Chapter 15

Diffie-Hellman

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.

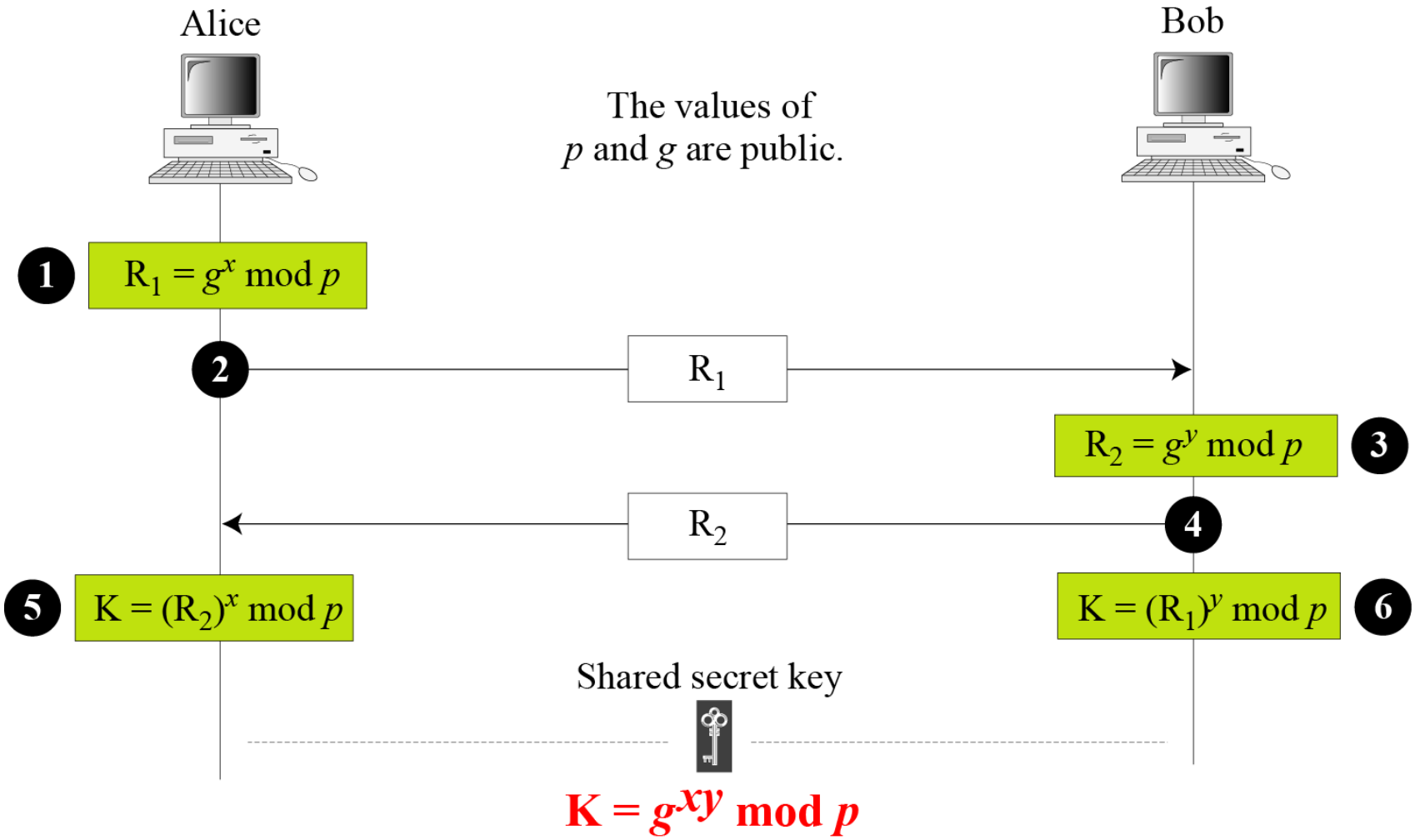
Topics discussed in this section:

15.3.1 Diffie-Hellman Key Agreement

15.3.2 Station-to-Station Key Agreement

15.3.1 Diffie-Hellman Key Agreement

Figure 15.9 *Diffie-Hellman method*



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 $R_1 = 73 \bmod 23 = 21$.**
2. **Bob chooses $y = 6$ and calculates $R_2 = 76 \bmod 23 = 4$.**
3. **Alice sends the number 21 to Bob.**
4. **Bob sends the number 4 to Alice.**
5. **Alice calculates the symmetric key $K = 43 \bmod 23 = 18$.**
6. **Bob calculates the symmetric key $K = 216 \bmod 23 = 18$.**
7. **The value of K is the same for both Alice and Bob; $g^{xy} \bmod p = 718 \bmod 35 = 18$.**

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	764624298563493572182493765955030507476338096726949748923573772860925235666660755423637423309661180033338106194730130950414738700999178043654878580798758 1
g	2
x	557
y	273

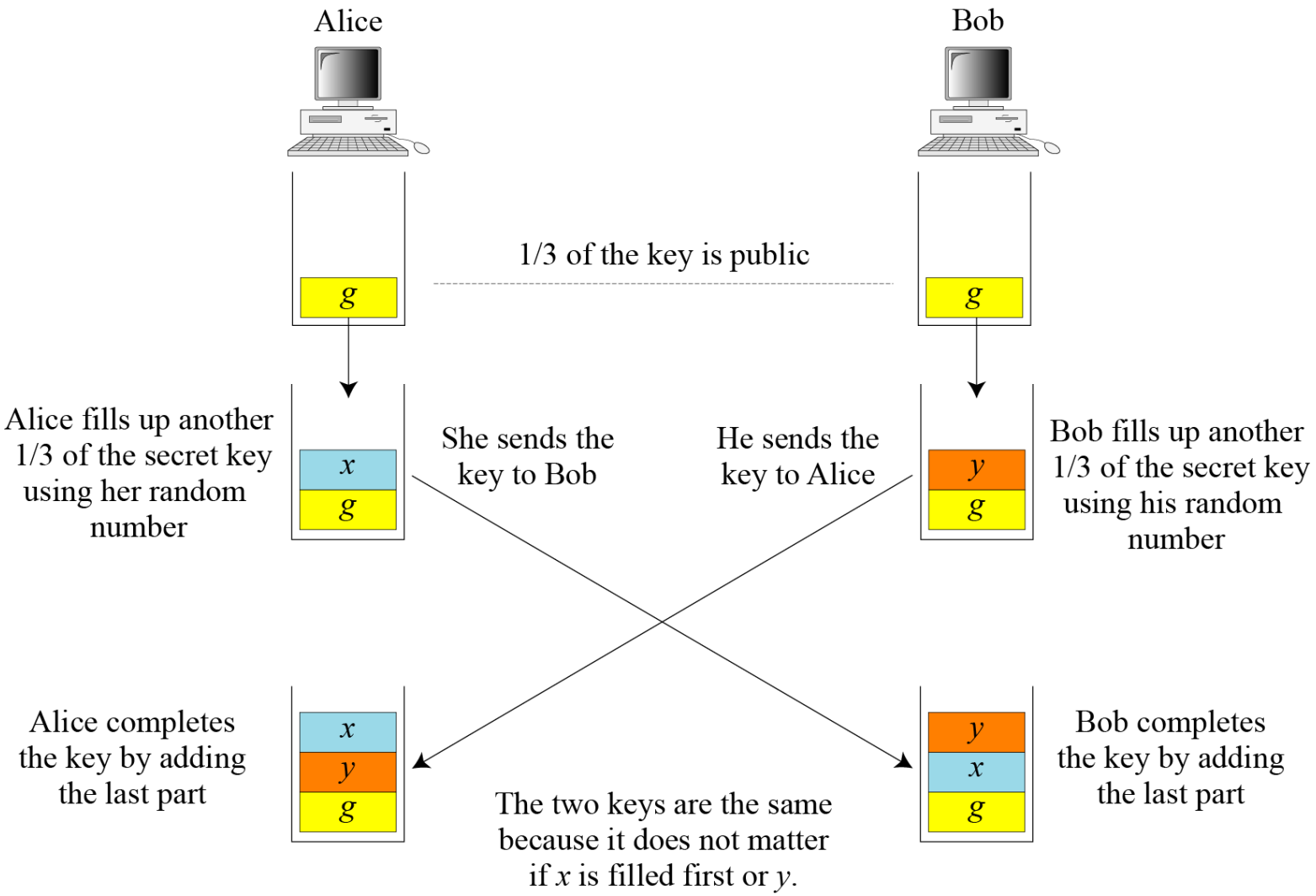
15.3.1 Continued

Example 15.2 *Continued*

The following shows the values of R_1, R_2, and K.

R_1	844920284205665505216172947491035094143433698520012660862863631067673619959280828586700802131859290945140217500319973312945836083821943065966020157955354
R_2	435262838709200379470747114895581627636389116262115557975123379218566310011435718208390040181876486841753831165342691630263421106721508589625520128859414 3
K	155638000664522290596225827523270765273218046944423678520320400146406500887936651204257426776608327911017153038674561252213151610976584200120408643361774 0

Figure 15.10 *Diffie-Hellman idea*



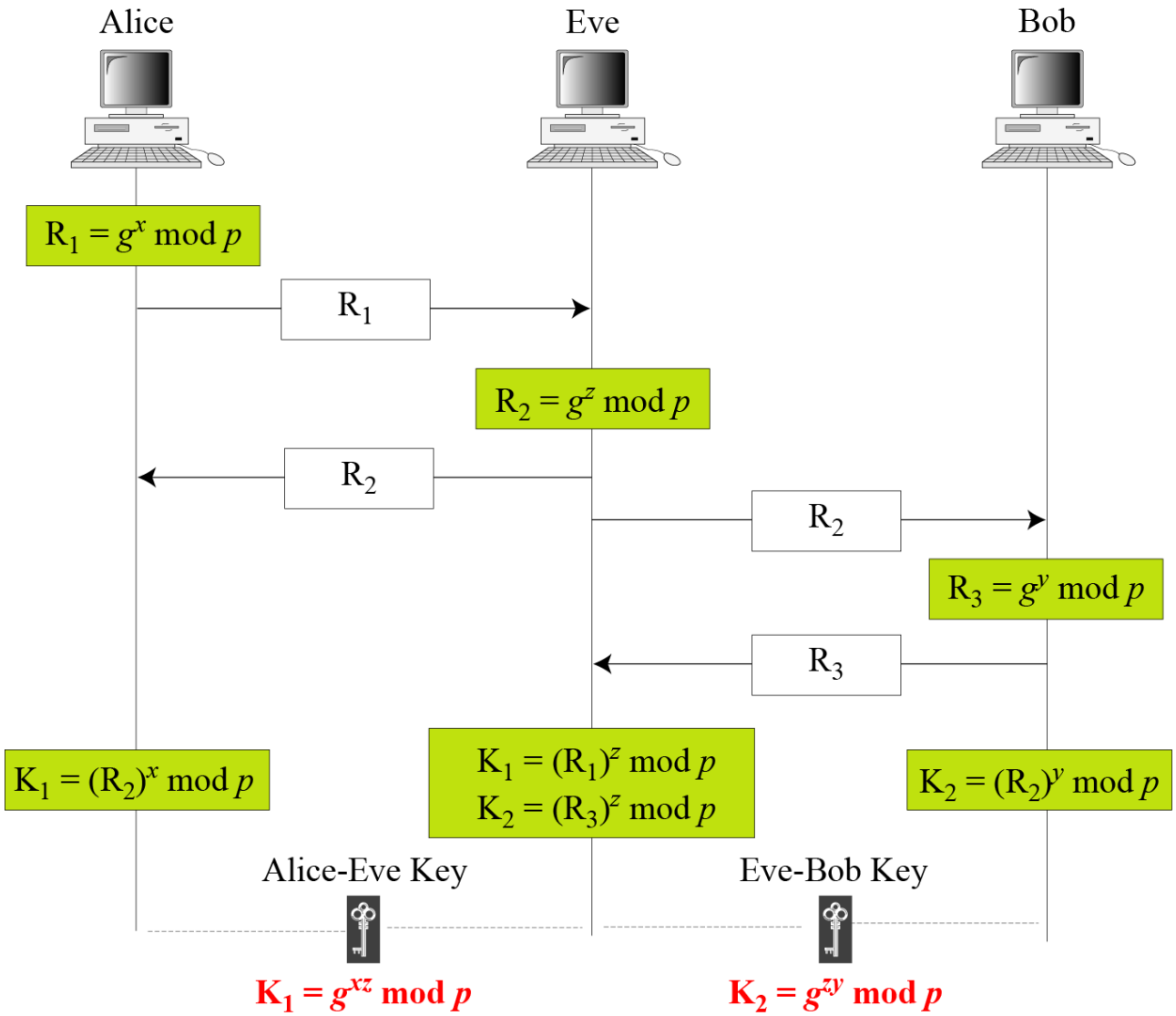
Security of Diffie-Hellman

Discrete Logarithm Attack

Man-in-the-Middle Attack

15.3.1 Continued

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



15.3.2 Station-to-Station Key Agreement

Figure 15.12 *Station-to-station key agreement method*