Chapter 4- Number theory and Public key Cryptography

Number theory

Divisibility

We say that a nonzero **b divides a** if $a=mb$ for some m, where a, b and m are integers. That is, b divides a if there is no remainder on division. The $b|a$ notation is commonly used to mean b divides a.

Example: The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

- Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer q quotient and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \le r < n; q = \lfloor a/n \rfloor$$

- We will use the notation **gcd(a, b)** to mean the **greatest common divisor** of a and b.

$$\gcd(a, b) = \max[k, \text{such that } k|a \text{ and } k|b]$$

- Two integers are **relatively prime** if their only common positive integer factor is 1, i.e **gcd(a,b)=1**.
- Note that $gcd(b, 0) = gcd(0, b) = b$.

THE EUCLIDEAN ALGORITHM

It is a simple procedure for determining the greatest common divisor of two positive integers.

Euclidean Algorithm

Comment: compute $\gcd(a,b)$, where $a > b > 1$.

$r_0 := a$

$r_1 := b$

for $i := 1, 2, \ldots$ until $r_{n+1} = 0$

$\quad r_{i+1} := r_{i-1} \bmod r_i$

return (r_n)

Example: compute the GCD(1160718174, 316258250).

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943434	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

The Modulus

If a is an integer and n is a positive integer, we define **a mod n** to be the remainder when a is divided by n. The integer n is called the **modulus**. *Example*: 11 mod 7 = 4;

- Two integers and are said to be **congruent modulo** n, if (a mod n)=(b mod n).
- This is written as $a \equiv b \pmod{n}$, *example*: $73 \equiv 4 \pmod{23}$;

Modular Arithmetic

Define Z_n the set as the set of nonnegative integers less than n :

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Example:

$11 \bmod 8 = 3; 15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

- Exponentiation is performed by repeated multiplication

  To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$
$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$
$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

- Tables below provides an illustration of modular addition and multiplication modulo 8.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

- Note that **not** all integers mod 8 have a *multiplicative inverse*.
- In general, an integer has a multiplicative inverse in Z_n if that integer is relatively prime to *n*. integers 1, 3, 5, and 7 have a multiplicative inverse in Z_8; but 2, 4, and 6 do not.
- The set $Z_n^*$is all elements in Zn that are relatively prime to *n*,

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n | \gcd(a, n) = 1\}$$

Example: For $n = 10 = 2 * 5$ the following applies:

full remainder set $R = \mathbb{Z}_n = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

reduced remainder set $R' = \mathbb{Z}_n^* = \{1, 3, 7, 9\} \longrightarrow \phi(n) = 4.$

The Extended Euclidean Algorithm

For given integers *a* and *b*, the extended Euclidean algorithm not only calculate the greatest common divisor but also two additional integers *x* and *y* that satisfy the following equation.

$$ax + by = d = \gcd(a, b)$$

- Now let us show how to extend the Euclidean algorithm to determine (*x,y,d*) given *a* and *b*.

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
• • •	• • •	• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-3} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_{n-2} \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

Example: suppose that *a=1759, b=550,* solve *ax+yb=gcd(a,b).*

i	r_i	q_i	x_i	y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: $d = 1$; $x = -111$; $y = 355$

Computing Multiplicative Inverses

Given N and $a \in Z_N$ with gcd(a, N) =1, then there exist integers X, Y with $Xa+YN = 1$. We can use the following algorithm to find the multiplicative inverse:

ALGORITHM B.11
Computing modular inverses

Input: Modulus N; element a
Output: a^{-1} (if it exists)

$(d, X, Y) :=$ eGCD(a, N) /* note that $Xa + YN = \gcd(a, N)$ */
if $d \neq 1$ **return** "a is not invertible modulo N"
else return $[X \bmod N]$

PRIME NUMBERS

- An integer p is a prime number if and only if its only divisors are ±1 and ±p.
- Any integer a>1 can be factored in a unique way as

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

Example:

$$91 = 7 \times 13$$
$$3600 = 2^4 \times 3^2 \times 5^2$$
$$11011 = 7 \times 11^2 \times 13$$

- The quantity of prime numbers is infinite.

  Proof according to Euclid (proof by contradiction)

  Assumption: There is a *finite* number of primes.

  Conclusion: Then these can be listed $p_1 < p_2 < p_3 < \cdots < p_n$, where n is the (finite) number of prime numbers. p_n is therefore the largest prime. Euclid now looks at the number $a = p_1 \cdot p_2 \cdots p_n + 1$. This number cannot be a prime number because it is not included in our list of primes. It must therefore be divisible by a prime, i.e. there is a natural number i between 1 and n, such that p_i divides the number a. Of course, p_i also divides the product $a - 1 = p_1 \cdot p_2 \cdots p_n$, because p_i is a factor of $a - 1$. Since p_i divides the numbers a and $a - 1$, it also divides the difference of these numbers. Thus: p_i divides $a - (a - 1) = 1$. p_i must therefore divide 1, which is impossible.

  Contradiction: Our assumption was false.

- Below we list the first 2000 prime numbers.

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Fermat's Theorem

Fermat's theorem states the following: If p is prime and is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Example:

$a = 7, p = 19$

$7^2 = 49 \equiv 11 \pmod{19}$

$7^4 \equiv 121 \equiv 7 \pmod{19}$

$7^8 \equiv 49 \equiv 11 \pmod{19}$

$7^{16} \equiv 121 \equiv 7 \pmod{19}$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$

Also, we have:

$$a^p \equiv a (\bmod p)$$

Euler's Totient Function

Euler's totient function, written $\emptyset(n)$, and defined as the number of positive integers less than *n* and relatively prime to *n*.

$\boldsymbol{\emptyset(N) = |\mathbb{Z}_N^*|}$, the *order* of the group $\mathbb{Z}_N^*$

- If $N = p$ is prime. Then all elements in $\{1, \ldots, p-1\}$ are relatively prime to *p*, and so

$$\emptyset(p) = p - 1$$

- If $N = pq$, where *p, q* are distinct primes, then

$$\emptyset(N) = (p-1)(q-1)$$

DETERMINE $\phi(37)$ AND $\phi(35)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.

To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

There are 24 numbers on the list, so $\phi(35) = 24$.

- Below we list some of Euiler's totient functions

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Euler's Theorem

Euler's theorem states that for every *a* and *n* that are relatively prime:

$$a^{\phi(n)} \equiv 1 (\bmod n)$$

Example:

$a = 3; n = 10;\ \phi(10) = 4 \quad a^{\phi(n)} = 3^4 = 81 = 1 (\bmod 10) = 1 (\bmod n)$

$a = 2; n = 11;\ \phi(11) = 10 \quad a^{\phi(n)} = 2^{10} = 1024 = 1 (\bmod 11) = 1 (\bmod n)$

DISCRETE LOGARITHMS

Discrete logarithms are fundamental to a number of public-key algorithms, including Diffie-Hellman key exchange and the digital signature algorithm (DSA).

- If a and n are relatively prime, then there is at least one integer m that satisfies:

$$a^m \equiv 1 \pmod{n}$$

Where m=$\emptyset(n)$, is called the **order** of *a*.

- Table below shows all the powers of a, modulo 19 for all positive $a<19$.

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

Important Notes

- ✓ All sequences end in 1.
- ✓ Some of the sequences are of length 18. In this case, it is said that the base integer **generates** the set of nonzero integers modulo 19.
  - Each such integer is called a **primitive root** of the modulus 19.
- So, primitive root of n is the number a whose order is $\emptyset(n)$.
- The importance of this notion is that if a is a primitive root of n, then its powers

$$a, a^2, \ldots, a^{\phi(n)}$$

  are distinct and are all relatively prime to n.
- For the prime number 19, its primitive roots are 2, 3, 10, 13, 14, and 15.

Calculation of Discrete Logarithms

Consider the equation

$$y = g^x \bmod p$$

- Given g, x, and p, it is a straightforward matter to calculate y. At the worst, we must perform repeated multiplications.
- However, given y,g, and p, it is, in general, very difficult to calculate x (take the discrete logarithm).

PUBLIC-KEY CRYPTOGRAPHY AND RSA

- Public key is first developed by Diffie and Hellman in 1976.
- Public-key algorithms are based on mathematical functions rather than on substitution and permutation.

- public-key cryptography is asymmetric, involving the use of *two* separate keys, in contrast to symmetric encryption, which uses only one key.
- The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption.
    - The first problem is that of *key distribution*
    - The second problem is *digital signatures*.

Public-Key Cryptosystems

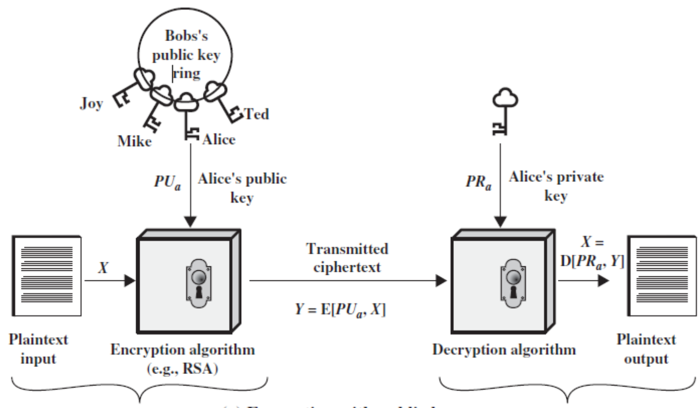
Asymmetric algorithms rely on *one key for encryption* and a *different* but related *key for decryption*.

These algorithms have the following important characteristic.

1- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.

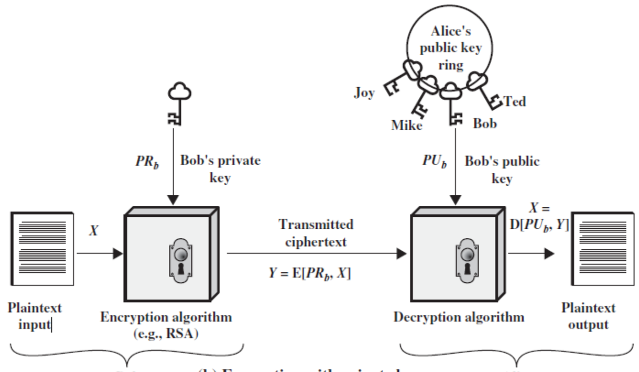
2- Either of the two related keys can be used for encryption, with the other used for decryption.

❖ We get *secrecy* (*confidentiality*) when encrypting by the receiver public key.



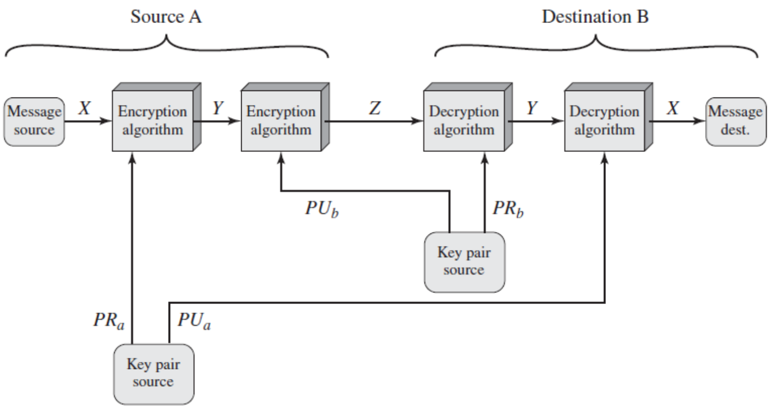
(a) Encryption with public key

❖ We get (*authentication*) when encrypting by the sender private key.



(b) Encryption with private key

❖ We can combine the (secrecy and authentication) as follows:



Applications for Public-Key Cryptosystems

1- **Encryption /decryption**: The sender encrypts a message with the recipient's public key.
2- **Digital signature**: The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
3- **Key exchange**: Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.
4-

- A *one-way function* is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible:

$$Y = f(X) \quad \text{easy}$$
$$X = f^{-1}(Y) \quad \text{infeasible}$$

- We now turn to the definition of a *trap-door one-way function*, which is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known.

$$Y = f_k(X) \quad \text{easy, if } k \text{ and } X \text{ are known}$$
$$X = f_k^{-1}(Y) \quad \text{easy, if } k \text{ and } Y \text{ are known}$$
$$X = f_k^{-1}(Y) \quad \text{infeasible, if } Y \text{ is known but } k \text{ is not known}$$

THE RSA ALGORITHM

- It is developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978.
- The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some n.
- A typical size for n is 1024 bits, or 309 decimal digits.
- That is, the block size must be less than or equal to $log2(n) + 1$.
- Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C.

$$C = M^e \bmod n$$
$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

- Both sender and receiver must know the value of n.
- The sender knows the value of e, and only the receiver knows the value of d.
- Thus, this is a public-key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$
- We need to find a relationship of the form

$$M^{ed} \bmod n = M$$

- The preceding relationship holds if e and d are *multiplicative inverses* modulo $\emptyset(n)$, where $\emptyset(n)$ is the Euler totient function.
- Recall that for p, q prime, $\emptyset(pq) = (p - 1)(q - 1)$. The relationship between e and d can be expressed as

$$ed \bmod \phi(n) = 1$$

- This is equivalent to saying

$$ed \equiv 1 \bmod \phi(n)$$

$$d \equiv e^{-1} \bmod \phi(n)$$

- So, the items of RSA scheme are:

p, q, two prime numbers	(private, chosen)
$n = pq$	(public, calculated)
e, with $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$	(public, chosen)
$d \equiv e^{-1} \pmod{\phi(n)}$	(private, calculated)

Example:

1. Select two prime numbers, $p = 17$ and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose $e = 7$.
5. Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. The correct value is $d = 23$, because $23 \times 7 = 161 = (1 \times 160) + 1$; d can be calculated using the extended Euclid's algorithm (Chapter 4).

- The resulting keys are public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$.
- The example shows the use of these keys for a plaintext input of $M = 88$.
- For **encryption**, we need to calculate $C = 88^7 \bmod 187$.

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$88^1 \bmod 187 = 88$$

$$88^2 \bmod 187 = 7744 \bmod 187 = 77$$

$$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$$

$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$$

- For **decryption**, we calculate $M = 11^{23} \bmod 187$:

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$

$$11^1 \bmod 187 = 11$$

$$11^2 \bmod 187 = 121$$

$$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$$

$$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$$

$$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$$

EXPONENTIATION IN MODULAR ARITHMETIC

- Both encryption and decryption in RSA involve raising an integer to an integer power, mod n.
- If the exponentiation is done over the integers and then reduced modulo n, the intermediate values would be huge.
- Fortunately, as the preceding example shows, we can make use of a property of modular arithmetic:

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

- To calculate the exponent operation in efficient way, we use the **fast power method**.
- Suppose we wish to calculate $x^{11} \bmod n$ for some integers x and n. Observe that $x^{11} = x^{1+2+8} = (x)(x^2)(x^8)$. In this case, we compute $x \bmod n$, $x^2 \bmod n$, $x^4 \bmod n$, and $x^8 \bmod n$ and then calculate $[(x \bmod n) \times (x^2 \bmod n) \times (x^8 \bmod n)] \bmod n$.
- More generally, suppose we wish to find the value a^b with a and m positive integers. If we express b as a binary number *bkbk*-1. . . *b*0, then we have

$$b = \sum_{b_i \neq 0} 2^i$$

$$a^b \bmod n = \left[\prod_{b_i \neq 0} a^{(2^i)}\right] \bmod n = \left(\prod_{b_i \neq 0}\left[a^{(2^i)} \bmod n\right]\right) \bmod n$$

```
c ← 0; f ← 1
for i ← k downto 0
    do  c ← 2 × c
        f ← (f × f) mod n
    if  b_i = 1
        then c ← c + 1
             f ← (f × a) mod n
return f
```

Note: The integer b is expressed as a binary number $b_k b_{k-1} \ldots b_0$.

Figure 9.8 Algorithm for Computing a^b mod n

Table 9.4 Result of the Fast Modular Exponentiation Algorithm for $a^b \bmod n$, where $a = 7$, $b = 560 = 1000110000$, and $n = 561$

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
f	7	49	157	526	160	241	298	166	67	1

- To speed up the operation of the RSA algorithm using the public key, a specific choice of e is usually made. The most common choice is 65537 ($2^{16} + 1$); two other popular choices are 3 and 17.
    - Each of these choices has only two 1 bits, so the number of multiplications required to perform exponentiation is minimized.

The Security of RSA

Four possible approaches to attacking the RSA algorithm are

- **Brute force:** This involves trying all possible private keys.
- **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes.
- **Timing attacks:** These depend on the running time of the decryption algorithm.
- **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.

THE FACTORING PROBLEM

We can identify three approaches to attacking RSA mathematically.

1. Factor n into its two prime factors. This enables calculation of $\phi(n) = (p - 1) \times (q - 1)$, which in turn enables determination of $d \equiv e^{-1} \pmod{\phi(n)}$.
2. Determine $\phi(n)$ directly, without first determining p and q. Again, this enables determination of $d \equiv e^{-1} \pmod{\phi(n)}$.
3. Determine d directly, without first determining $\phi(n)$.

- Most discussions of the cryptanalysis of RSA have focused on the task of factoring n into its two prime factors.
- For a large n with large prime factors, factoring is a hard problem.
- Currently we know that RSA is at most as difficult as factorization, but we cannot prove that its exactly as difficult as factorization. Or in other words: We cannot prove, that if RSA (the cryptosystem) is broken, that then factorization (the hard mathematical problem) can be solved.
- The Rabin cryptosystem was the first cryptosystem which could be proven to be computationally equivalent to a hard problem.

Number of Decimal Digits	Approximate Number of Bits	Date Achieved	MIPS-Years	Algorithm
100	332	April 1991	7	Quadratic sieve
110	365	April 1992	75	Quadratic sieve
120	398	June 1993	830	Quadratic sieve
129	428	April 1994	5000	Quadratic sieve
130	431	April 1996	1000	Generalized number field sieve
140	465	February 1999	2000	Generalized number field sieve
155	512	August 1999	8000	Generalized number field sieve
160	530	April 2003	—	Lattice sieve
174	576	December 2003	—	Lattice sieve
200	663	May 2005	—	Lattice sieve

TIMING ATTACKS

This attack can determine a private key by keeping track of how long a computer takes to decipher messages.

- Although the timing attack is a serious threat, there are simple countermeasures that can be used, including the following.

1- **Constant exponentiation time:** Ensure that all exponentiations take the same amount of time before returning a result.

2- **Random delay:** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.

3- **Blinding:** Multiply the ciphertext by a random number before performing exponentiation. This process prevents the attacker from knowing what ciphertext bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack.

- RSA Data Security incorporates a blinding feature into some of its products.
- The private-key operation $M = C^d \bmod n$ is implemented as follows.

1. Generate a secret random number r between 0 and $n - 1$.
2. Compute $C' = C(r^e) \bmod n$, where e is the public exponent.
3. Compute $M' = (C')^d \bmod n$ with the ordinary RSA implementation.
4. Compute $M = M'r^{-1} \bmod n$. In this equation, r^{-1} is the multiplicative inverse of $r \bmod n$; see Chapter 4 for a discussion of this concept. It can be demonstrated that this is the correct result by observing that $r^{ed} \bmod n = r \bmod n$.

CHOSEN CIPHERTEXT ATTACK

- The basic RSA algorithm is vulnerable to a **chosen ciphertext attack** (CCA).
- CCA is defined as an attack in which the adversary chooses a number of ciphertexts and is then given the corresponding plaintexts, decrypted with the target's private key.
- A simple example of a CCA against RSA takes advantage of the following *homomorphism* property of RSA:

$$\mathrm{E}(PU, M_1) \times \mathrm{E}(PU, M_2) = \mathrm{E}(PU, [M_1 \times M_2])$$

- We can decrypt $C = M^e \bmod n$ using a CCA as follows.

1. Compute $X = (C \times 2^e) \bmod n$.
2. Submit X as a chosen ciphertext and receive back $Y = X^d \bmod n$.

   But now note that

$$\begin{aligned} X &= (C \bmod n) \times (2^e \bmod n) \\ &= (M^e \bmod n) \times (2^e \bmod n) \\ &= (2M)^e \bmod n \end{aligned}$$

Therefore, $Y = (2M) \bmod n$.

- To overcome this simple attack, practical RSA-based cryptosystems *randomly pad* the plaintext prior to encryption.