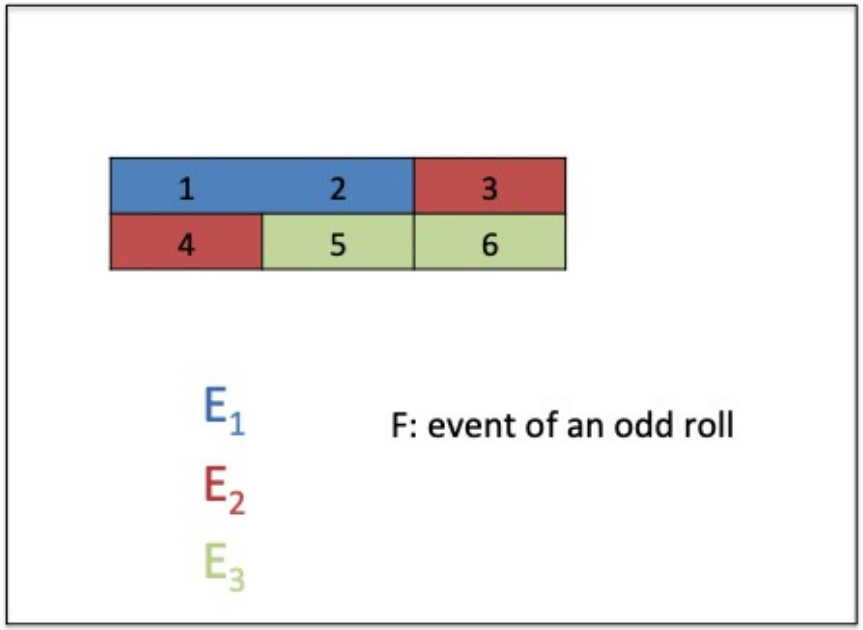
Let E_i be independent events that sum to 1.
Formally: $\forall i, j : \Pr[E_i \wedge E_j] = 0$ and $\sum_i \Pr[E_i] = 1$

For any event F,

$$\Pr[F] = \sum_i \Pr[E_i \wedge F]$$

$$= \sum_i \Pr[F \mid E_i] \Pr[E_i]$$

Probability Theory (refresher)



Let E_i be independent events that sum to 1.
Formally: $\forall i, j : \Pr[E_i \wedge E_j] = 0$ and $\sum_i \Pr[E_i] = 1$

For any event F,

$$\begin{aligned}\Pr[F] &= \sum_i \Pr[E_i \wedge F] \\ &= \sum_i \Pr[F \mid E_i] \Pr[E_i] \\ &= \frac{1}{6} + \frac{1}{6} + \frac{1}{6}\end{aligned}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$\Pr[m = \text{“}DOG\text{”}] = ???$
$\Pr[m = \text{“}DOG\text{”} \mid c = \text{“}RFF\text{”}] = ???$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$\Pr[m = \text{“}DOG\text{”}] = \frac{1}{3}$

$\Pr[m = \text{“}DOG\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c=\text{“}RFF\text{”} \mid m=\text{“}DOG\text{”}] \Pr[m=\text{“}DOG\text{”}]}{\Pr[c=\text{“}RFF\text{”}]} = 0$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$\Pr[m = \text{“}DOG\text{”}] = \frac{1}{3}$
$\Pr[m = \text{“}DOG\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c=\text{“}RFF\text{”} \mid m=\text{“}DOG\text{”}] \Pr[m=\text{“}DOG\text{”}]}{\Pr[c=\text{“}RFF\text{”}]} = 0$

This follows because $\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}DOG\text{”}] = 0$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$\Pr[m = \text{“}DOG\text{”}] = \frac{1}{3}$
$\Pr[m = \text{“}DOG\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c=\text{“}RFF\text{”} \mid m=\text{“}DOG\text{”}] \Pr[m=\text{“}DOG\text{”}]}{\Pr[c=\text{“}RFF\text{”}]} = 0$

This follows because $\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}DOG\text{”}] = 0$

The ciphertext c reveals something about the plaintext!

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] = \ ???$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

$$= \frac{\Pr[k \text{ maps “}Z\text{” to “}R\text{” and “}O\text{” to “}F\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

$$= \frac{\Pr[k \text{ maps “}Z\text{” to “}R\text{” and “}O\text{” to “}F\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

$$= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] = \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

$$= \frac{\Pr[k \text{ maps “}Z\text{” to “}R\text{” and “}O\text{” to “}F\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

$$= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]}$$

$$= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3}}{\Pr[c = \text{“}RFF\text{”}]}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\begin{aligned}
\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] &= \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\Pr[k \text{ maps “}Z\text{” to “}R\text{” and “}O\text{” to “}F\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3}}{\Pr[c = \text{“}RFF\text{”}]}
\end{aligned}$$

$$\begin{aligned}
\Pr[c = \text{“}RFF\text{”}] = \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}DOG\text{”}] \Pr[m = \text{“}DOG\text{”}] \\
+ \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}] \\
+ \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}BEE\text{”}] \Pr[m = \text{“}BEE\text{”}]
\end{aligned}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\begin{aligned}
\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] &= \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\Pr[k \text{ maps “}Z\text{” to “}R\text{” and “}O\text{” to “}F\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3}}{\Pr[c = \text{“}RFF\text{”}]}
\end{aligned}$$

$$\begin{aligned}
\Pr[c = \text{“}RFF\text{”}] &= \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}DOG\text{”}] \Pr[m = \text{“}DOG\text{”}] \\
&\quad + \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}] \\
&\quad + \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}BEE\text{”}] \Pr[m = \text{“}BEE\text{”}] \\
&= (0 \cdot \frac{1}{3}) + (\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3}) + (\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3})
\end{aligned}$$

Insecurity of Substitution Cipher

Consider the following random experiment:

Choose $k \leftarrow \text{Gen}$
Choose $m \leftarrow \{\text{“}DOG\text{”}, \text{“}ZOO\text{”}, \text{“}BEE\text{”}\}$, uniformly at random
$c = \text{Enc}(k, m)$

$Pr[m = \text{“}ZOO\text{”}] = \frac{1}{3}$

$$\begin{aligned}
\Pr[m = \text{“}ZOO\text{”} \mid c = \text{“}RFF\text{”}] &= \frac{\Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\Pr[k \text{ maps “}Z\text{” to “}R\text{” and “}O\text{” to “}F\text{”}] \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \Pr[m = \text{“}ZOO\text{”}]}{\Pr[c = \text{“}RFF\text{”}]} \\
&= \frac{\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3}}{\Pr[c = \text{“}RFF\text{”}]} = \frac{1}{2}
\end{aligned}$$

$$\begin{aligned}
\Pr[c = \text{“}RFF\text{”}] &= \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}DOG\text{”}] \Pr[m = \text{“}DOG\text{”}] \\
&\quad + \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}ZOO\text{”}] \Pr[m = \text{“}ZOO\text{”}] \\
&\quad + \Pr[c = \text{“}RFF\text{”} \mid m = \text{“}BEE\text{”}] \Pr[m = \text{“}BEE\text{”}] \\
&= (0 \cdot \frac{1}{3}) + (\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3}) + (\frac{1}{26} \cdot \frac{1}{25} \cdot \frac{1}{3})
\end{aligned}$$

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

$$\Pr[m = \text{“ann”} \mid c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}] \frac{\Pr[m = \text{“ann”}]}{\Pr[c = \text{“DQQ”}]}$$

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

$$\Pr[m = \text{“ann”} \mid c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}] \frac{\Pr[m = \text{“ann”}]}{\Pr[c = \text{“DQQ”}]}$$
$$= \Pr_{k \leftarrow \mathcal{K}}[k = 3] \left(\frac{.2}{\Pr[c = \text{“DQQ”}]} \right)$$

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

$$\Pr[m = \text{“ann”} \mid c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}] \frac{\Pr[m = \text{“ann”}]}{\Pr[c = \text{“DQQ”}]}$$
$$= \Pr_{k \leftarrow \mathcal{K}}[k = 3] \left(\frac{.2}{\Pr[c = \text{“DQQ”}]} \right)$$

$$\Pr[c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“kim”}].5$$
$$+ \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}].2$$
$$+ \Pr[c = \text{“DQQ”} \mid m = \text{“boo”}].3$$

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

$$\Pr[m = \text{“ann”} \mid c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}] \frac{\Pr[m = \text{“ann”}]}{\Pr[c = \text{“DQQ”}]}$$
$$= \Pr_{k \leftarrow \mathcal{K}}[k = 3] \left(\frac{.2}{\Pr[c = \text{“DQQ”}]} \right)$$

$$\Pr[c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“kim”}].5$$
$$+ \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}].2$$
$$+ \Pr[c = \text{“DQQ”} \mid m = \text{“boo”}].3$$
$$= 0 + \frac{1}{26}.2 + \frac{1}{26}.3 = \frac{1}{26}.5$$

Insecurity of Caesar cipher

Consider the following message distribution, $\mathcal{M}$:

$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“kim”}] = .5$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“ann”}] = .2$$
$$\Pr_{m \leftarrow \mathcal{M}}[m = \text{“boo”}] = .3$$

Suppose the adversary sees ciphertext $c =$ “DQQ”.

$$\Pr[m = \text{“ann”} \mid c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}] \frac{\Pr[m = \text{“ann”}]}{\Pr[c = \text{“DQQ”}]}$$
$$= \Pr_{k \leftarrow \mathcal{K}}[k = 3] \left(\frac{.2}{\Pr[c = \text{“DQQ”}]} \right)$$
$$= \frac{1}{26} \left(\frac{.2}{\frac{1}{26}.5} \right) = .4 > .2$$

$$\Pr[c = \text{“DQQ”}] = \Pr[c = \text{“DQQ”} \mid m = \text{“kim”}].5$$
$$+ \Pr[c = \text{“DQQ”} \mid m = \text{“ann”}].2$$
$$+ \Pr[c = \text{“DQQ”} \mid m = \text{“boo”}].3$$
$$= 0 + \frac{1}{26}.2 + \frac{1}{26}.3 = \frac{1}{26}.5$$