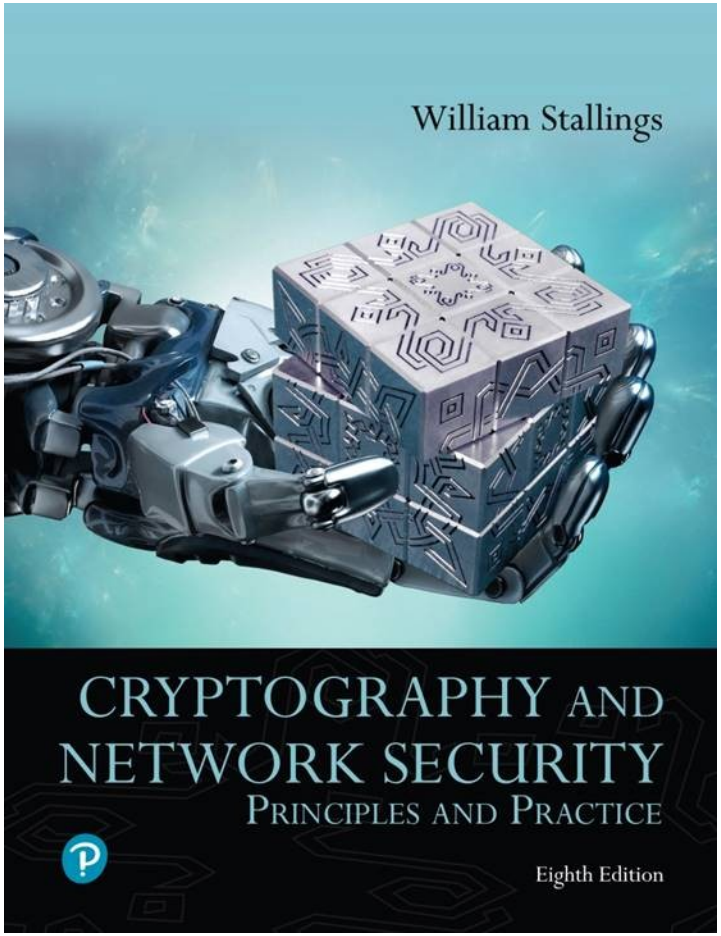
Cryptography and Network Security: Principles and Practice

Eighth Edition



Chapter 10

Other Public-Key Cryptosystems

Pearson

Diffie-Hellman Key Exchange

- First published public-key algorithm
- A number of commercial products employ this key exchange technique
- Purpose is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages
- The algorithm itself is limited to the exchange of secret values
- Its effectiveness depends on the difficulty of computing discrete logarithms

Figure 10.1 The Diffie–Hellman Key Exchange

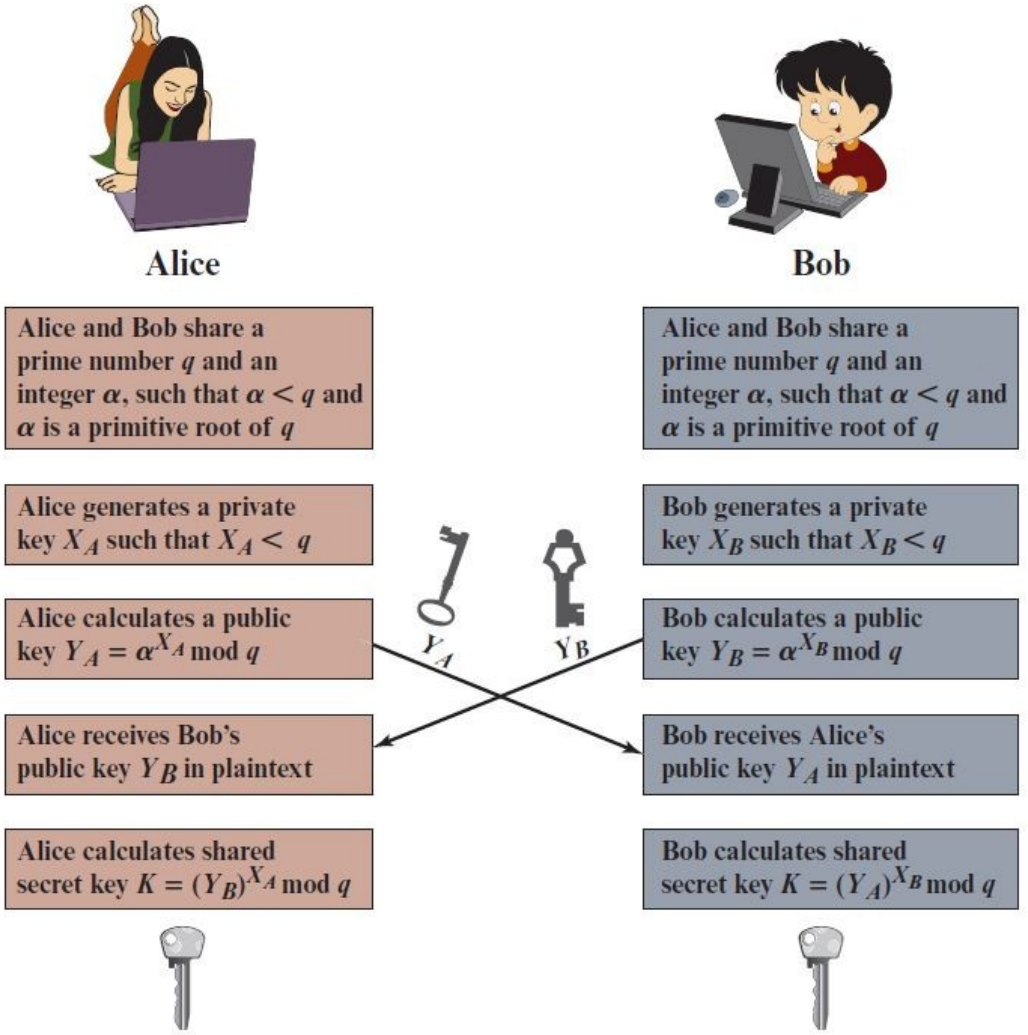
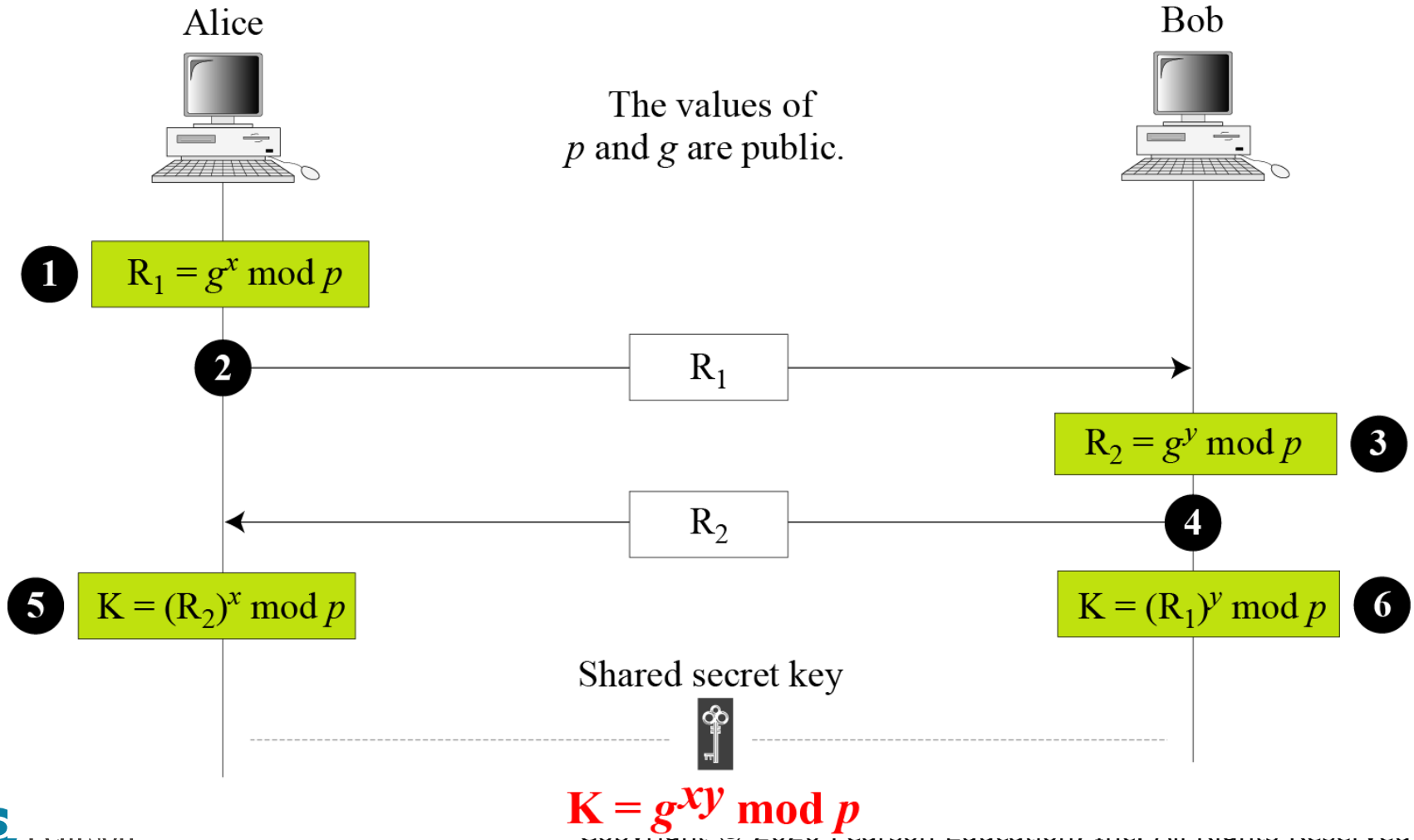


Figure 15.9 *Diffie-Hellman method*



Note

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

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; $g^{xy} \bmod p = 718 \bmod 35 = 18$.

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:

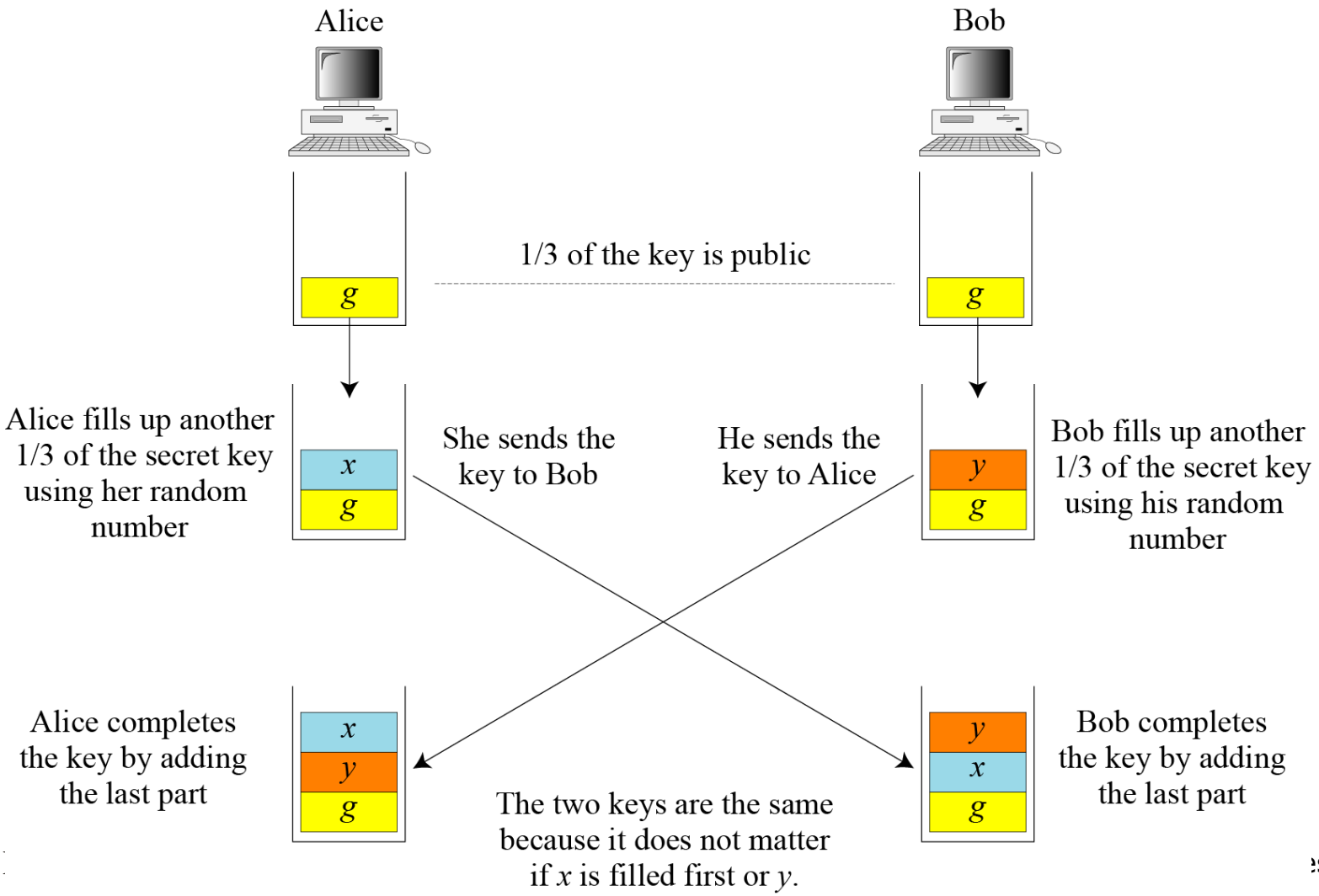
p	764624298563493572182493765955030507476338096726949748923573772860925235666660755423637423309661180033338106194730130950414738700999178043654878580798758 1
g	2
x	557
y	273

Example 15.2 Continued

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

$\mathbf{R_1}$	844920284205665505216172947491035094143433698520012660862863631067673619959280828586700802131859290945140217500319973312945836083821943065966020157955354
$\mathbf{R_2}$	435262838709200379470747114895581627636389116262115557975123379218566310011435718208390040181876486841753831165342691630263421106721508589625520128859414 3
K	155638000664522290596225827523270765273218046944423678520320400146406500887936651204257426776608327911017153038674561252213151610976584200120408643361774 0

Figure 15.10 *Diffie-Hellman idea*



Security of Diffie-Hellman

- Discrete Logarithm Attack
- Man-in-the-Middle Attack

Logarithm

In cryptography, we also need to discuss modular logarithm.

Exhaustive Search

Algorithm 9.8 *Exhaustive search for modular logarithm*

```
Modular_Logarithm (a, y, n)
{
    for (x = 1 to n −1)                          // k is the number of bits in x
    {
        if (y ≡ a^x mod n) return x
    }
    return failure
}
```

Continued

Order of the Group.

Example 9.46

What is the order of group $G = \langle Z_{21}^*, \times \rangle$? $|G| = \phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$. There are 12 elements in this group: 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, and 20. All are relatively prime with 21.

Order of an Element

Example 9.47

Find the order of all elements in $G = \langle Z_{10}^*, \times \rangle$.

Solution

This group has only $\phi(10) = 4$ elements: 1, 3, 7, 9. We can find the order of each element by trial and error.

a. $1^1 \equiv 1 \bmod (10) \rightarrow \text{ord}(1) = 1$.

b. $3^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(3) = 4$.

c. $7^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(7) = 4$.

d. $9^2 \equiv 1 \bmod (10) \rightarrow \text{ord}(9) = 2$.

Continued

Euler's Theorem

Example 9.48

Table 9.4 *Finding the orders of elements in Example 9.48*

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$	$i = 7$
$a = 1$	**x: 1**	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 3$	x: 3	**x: 1**	x: 3	x: 1	x: 3	x: 1	x: 3
$a = 5$	x: 5	**x: 1**	x: 5	x: 1	x: 5	x: 1	x: 5
$a = 7$	x: 7	**x: 1**	x: 7	x: 1	x: 7	x: 1	x: 7

Continued

Primitive Roots ***In the group $G = \langle Z_n^*, \times \rangle$, when the order of an element is the same as $\phi(n)$, that element is called the primitive root of the group.***

Example 9.49

Table 9.4 shows that there are no primitive roots in $G = \langle Z_8^*, \times \rangle$ because no element has the order equal to $\phi(8) = 4$. The order of elements are all smaller than 4.

Continued

Example 9.50

Table 9.5 shows the result of $a^i \equiv x \pmod 7$ for the group $G = \langle Z_7^*, \times \rangle$. In this group, $\phi(7) = 6$.

Table 9.5 *Example 9.50*

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
$a = 1$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 2$	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
Primitive root → $a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
$a = 4$	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
Primitive root → $a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
$a = 6$	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

Table 2.7 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Table 2.8 Tables of Discrete Logarithms, Modulo 19 (1 of 2)

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

Continued

Note

The group $G = \langle Z_n^*, \times \rangle$ has primitive roots only if n is 2, 4, p^t, or $2p^t$.

Example 9.51

For which value of n, does the group $G = \langle Z_n^*, \times \rangle$ have primitive roots: 17, 20, 38, and 50?

Solution

a. $G = \langle Z_{17}^*, \times \rangle$ has primitive roots, 17 is a prime.

b. $G = \langle Z_{20}^*, \times \rangle$ has no primitive roots.

c. $G = \langle Z_{38}^*, \times \rangle$ has primitive roots, $38 = 2 \times 19$ prime.

d. $G = \langle Z_{50}^*, \times \rangle$ has primitive roots, $50 = 2 \times 5^2$ and 5 is a prime.

Continued

Note

If the group $G = \langle Z_n^*, \times \rangle$ has any primitive root, the number of primitive roots is $\phi(\phi(n))$.

Continued

Cyclic Group ***If g is a primitive root in the group, we can generate the set Z_n^* as $Z_n^* = \{g^1, g^2, g^3, \ldots, g^{\phi(n)}\}$***

Example 9.52

The group $G = \langle Z_{10}^*, \times \rangle$ has two primitive roots because $\phi(10) = 4$ and $\phi(\phi(10)) = 2$. It can be found that the primitive roots are 3 and 7. The following shows how we can create the whole set Z_{10}^* using each primitive root.

$g = 3 \rightarrow$	$g^1 \bmod 10 = 3$	$g^2 \bmod 10 = 9$	$g^3 \bmod 10 = 7$	$g^4 \bmod 10 = 1$
$g = 7 \rightarrow$	$g^1 \bmod 10 = 7$	$g^2 \bmod 10 = 9$	$g^3 \bmod 10 = 3$	$g^4 \bmod 10 = 1$

The group $G = \langle Z_n^*, \times \rangle$ is a cyclic group if it has primitive roots.
The group $G = \langle Z_p^*, \times \rangle$ is always cyclic.

Continued

The idea of Discrete Logarithm

Properties of $G = \langle Z_p^*, \times \rangle$:

1. **Its elements include all integers from 1 to $p - 1$.**

2. **It always has primitive roots.**

3. **It is cyclic. The elements can be created using g^x where x is an integer from 1 to $\phi(p) = p - 1$.**

4. **The primitive roots can be thought as the base of logarithm.**

Solution to Modular Logarithm Using Discrete Logs

Tabulation of Discrete Logarithms

Table 9.6 *Discrete logarithm for* $\mathbf{G} = \langle \mathbf{Z}_7^*, \times \rangle$

y	1	2	3	4	5	6
$x = \mathrm{L}_3\, y$	6	2	1	4	5	3
$x = \mathrm{L}_5\, y$	6	4	5	2	1	3

Table 2.8 Tables of Discrete Logarithms, Modulo 19 (2 of 2)

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Continued

Example 9.53

Find x in each of the following cases:

a. $4 \equiv 3^x \pmod 7$.

b. $6 \equiv 5^x \pmod 7$.

Solution

We can easily use the tabulation of the discrete logarithm in Table 9.6.

a. $4 \equiv 3^x \bmod 7 \rightarrow x = L_3 4 \bmod 7 = 4 \bmod 7$

b. $6 \equiv 5^x \bmod 7 \rightarrow x = L_5 6 \bmod 7 = 3 \bmod 7$

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

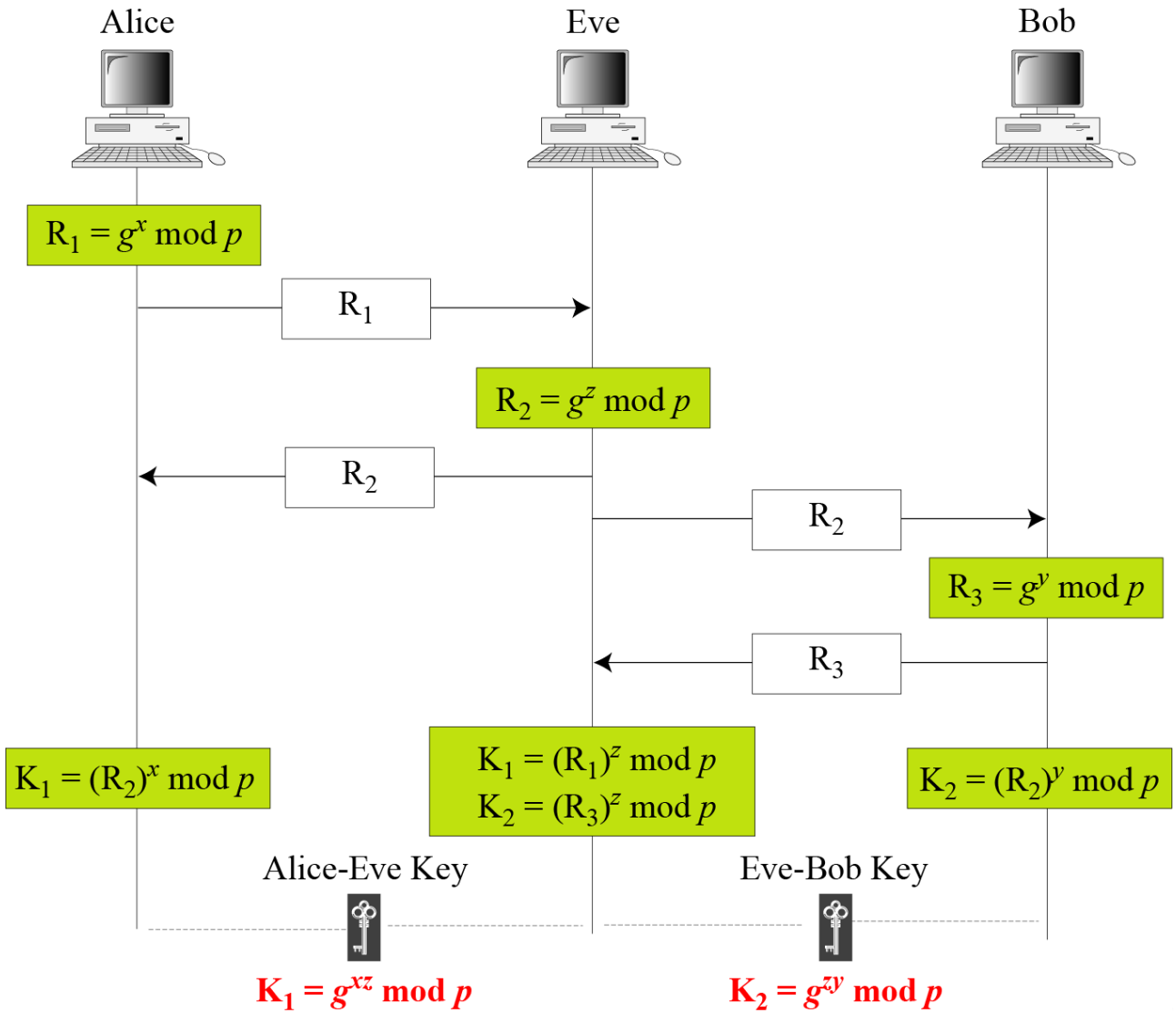
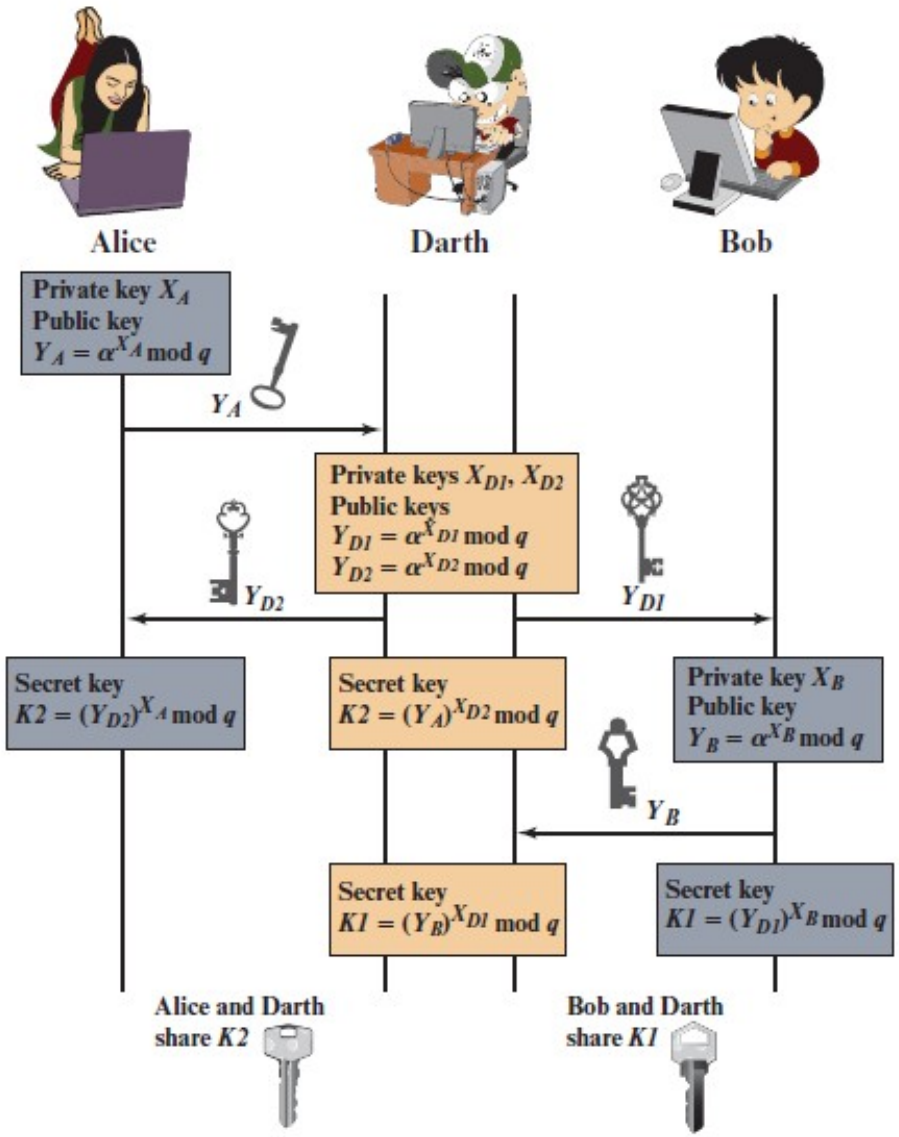


Figure 10.2 Man-in-the-Middle Attack

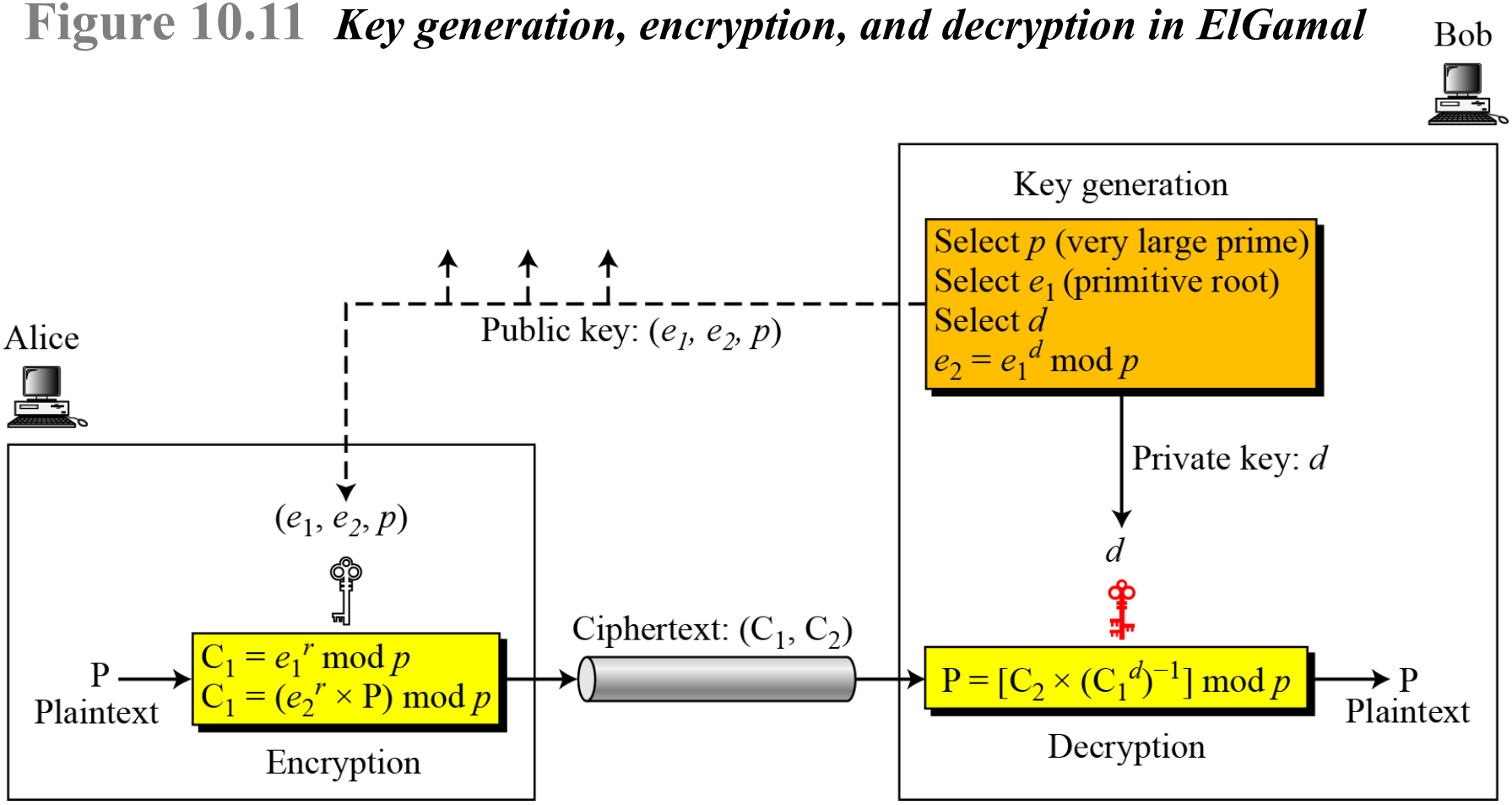


ElGamal Cryptography

- Announced in 1984 by T. Elgamal
- Public-key scheme based on discrete logarithms closely related to the Diffie-Hellman technique
- Used in the digital signature standard (DSS) and the S/MIME e-mail standard
- Global elements are a prime number q and a which is a primitive root of q
- Security is based on the difficulty of computing discrete logarithms

10.4.2 Procedure

Figure 10.11 *Key generation, encryption, and decryption in ElGamal*



10.4.2 Continued

Key Generation

Algorithm 10.9 *ElGamal key generation*

ElGamal_Key_Generation

{

Select a large prime p

Select d to be a member of the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$ such that $1 \leq d \leq p - 2$

Select e_1 to be a primitive root in the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$

$e_2 \leftarrow e_1^{\,d} \bmod p$

Public_key $\leftarrow (e_1, e_2, p)$ // To be announced publicly

Private_key $\leftarrow d$ // To be kept secret

return Public_key and Private_key

}

10.4.2 Continued

Algorithm 10.10 *ElGamal encryption*

ElGamal_Encryption (e_1, e_2, p, P) // P is the plaintext

{

Select a random integer r in the group $\mathbf{G} = < \mathbf{Z}_p^*, \times >$

$\text{C}_1 \leftarrow e_1^{\,r} \bmod p$

$\text{C}_2 \leftarrow (\text{P} \times e_2^{\,r}) \bmod p$ // C_1 and C_2 are the ciphertexts

return C_1 and C_2

}

10.4.2 Continued

Algorithm 10.11 *ElGamal decryption*

```
ElGamal_Decryption (d, p, C1, C2)          // C1 and C2 are the ciphertexts
{
    P ← [C2 (C1^d)^−1] mod p               // P is the plaintext
    return P
}
```

Note

The bit-operation complexity of encryption or decryption in ElGamal cryptosystem is polynomial.

Figure 10.3 The ElGamal Cryptosystem

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice	
Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$\{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

10.4.3 Continued

Example 10. 10

Here is a trivial example. Bob chooses p = 11 and $e_1 = 2$. and d = 3 $e_2 = e_1^d = 8$. So the public keys are (2, 8, 11) and the private key is 3. Alice chooses r = 4 and calculates C1 and C2 for the plaintext 7.

Plaintext: 7

$$C_1 = e_1^{\,r} \bmod 11 = 16 \bmod 11 = 5 \bmod 11$$

$$C_2 = (P \times e_2^{\,r}) \bmod 11 = (7 \times 4096) \bmod 11 = 6 \bmod 11$$

Bob receives the ciphertexts (5 and 6) and calculates the plaintext.

$$[C_2 \times (C_1^{\,d})^{-1}] \bmod 11 = 6 \times (5^3)^{-1} \bmod 11 = 6 \times 3 \bmod 11 = 7 \bmod 11$$

Plaintext: 7

Example 10. 11

Instead of using $P = [C_2 \times (C_1^d)^{-1}] \bmod p$ for decryption, we can avoid the calculation of multiplicative inverse and use $P = [C_2 \times C_1^{p-1-d}] \bmod p$ (see Fermat's little theorem in Chapter 9). In Example 10.10, we can calculate $P = [6 \times 5^{11-1-3}] \bmod 11 = 7 \bmod 11$.

Note

For the ElGamal cryptosystem, *p* must be at least 300 digits and *r* must be new for each encipherment.

10.4.3 Continued

Example 10. 12

Bob uses a random integer of 512 bits. The integer p is a 155-digit number (the ideal is 300 digits). Bob then chooses e_1, d, and calculates e_2, as shown below:

p =	11534899272561676244925313717014331740490094532609834959814346921905689869862264593212975473787189514436889176526473093615929993728061165964347353440008577
e_1 =	2
d =	1007
e_2 =	97886413043009189508766856938097739043880062887337687610022062233255450707415618921231831770461014167336015088413294085724853770315820660100725587074 55

10.4.3 Continued

Example 10. 10

Alice has the plaintext P = 3200 to send to Bob. She chooses r = 545131, calculates C1 and C2, and sends them to Bob.

P =	3200
***r* =**	545131
C_1 =	887297069383528471022570471492275663120260067256562125018835142941722359971268111410536366170517305158153318916540097373635508029573678856906061915288 1
C_2 =	708454333048929944577016012380794999567436021836192446961774506921244696155165800779455593080345889614402408599525919579209721628879681350582779566430295 0

Bob calculates the plaintext $P = C_2 \times ((C_1)^d)^{-1} \bmod p = 3200 \bmod p$.

P =	3200

Summary

- Define Diffie-Hellman Key Exchange
- Understand the Man-in-the-middle attack
- Present an overview of the Elgamal cryptographic system
- Understand Elliptic curve arithmetic
- Present an overview of elliptic curve cryptography
- Present two techniques for generating pseudorandom numbers using an asymmetric cipher

Copyright