Chapter 15

Key Management

15-3   SYMMETRIC-KEY AGREEMENT

Alice and Bob can create a session key between themselves without using a KDC. This method of session-key creation is referred to as the symmetric-key agreement.
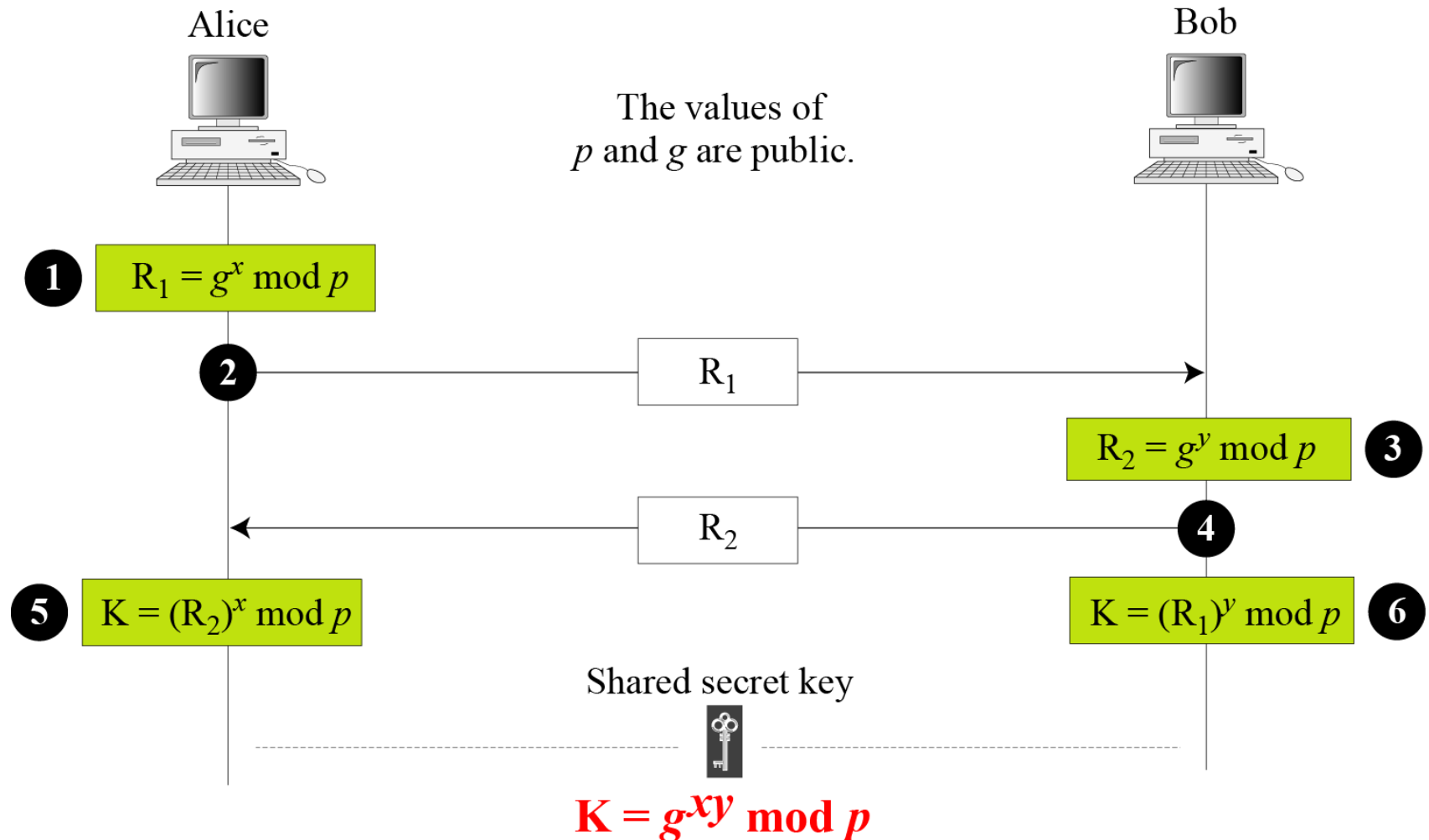
Topics discussed in this section:

15.3.1 Diffie-Hellman Key Agreement

Figure 15.9 *Diffie-Hellman method*

Alice   Bob

The values of
p and g are public.

1 $R_1 = g^x \bmod p$

2 R_1

3 $R_2 = g^y \bmod p$

4 R_2

5 $K = (R_2)^x \bmod p$

6 $K = (R_1)^y \bmod p$

Shared secret key

$$K = g^{xy} \bmod p$$

Note

The symmetric (shared) key in the Diffie-Hellman method is $K = g^{xy} \bmod p$.

15.3.1   Continued

Example 15.1

Let us give a trivial example to make the procedure clear. Our example uses small numbers, but note that in a real situation, the numbers are very large. Assume that $g = 7$ and $p = 23$. The steps are as follows:

1. Alice chooses $x = 3$ and calculates $R_1 = 7^3 \bmod 23 = 21$.
2. Bob chooses $y = 6$ and calculates $R_2 = 7^6 \bmod 23 = 4$.
3. Alice sends the number 21 to Bob.
4. Bob sends the number 4 to Alice.
5. Alice calculates the symmetric key $K = 4^3 \bmod 23 = 18$.
6. Bob calculates the symmetric key $K = 21^6 \bmod 23 = 18$.
7. The value of K is the same for both Alice and Bob; $g^{xy} \bmod p = 7^{18} \bmod 23 = 18$.

15.3.1 Continued

Example 15.2

Let us give a more realistic example. We used a program to create a random integer of 512 bits (the ideal is 1024 bits). The integer *p* is a 159-digit number. We also choose *g*, *x*, and *y* as shown below:

|	
p	764624298563493572182493765955030507476338096726949748923573772860925 235666660755423637423309661180033338106194730130950414738700999178043 6548785807987581
g	2
x	557
y	273

Example 15.2   *Continued*

The following shows the values of R₁, R₂, and K.

R_1	844920284205665505216172947491035094143433698520012660862863631067673 6199592808285867008021318592909451402175003199733129458360838219430659 66020157955354
R_2	435262838709200379470747114895581627636389116262115557975123379218566 3100114357182083900401818764868417538311653426916302634211067215085896 255201288594143
K	155638000664522290596225827523270765273218046944236785203204001464065 008879366512042574267766083279110171530386745612522131516109765842001 204086433617740

Figure 15.10 *Diffie-Hellman idea*
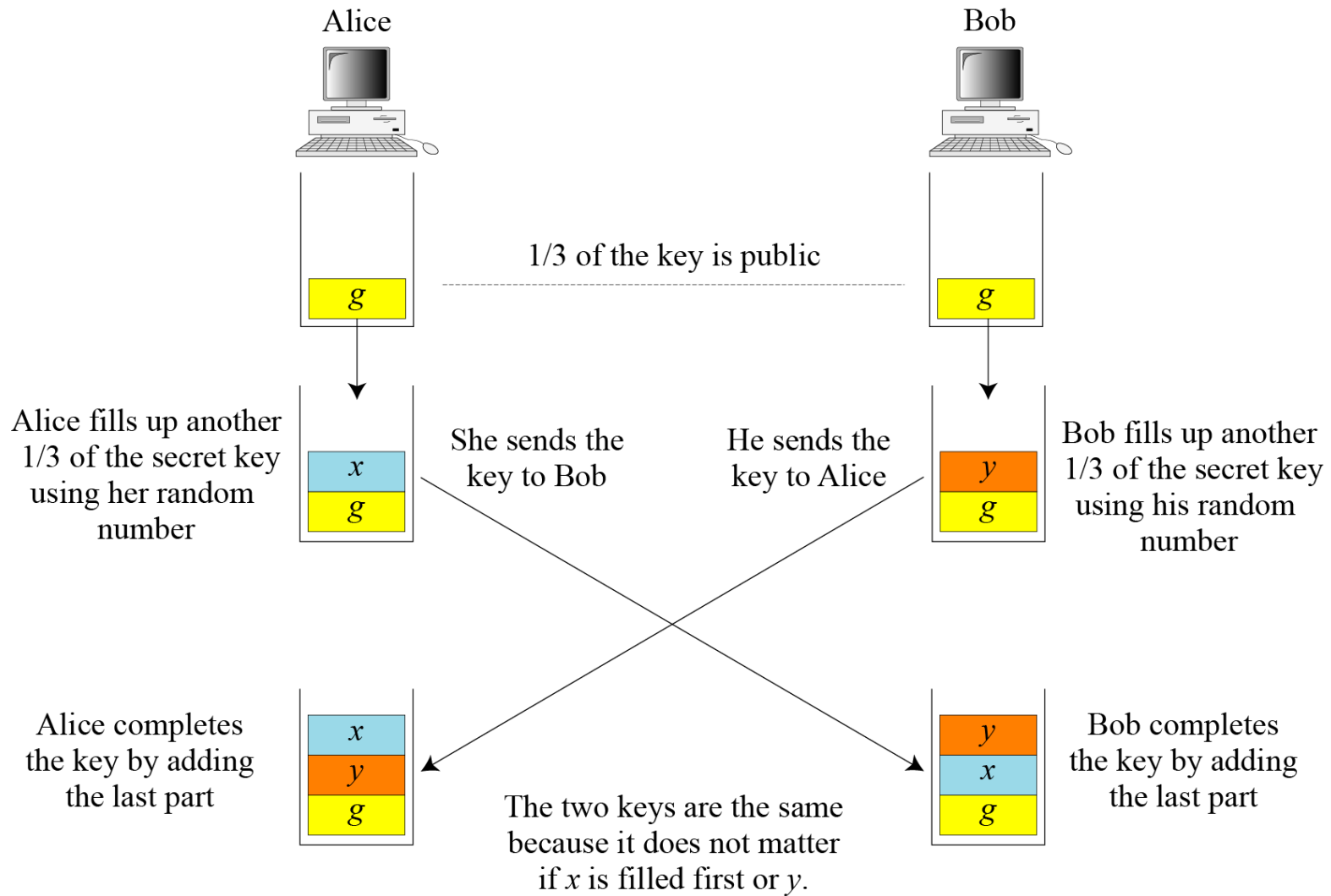
15.3.1 Continued

Security of Diffie-Hellman

> **Discrete Logarithm Attack**

> **Man-in-the-Middle Attack**

15.3.1 *Continued*

Figure 15.11 *Man-in-the-middle attack*

Alice　　　　　　　　　　Eve　　　　　　　　　　Bob

$R_1 = g^x \bmod p$

R_1

$R_2 = g^z \bmod p$

R_2

R_2

$R_3 = g^y \bmod p$

R_3

$K_1 = (R_2)^x \bmod p$

$K_1 = (R_1)^z \bmod p$
$K_2 = (R_3)^z \bmod p$

$K_2 = (R_2)^y \bmod p$

Alice-Eve Key　　　　　　Eve-Bob Key

$K_1 = g^{xz} \bmod p$　　　　　$K_2 = g^{zy} \bmod p$