Answers to Exercise 1

1. Which of the following statements is true?
   - $3 \in Y$: This is not true, as 3 is not an element of the set Y.
   - $8 \notin X$: This is not true, as 8 is an element of the set Y.
   - $5 \in Z$: This is true, as 5 is a prime number smaller than 20.
   - $X \subseteq Y$: This is not true, none of the elements of X exist in Y.
2. Compute the following sets:
   - $X \cup Y = \{1, 3, 8\} \cup \{0, 4, 7\} = \{0, 1, 3, 4, 7, 8\}$
   - $X \cap Z = \{3\}$
3. Convince yourself that the following laws hold:
   - We can easily show $\emptyset \cap A = \emptyset$ by using the definition of $\_ \cap \_$ and the fact that $\forall x. \neg x \in \emptyset$ (i.e., $x \in \emptyset = \bot$ where $\bot$ represents logical falsehood):
$$\begin{aligned} \emptyset \cap A \quad &= \{x \mid x \in \emptyset \ \wedge x \in A\} \\ &= \{x \mid \bot \wedge x \in A\} \\ &= \{x \mid \bot\} \\ &= \emptyset \end{aligned}$$
   - We can easily show $A \cup B = B \cup A$ by using the definition of $\_ \cup \_$ and the commutativity of $\_ \vee \_$:
$$\begin{aligned} A \cup B \quad &= \{x \mid x \in A \ \vee x \in B\} \\ &= \{x \mid x \in A \ \vee x \in B\} \\ &= B \cup A \end{aligned}$$
   - We can easily show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ by using the definition of the set operations and the distributivity of the logical connectives:
$$\begin{aligned} A \cap (B \cup C) \quad &= \{x \mid x \in A \ \wedge x \in B \cup C\} \\ &= \{x \mid x \in A \ \wedge x\{y|y \in B \vee y \in C\}\} \\ &= \{x \mid x \in A \ \wedge (x \in B \vee x \in C)\} \\ &= \{x \mid (x \in A \wedge x \in B) \vee (\ x \in A \wedge x \in C)\} \\ &= \{x \mid (x \in A \wedge x \in B\} \cup \{x \in A \wedge x \in C)\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$

Answers to Exercise 2

1. $\mathbf{1} = 10 \bmod 3: 3 \cdot 3 + 1 = 10$
2. $\mathbf{0} = 6 \bmod 2: 3 \cdot 2 + 0 = 6$
3. $2 = 7 \bmod \mathbf{5}: 1 \cdot 5 + 2 = 7$
4. $1 = 5 \bmod \mathbf{4}: 1 \cdot 4 + 1 = 5$
5. $5 = x \bmod 11: 0 \cdot 11 + 5 = 5$ (x can also be $16, 27, \ldots$ ($x = n \cdot 11 + 5$ where $n = 1, 2, \ldots$))
6. $x = (8 \bmod 7 + 9 \bmod 7) \bmod 7 = (1 \bmod 7 + 2 \bmod 7) \bmod 7 = 3 \bmod 7 = 3$
7. $\mathbf{3} = 17 \bmod 7: 2 \cdot 7 + 3 = 17$
8. $x = (8 \bmod 7 \cdot 9 \bmod 7) \bmod 7 = (1 \bmod 7 \cdot 2 \bmod 7) \bmod 7 = 2 \bmod 7 = 2$
9. $\mathbf{2} = 72 \bmod 7: 10 \cdot 7 + 2 = 72$

Answers to Exercise 3

1. We start with

$$8^{15} \bmod 13 = (8 \bmod 13) \cdot (8^7 \bmod 13) \cdot (8^7 \bmod 13) \bmod 13$$

Now we simplify ($8^7 \bmod 13$):

$$8^7 \bmod 13 = (8 \bmod 13) \cdot (8^3 \bmod 13) \cdot (8^3 \bmod 13) \bmod 13$$

and then ($8^3 \bmod 13$):

$$\begin{aligned} 8^3 \bmod 13 &= (8 \bmod 13) \cdot (8^2 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (12 \bmod 13) \bmod 13 \\ &= 96 \bmod 13 = 5 \bmod 13 \end{aligned}$$

Thus

$$\begin{aligned} 8^7 \bmod 13 &= (8 \bmod 13) \cdot (8^3 \bmod 13) \cdot (8^3 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (5 \bmod 13) \cdot (5 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (25 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (12 \bmod 13) \bmod 13 \\ &= 96 \bmod 13 = 5 \bmod 13 \end{aligned}$$

Finally

$$\begin{aligned} 8^{15} \bmod 13 &= (8 \bmod 13) \cdot (8^7 \bmod 13) \cdot (8^7 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (5 \bmod 13) \cdot (5 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (25 \bmod 13) \bmod 13 \\ &= (8 \bmod 13) \cdot (12 \bmod 13) \bmod 13 \\ &= 96 \bmod 13 = 5 \bmod 13 \end{aligned}$$

Note that the largest intermediate computation which can be calculated without a calculator was $96 \bmod 13$.

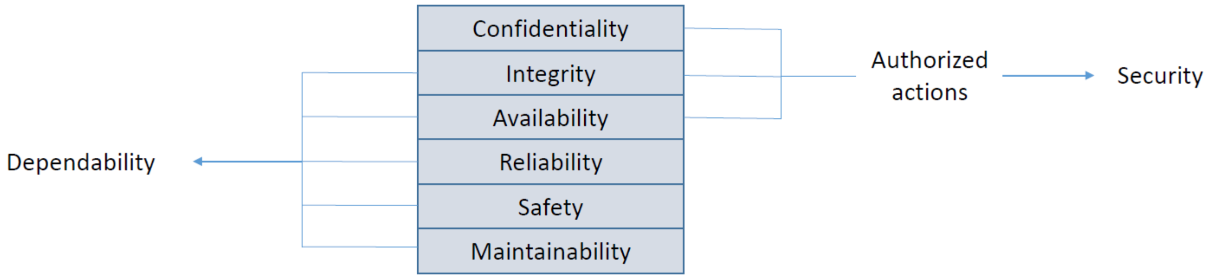
2. We can generalise the scheme used in the last exercise to define a fast exponentiation scheme:

$$b^e \bmod n = \begin{cases} b^{e/2} \cdot b^{e/2} \bmod n & \text{if } n \text{ is even} \\ b \cdot b^{(e-1)/2} \cdot b^{(e-1)/2} \bmod n & \text{if } n \text{ is odd} \end{cases}$$

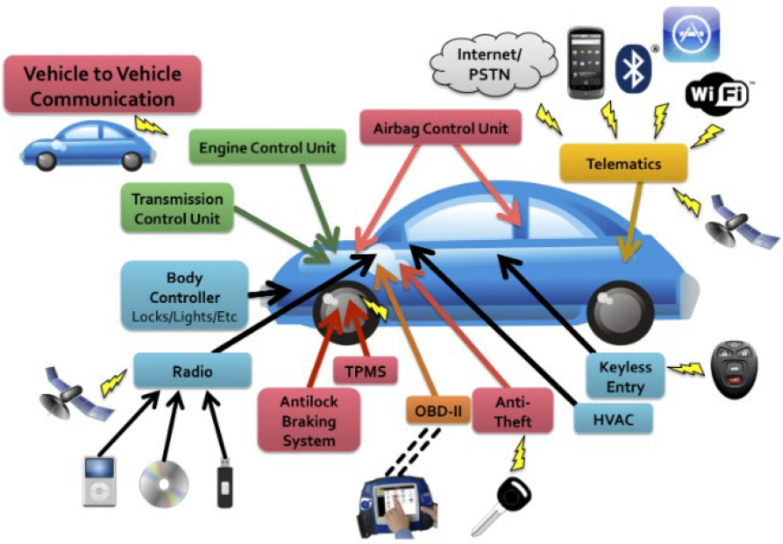
Applying this scheme recursively (exploiting that the same factors only need to be computed once) results in a scheme where the number of multiplications required only grows logarithmic (instead linear) in the size of the exponent.

Answers to Exercise 4

1. Functionality, Efficiency, Dependability, Security
2. Integrity, Availability, Reliability, Safety, Maintainability
3. Confidentiality



Answers to Exercise 5



*Source: Checkoway et al.; Comprehensive Experimental Analyses of Automotive Attack Surfaces; USENIX Security Conference; 2011.