4-2 Projectile Motion: Basic Equations

We now apply the independence of horizontal and vertical motions to projectiles. Just what do we mean by a projectile? Well, a **projectile** is an object that is thrown, kicked, batted, or otherwise launched into motion and then allowed to follow a path determined solely by the influence of gravity. As you might expect, this covers a wide variety of physical systems.

In studying projectile motion we make the following assumptions:

- Air resistance is ignored.
- The acceleration due to gravity is constant, downward, and has a magnitude equal to $g = 9.81\ \text{m/s}^2$.
- The Earth's rotation is ignored.

Air resistance can be significant if a projectile moves with relatively high speed or if it encounters a strong wind. In many everyday situations, however, like tossing a ball to a friend or dropping a book, air resistance is relatively insignificant. As for the acceleration due to gravity, $g = 9.81\ \text{m/s}^2$, this value varies slightly from place to place on the Earth's surface and decreases with increasing altitude. In addition, the rotation of the Earth can be significant when we consider projectiles that cover great distances. Little error is made in ignoring the variation of g or the rotation of the Earth, however, in the examples of projectile motion considered in this chapter.

Equations of Motion for Projectiles Let's incorporate the preceding assumptions into the equations of motion given in the previous section. Suppose, as in **FIGURE 4-2**, that the x axis is horizontal and the y axis is vertical, with the positive direction upward. Noting that downward is the negative direction, it follows that

$$a_y = -9.81\ \text{m/s}^2 = -g$$

Gravity causes no acceleration in the x direction. Thus, the x component of acceleration is zero:

$$a_x = 0$$

With these acceleration components substituted into the fundamental constant-acceleration equations of motion (Table 4-1) we find:

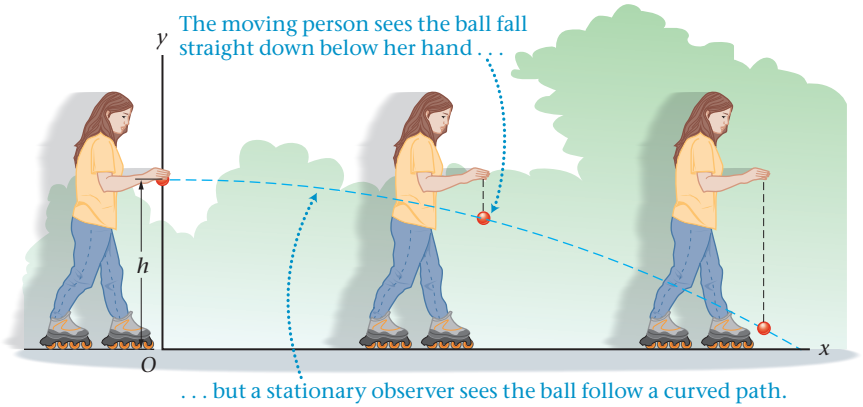
Projectile Motion ($a_x = 0$, $a_y = -g$)

$$x = x_0 + v_{0x}t \qquad v_x = v_{0x} \qquad v_x^2 = v_{0x}^2$$
$$y = y_0 + v_{0y}t - \tfrac{1}{2}gt^2 \qquad v_y = v_{0y} - gt \qquad v_y^2 = v_{0y}^2 - 2g\Delta y \qquad \text{4-6}$$

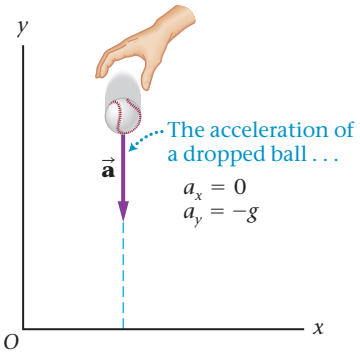
In these expressions, the positive y direction is upward and the quantity g is positive. *All* of our studies of projectile motion use Equations 4-6 as our fundamental equations—again, special cases simply correspond to substituting different specific values for the constants.

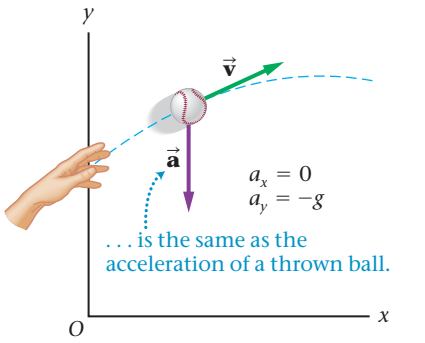
Demonstrating Independence of Motion A simple demonstration illustrates the independence of horizontal and vertical motions in projectile motion. First, while standing still, drop a rubber ball to the floor and catch it on the rebound. Notice that the ball goes straight down, lands near your feet, and returns almost to the level of your hand in about a second.

Next, walk—or roller skate—with constant speed before dropping the ball, then observe its motion carefully. To you, its motion looks the same as before: It goes straight down, lands near your feet, bounces straight back up, and returns in about one second. This is illustrated in **FIGURE 4-3**. The fact that you were moving in the horizontal direction the whole time had no effect on the ball's vertical motion—the motions are independent.



▲ **FIGURE 4-3 Independence of vertical and horizontal motions** When you drop a ball while walking, running, or skating with constant velocity, it appears to you to drop straight down from the point where you released it. To a person at rest, the ball follows a curved path that combines horizontal and vertical motions.





▲ **FIGURE 4-2 Acceleration in free fall** All objects in free fall have acceleration components $a_x = 0$ and $a_y = -g$ when the coordinate system is chosen as shown here. This is true regardless of whether the object is dropped, thrown, kicked, or otherwise set into motion.

Big Idea 2 Projectiles are objects that move under the influence of gravity alone. Projectiles can be dropped from rest or thrown at some angle to the horizontal. Once they are launched, they have all the characteristics of projectile motion, irrespective of how their motion started.

PHYSICS IN CONTEXT
Looking Ahead

The basic idea behind projectile motion is used again in Chapter 12, when we consider orbital motion.

PROBLEM-SOLVING NOTE

Acceleration of a Projectile

When the x axis is chosen to be horizontal and the y axis points vertically upward, it follows that the acceleration of an ideal projectile is $a_x = 0$ and $a_y = -g$.

(a)

(b)

(c)

▲ **FIGURE 4-4 Visualizing Concepts** **Independence of Motion** **(a)** An athlete jumps upward from a moving skateboard. The athlete retains his initial horizontal velocity, and hence remains directly above the skateboard at all times. **(b)** The pilot ejection seat of a jet fighter is being ground-tested. The horizontal and vertical motions are independent, and hence the test dummy is still almost directly above the cockpit from which it was ejected. (Notice that air resistance is beginning to reduce the dummy's horizontal velocity.) **(c)** This rollerblader may not be thinking about independence of motion, but the ball she released illustrates the concept perfectly as it falls directly below her hand.

To an observer who sees you walking by, the ball follows a curved path, as shown. The precise shape of this curved path—a parabola—is verified in the next section. Additional examples of this principle are shown in **FIGURE 4-4**.

Chapter 2

Encryption

Suppose Alice and Bob share a secret key k. Alice wants to transmit a message m to Bob over a network while maintaining the secrecy of m in the presence of an eavesdropping adversary. This chapter begins the development of basic techniques to solve this problem. Besides transmitting a message over a network, these same techniques allow Alice to store a file on a disk so that no one else with access to the disk can read the file, but Alice herself can read the file at a later time.

We should stress that while the techniques we develop in this chapter to solve this fundamental problem are important and interesting, they do not by themselves solve all problems related to "secure communication."

- The techniques only provide secrecy in the situation where Alice transmits a *single* message per key. If Alice wants to secretly transmit several messages using the *same* key, then she must use methods developed in Chapter 5.
- The techniques do not provide any assurances of *message integrity*: if the attacker has the ability to modify the bits of the ciphertext while it travels from Alice to Bob, then Bob may not realize that this happened, and accept a message other than the one that Alice sent. We will discuss techniques for providing message integrity in Chapter 6.
- The techniques do not provide a mechanism that allow Alice and Bob to come to share a secret key in the first place. Maybe they are able to do this using some secure network (or a physical, face-to-face meeting) at some point in time, while the message is sent at some later time when Alice and Bob must communicate over an insecure network. However, with an appropriate infrastructure in place, there are also protocols that allow Alice and Bob to exchange a secret key even over an insecure network: such protocols are discussed in Chapters 21 and 21.12.

2.1 Shannon ciphers and perfect security

2.1.1 Definition of a Shannon cipher

The basic mechanism for encrypting a message using a shared secret key is called a *cipher* (or *encryption scheme*). In this section, we introduce a slightly simplified notion of a cipher, which we call a **Shannon cipher**.

A **Shannon cipher** is a pair $\mathcal{E} = (E, D)$ of functions.

- The function E (the **encryption function**) takes as input a **key** k and a **message** m (also called a **plaintext**), and produces as output a **ciphertext** c. That is,

$$c = E(k, m),$$

  and we say that c is the **encryption of** m **under** k.

- The function D (the **decryption function**) takes as input a key k and a ciphertext c, and produces a message m. That is,

$$m = D(k, c),$$

  and we say that m is the **decryption of** c **under** k.

- We require that decryption "undoes" encryption; that is, the cipher must satisfy the following **correctness property**: for all keys k and all messages m, we have

$$D(k,\ E(k,\ m)\ ) = m.$$

To be slightly more formal, let us assume that $\mathcal{K}$ is the set of all keys (the **key space**), $\mathcal{M}$ is the set of all messages (the **message space**), and that $\mathcal{C}$ is the set of all ciphertexts (the **ciphertext space**). With this notation, we can write:

$$E : \mathcal{K} \times \mathcal{M} \to \mathcal{C},$$
$$D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}.$$

Also, we shall say that $\mathcal{E}$ is **defined over** $(\mathcal{K}, \mathcal{M}, \mathcal{C})$.

Suppose Alice and Bob want to use such a cipher so that Alice can send a message to Bob. The idea is that Alice and Bob must somehow agree in advance on a key $k \in \mathcal{K}$. Assuming this is done, then when Alice wants to send a message $m \in \mathcal{M}$ to Bob, she encrypts m under k, obtaining the ciphertext $c = E(k, m) \in \mathcal{C}$, and then sends c to Bob via some communication network. Upon receiving c, Bob decrypts c under k, and the correctness property ensures that $D(k, c)$ is the same as Alice's original message m. For this to work, we have to assume that c is not tampered with in transit from Alice to Bob. Of course, the goal, intuitively, is that an eavesdropper, who may obtain c while it is in transit, does not learn too much about Alice's message m — this intuitive notion is what the formal definition of security, which we explore below, will capture.

In practice, keys, messages, and ciphertexts are often sequences of bytes. Keys are usually of some fixed length; for example, 16-byte (i.e., 128-bit) keys are very common. Messages and ciphertexts may be sequences of bytes of some fixed length, or of variable length. For example, a message may be a 1GB video file, a 10MB music file, a 1KB email message, or even a single bit encoding a "yes" or "no" vote in an electronic election.

Keys, messages, and ciphertexts may also be other types of mathematical objects, such as integers, or tuples of integers (perhaps lying in some specified interval), or other, more sophisticated types of mathematical objects (polynomials, matrices, or group elements). Regardless of how fancy these mathematical objects are, in practice, they must at some point be represented as sequences of bytes for purposes of storage in, and transmission between, computers.

For simplicity, in our mathematical treatment of ciphers, we shall assume that $\mathcal{K}$, $\mathcal{M}$, and $\mathcal{C}$ are sets of *finite* size. While this simplifies the theory, it means that if a real-world system allows

messages of unbounded length, we will (somewhat artificially) impose a (large) upper bound on legal message lengths.

To exercise the above terminology, we take another look at some of the example ciphers discussed in Chapter 1.

Example 2.1. A **one-time pad** is a Shannon cipher $\mathcal{E} = (E, D)$, where the keys, messages, and ciphertexts are bit strings of the same length; that is, $\mathcal{E}$ is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where

$$\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0,1\}^L,$$

for some fixed parameter L. For a key $k \in \{0,1\}^L$ and a message $m \in \{0,1\}^L$ the encryption function is defined as follows:

$$E(k, m) := k \oplus m,$$

and for a key $k \in \{0,1\}^L$ and ciphertext $c \in \{0,1\}^L$, the decryption function is defined as follows:

$$D(k, c) := k \oplus c.$$

Here, "$\oplus$" denotes bit-wise exclusive-OR, or in other words, component-wise addition modulo 2, and satisfies the following algebraic laws: for all bit vectors $x, y, z \in \{0,1\}^L$, we have

$$x \oplus y = y \oplus x, \quad x \oplus (y \oplus z) = (x \oplus y) \oplus z, \quad x \oplus 0^L = x, \quad \text{and} \quad x \oplus x = 0^L.$$

These properties follow immediately from the corresponding properties for addition modulo 2. Using these properties, it is easy to check that the correctness property holds for $\mathcal{E}$: for all $k, m \in \{0,1\}^L$, we have

$$D(k,\ E(k,\ m)\ ) = D(k,\ k \oplus m) = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0^L \oplus m = m.$$

The encryption and decryption functions happen to be the same in this case, but of course, not all ciphers have this property. □

Example 2.2. A **variable length one-time pad** is a Shannon cipher $\mathcal{E} = (E, D)$, where the keys are bit strings of some fixed length L, while messages and ciphertexts are variable length bit strings, of length at most L. Thus, $\mathcal{E}$ is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where

$$\mathcal{K} := \{0,1\}^L \quad \text{and} \quad \mathcal{M} := \mathcal{C} := \{0,1\}^{\leq L}.$$

for some parameter L. Here, $\{0,1\}^{\leq L}$ denotes the set of all bit strings of length at most L (including the empty string). For a key $k \in \{0,1\}^L$ and a message $m \in \{0,1\}^{\leq L}$ of length ℓ, the encryption function is defined as follows:

$$E(k, m) := k[0\,..\,\ell - 1] \oplus m,$$

and for a key $k \in \{0,1\}^L$ and ciphertext $c \in \{0,1\}^{\leq L}$ of length ℓ, the decryption function is defined as follows:

$$D(k, c) := k[0\,..\,\ell - 1] \oplus c.$$

Here, $k[0\,..\,\ell - 1]$ denotes the truncation of k to its first ℓ bits. The reader may verify that the correctness property holds for $\mathcal{E}$. □