Chapter 2: Perfect Secrecy, Product Cryptosystems

Math 495, Fall 2008

Hope College

September 15 and 17, 2008

Levels of Security

- **Computational Security:** Breaking the cryptosystem requires N operations, where N is some specified very large number.
- **Provable Security:** It can be proven that breaking the cryptosystem requires solving some other problem in mathematics, which is believed to be difficult.
- **Unconditional Security:** The cryptosystem cannot be broken, even with unlimited computational resources.

Probability

- A discrete random variable (RV) $\mathbf{X}$ consists of a finite set X with a probability distribution defined on X. The probability that $\mathbf{X}$ takes on a value $x \in X$ is written $\Pr[\mathbf{X} = x]$ or $\Pr[x]$. We must have
  - $\Pr[x] \geq 0$ for all $x \in X$.
  - $\sum_{x \in X} \Pr[x] = 1$.
- A subset $E \subseteq X$ is called an **event**, and

$$\Pr[\mathbf{X} \in E] = \sum_{x \in E} \Pr[x].$$

- If $\Pr[x]$ is the same for all $x \in X$, then we say $\mathbf{X}$ has **equally likely outcomes**, and for all x,

$$\Pr[x] = \frac{1}{|X|}.$$

Examples of Probability

- A 6-sided die is called 'fair' if the six faces are equally likely to appear. Let $\mathbf{X}$ be the outcome of one roll of a fair die, and let E be the event "the roll is 3 or lower."
- In this case, $X = \{1, 2, 3, 4, 5, 6\}$, and for each $x \in X$,

$$\Pr[x] = \frac{1}{6}.$$

- We have

$$\Pr[\mathbf{X} \in E] = \sum_{x=1}^{3} \Pr[x] = \sum_{x=1}^{3} \frac{1}{6} = \frac{3}{6} = \frac{1}{2}.$$

- Note that, in the case of equally likely outcomes, for any event $E \subseteq X$, we have

$$\Pr[\mathbf{X} \in E] = \frac{|E|}{|X|}.$$

The quantity $\Pr[\mathbf{X} \in E]$ is sometimes written as $\Pr[E]$.

Examples of Probability

- Two fair 6-sided dice are rolled, and **Z** denotes the sum of the numbers appearing. We have outcome set

$$\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

  but these outcomes are not equally likely.
- Instead, we consider outcomes as (equally likely) ordered pairs (a, b), where $1 \leq a, b \leq 6$. That is,

$$Z = \{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\},$$

  with each pair (a, b) having probability $1/36$.
- Now, for example,

$$\Pr[\mathbf{Z} = 5] = \Pr[\{(1, 4), (2, 3), (3, 2), (4, 1)\}] = \frac{4}{36} = \frac{1}{9}.$$

Joint and Conditional Probability

- If **X** and **Y** are two RVs defined on sets X and Y, we define the **joint probability** $\Pr[x, y]$ to be the probability that $\mathbf{X} = x$ and $\mathbf{Y} = y$.
- We define the **conditional probability** $\Pr[x|y]$ to be the probability that $\mathbf{X} = x$ given that we know $\mathbf{Y} = y$. The quantity $\Pr[y|x]$ is defined similarly.
- Joint and conditional probabilities are related by the formula

$$\Pr[x, y] = \Pr[x|y]\Pr[y] \qquad \text{for all } x \in X, y \in Y.$$

- The RVs **X** and **Y** are said to be **independent** if $\Pr[x, y] = \Pr[x]\Pr[y]$ for all $x \in X$ and $y \in Y$, (or, equivalently, $\Pr[x|y] = \Pr[x]$ for all $x \in X$ and $y \in Y$).

Examples of Joint Probability

- A fair 6-sided red die and blue die are rolled. Let **X** be the number on the red die and **Y** the number on the blue die. Then, for example,

$$\Pr[\mathbf{X} = 5, \mathbf{Y} = 4] = \Pr[\{(5, 4)\}] = \frac{1}{36},$$

and

$$\Pr[\mathbf{X} = 5]\Pr[\mathbf{Y} = 4] = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}.$$

- The same is true for any outcomes x of **X** and y of **Y**, and therefore **X** and **Y** are independent.
- We can also say that

$$\Pr[\mathbf{X} = 5 \mid \mathbf{Y} = 4] = \frac{1}{6} = \Pr[\mathbf{X} = 5],$$

since the number on the blue die will not affect the roll of the red die.

Examples of Joint Probability

- Suppose we roll a fair red die and a fair blue die and $\mathbf{X}$ is the number showing on the red die, but $\mathbf{Z}$ is the sum of the dice.
- Notice that

$$\Pr[\mathbf{X} = 4, \mathbf{Z} = 5] = \Pr[\mathbf{Z} = 5 \,|\, \mathbf{X} = 4]\Pr[\mathbf{X} = 4] = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36},$$

  and

$$\Pr[\mathbf{X} = 4]\Pr[\mathbf{Z} = 5] = \frac{1}{6} \cdot \frac{1}{9} = \frac{1}{54}.$$

  Therefore, $\mathbf{X}$ and $\mathbf{Z}$ are not independent.
- How could we compute a ‘reverse’ conditional probability, such as

$$\Pr[\mathbf{X} = 4 \,|\, \mathbf{Z} = 5]\,?$$

Examples of Joint Probability

- With **X** and **Z** as in the previous slide, we compute $\Pr[\mathbf{X} = 4 \mid \mathbf{Z} = 5]$. We could do this directly: if we know $\mathbf{Z} = 5$, that restricts our outcomes (x, y) to

$$\{(1,4),(2,3),(3,2),(4,1)\}.$$

  Since $\mathbf{X} = 4$ in only one of these, $\Pr[\mathbf{X} = 4 \mid \mathbf{Z} = 5] = 1/4$.
- Instead, we could use

$$\Pr[x|z]\Pr[z] = \Pr[x,z] = \Pr[z|x]\Pr[x]$$

  and solve for $\Pr[x|z]$.
- This results in **Bayes' Theorem**: If $\Pr[z] > 0$, then

$$\Pr[x|z] = \frac{\Pr[z|x]\Pr[x]}{\Pr[z]}.$$

Conditioning

- Using the notation of the previous examples, let **W** be the difference of the two dice. Suppose we want to find the probability of the event $E =$ "**W** is a multiple of 4". One way to do this would be to look at all 36 ordered pairs and decide how many have differences that are multiples of 4.
- Another method, which is used liberally in the book, is to condition on some other variable (in this case, **X**).

$$\begin{aligned}
\Pr[E] &= \sum_{x=1}^{6} \Pr[E, \mathbf{X} = x] = \sum_{x=1}^{6} \Pr[E \mid \mathbf{X} = x]\Pr[\mathbf{X} = x] \\
&= \frac{2}{6}\cdot\frac{1}{6} + \frac{2}{6}\cdot\frac{1}{6} + \frac{1}{6}\cdot\frac{1}{6} + \frac{1}{6}\cdot\frac{1}{6} + \frac{2}{6}\cdot\frac{1}{6} + \frac{2}{6}\cdot\frac{1}{6} \\
&= \frac{10}{36} = \frac{5}{18}.
\end{aligned}$$

Perfect Secrecy

- A cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ has **perfect secrecy** if $\Pr[x|y] = \Pr[x]$ for all $x \in \mathcal{P}$ and $y \in \mathcal{C}$.
- For all $y \in \mathcal{C}$, assuming **K** and **X** are independent,

$$\Pr[\mathbf{Y} = y] = \sum_{\{K \,:\, y \in e_K(\mathcal{P})\}} \Pr[\mathbf{K} = K]\Pr[\mathbf{X} = d_K(y)].$$

- For all $y \in \mathcal{C}$ and $x \in \mathcal{P}$,

$$\Pr[\mathbf{Y} = y \,|\, \mathbf{X} = x] = \sum_{\{K \,:\, x = d_K(y)\}} \Pr[\mathbf{K} = K].$$

- If the preceding quantities are known, we can compute $\Pr[x|y]$ by Bayes' formula and compare to $\Pr[x]$.

An Example

- Suppose $\mathcal{P} = \{a, b, c, d\}$, $\mathcal{C} = \{A, B, C, D\}$, and $\mathcal{K} = \{K_1, K_2, K_3\}$ with encryptions as defined below:

	a	b	c	d
K_1	D	C	B	A
K_2	B	C	D	A
K_3	B	A	D	C

  Suppose that the probabilities on the plaintexts $\{a, b, c, d\}$ are $\{2/5, 1/5, 1/5, 1/5\}$, respectively, and that the key probabilities on $\{K_1, K_2, K_3\}$ are $\{1/4, 1/4, 1/2\}$.
- Find $\Pr[y|x]$ for every $y \in \mathcal{C}$ and $x \in \mathcal{P}$.