Discrete Mathematics

Number Theory

Lorena Ronquillo

lron@itu.dk

11/09/2014 [week 3]

Today's lecture

IT University of Copenhagen

1. Integer Representations and Algorithms
   - Representations of Integers
   - Base b expansion of n
   - Constructing the base b expansion
   - Conversion between different representations
   - Operations in binary notation
2. Divisibility
   - Divisibility
   - The Quotient-Remainder Theorem
3. Primes and Greatest Common Divisors
   - Primes
   - Greatest Common Divisor
   - Least Common Multiple
   - The Euclidean Algorithm
4. Modular Arithmetic
   - Modular Arithmetic
   - Inverse modulo m
   - Computing $a^k \bmod n$
5. Applications of Congruences
   - Classical Cryptography
   - RSA Cryptography

Outline

IT University of Copenhagen

Representations of Integers (I)

IT University of Copenhagen

We commonly use the decimal (base 10) representation of integers.
However, the binary (base 2), octal (base 8), and hexadecimal (base 16) representations are often used in computer science.

Example of uses:

- Computers represent data in sets of binary digits. A binary digit is known as bit, and 8 bits make 1 byte.
- MAC Addresses (e.g. 00:80:AD:00:49:9E) are given in hexadecimal representation.

- In UNIX systems, the command **chmod** changes the access permission of a file, and uses octal representation. Ex: chmod 777 slides.pdf

#	Permission
7	full
6	read and write
5	read and execute
4	read only
3	write and execute
2	write only
1	execute only
0	none

Representations of Integers (II)

IT University of Copenhagen

Example Given the number 349 in decimal notation, we have:

- Binary notation: $(101011101)_2$
- Hexadecimal notation: $(15D)_{16}$

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Base b expansion of n

IT University of Copenhagen

Given an integer $b > 1$, we have that any positive integer n can be expressed uniquely as

$$n = \mathbf{a}_k b^k + \mathbf{a}_{k-1} b^{k-1} + \cdots + \mathbf{a}_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

Example Given the integer 349 in decimal notation,

- Decimal expansion: $(349)_{10} = \mathbf{3} \cdot 10^2 + \mathbf{4} \cdot 10 + \mathbf{9}$.
- Binary expansion:
  $(101011101)_2 = \mathbf{1} \cdot 2^8 + \mathbf{0} \cdot 2^7 + \mathbf{1} \cdot 2^6 + \mathbf{0} \cdot 2^5 + \mathbf{1} \cdot 2^4 + \mathbf{1} \cdot 2^3 + \mathbf{1} \cdot 2^2 + \mathbf{0} \cdot 2^1 + \mathbf{1}$
- Hexadecimal expansion: $(15D)_{16} = \mathbf{1} \cdot 16^2 + \mathbf{5} \cdot 16 + \mathbf{D}$ (D in hexadecimal is 13 in decimal notation)

Constructing the base b expansion (I)

IT University of Copenhagen

Given an integer n (in its decimal notation), how can we construct its base b expansion?

ALGORITHM 1 Constructing Base b Expansions.

procedure *base b expansion*(n, b: positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q$ **mod** b
    $q := q$ **div** b
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$ {$(a_{k-1} \ldots a_1 a_0)_b$ is the base b expansion of n}

Constructing the base b expansion (II)

Example Find the binary representation of $(25)_{10}$.

$$
\begin{array}{r|l}
2 & 25 \\
\hline
 & 20 \\
\hline
 & 5 \\
 & 4 \\
\hline
 & 1
\end{array}
\qquad
\begin{array}{r|l}
2 & 12 \\
\hline
 & 12 \\
\hline
 & 0
\end{array}
\qquad
\begin{array}{r|l}
2 & 6 \\
\hline
 & 6 \\
\hline
 & 0
\end{array}
\qquad
\begin{array}{r|l}
2 & 3 \\
\hline
 & 2 \\
\hline
 & 1
\end{array}
\qquad
\begin{array}{r|l}
2 & 1 \\
\hline
 & 0 \\
\hline
 & 1
\end{array}
$$

It follows that $(25)_{10} = (11001)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1$.

Constructing the base b expansion (III)

Exercise Find the hexadecimal representation of $(4321)_{10}$.

$$\begin{array}{r|l} & 270 \\ 16 & 4321 \\ & 3200 \\ \hline & 1121 \\ & 1120 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} & 16 \\ 16 & 270 \\ & 160 \\ \hline & 110 \\ & 96 \\ \hline & 14 \end{array} \qquad \begin{array}{r|l} & 1 \\ 16 & 16 \\ & 16 \\ \hline & 0 \end{array} \qquad \begin{array}{r|l} & 0 \\ 16 & 1 \\ & 0 \\ \hline & 1 \end{array}$$

It follows that $(4321)_{10} = (10E1)_{16} = 1 \cdot 16^3 + 0 \cdot 16^2 + 14 \cdot 16^1 + 1$.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Conversion between different representations

The conversion between binary and hexadecimal representations is straightforward.

We need four binary digits in order to represent the integers $\{0, 1, \ldots, 15\}$, so each hexadecimal digit corresponds to a block of four binary digits.

Example Find the hexadecimal representation of $(01111001)_2$.

$$(0111\ 1001)_2 \longrightarrow (7\ 9)_{16}$$

Exercise Find the binary representation of $(F04)_{16}$.

$$(F\ 0\ 4)_{16} \longrightarrow (1111\ 0000\ 0100)_2$$

Operations in binary notation

- Addition We add pairs of binary digits together with carries (when they occur).

  Example

$$\begin{array}{cccc} & {\scriptstyle 1} & & \\ & 1 & 1 & 0 \\ + & 0 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 \end{array}$$

- Multiplication Also based on the conventional algorithm for multiplying numbers with paper and pencil.

  Example

$$\begin{array}{cccccc} & & & 1 & 1 & 0 \\ & & \times & 0 & 1 & 1 \\ \hline & & {\scriptstyle 1} & 1 & 1 & 0 \\ & {\scriptstyle 1} & 1 & 1 & 0 & \\ 0 & 0 & 0 & & & \\ \hline 1 & 0 & 0 & 1 & 0 & \end{array}$$

Outline

Divisibility

Given two integers a and b, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, or in other words, if $\frac{b}{a}$ is an integer.

Notation:

$a \mid b$ denotes that a divides b. Then a is a factor (or divisor) of b, and b is a multiple of a.

$a \nmid b$ denotes that a does not divide b.

Example $3 \mid 12$ because $\frac{12}{3}$ is an integer, but $5 \nmid 12$.

Theorem Let a, b, and c be integers, where $a \neq 0$. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

(ii) if $a \mid b$, then $a \mid bc$ for all integers c;

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$. (Transitivity of Divisibility)

Example

- if $3 \mid 9$ and $3 \mid 21$, then $3 \mid (9 + 21) = 3 \mid 30$.
- if $3 \mid 9$, then $3 \mid (9 \cdot 2)$, $3 \mid (9 \cdot 3)$, ...
- if $3 \mid 9$ and $9 \mid 45$, then $3 \mid 45$.

The Quotient-Remainder Theorem

IT University of Copenhagen

Let a be an integer and d a positive integer. Then there exist unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

$$\begin{array}{r|l} & q \\ d & a \\ & r \end{array}$$

The value d is called the divisor, a is the dividend, q is the quotient, and r is the remainder. Then $q = a$ **div** d, $r = a$ **mod** d.

Note that the remainder cannot be negative.

Example What are the quotient and remainder when -23 is divided by 4?

$$\begin{array}{r|l} & -6 \\ 4 & -23 \\ & -24 \\ \hline & 1 \end{array}$$

So -23 div $4 = -6$, and $-23 \mod 4 = 1$. Then,

$$-23 = 4(-6) + 1.$$

The Quotient-Remainder Theorem (II)

IT University of Copenhagen

Example Given an integer m, if $m \bmod 7 = 4$, what is $5m \bmod 7$?

$m \bmod 7 = 4$ means that the remainder of dividing m by 7 is 4, that is

$$m = 7q + 4.$$

Thus

$$\begin{aligned} 5m &= 35q + 20 \\ &= 35q + 14 + 6 \\ &= 7(5q + 2) + 6. \end{aligned}$$

Since $6 < 7$, the remainder when dividing $5m$ by 7 is 6.

Therefore,

$$5m \bmod 7 = 6.$$

Outline

Primes (I)

A prime p is an integer greater than 1 if its only positive factors are 1 and p. Any other integer greater than 1 but not being prime, is called a composite.

Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in increasing order.

Example

The prime factors of 1000 and 360 are given by

$1000 = 2^3 \cdot 5^3$.
$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$.

Primes (II)

Procedure to find the prime factorization of an integer n:

1. Begin by dividing n by successive primes, starting with the smallest prime. If n is a composite integer, a prime factor p will be found. Otherwise n is a prime.
2. If a prime factor p is found, continue by factoring $\frac{n}{p}$.
3. If $\frac{n}{p}$ has no prime factor $q \geq p$, then it is prime. Otherwise, if it has a prime factor q, continue by factoring $\frac{n}{pq}$.
4. Continue this procedure until the factorization ends up with a prime.

n	p
$\frac{n}{p}$	q
$\frac{n}{pq}$	$\cdots$
$\vdots$	$\vdots$
r	r
1	

$$n = p \cdot q \cdot \ldots \cdot r$$

Primes (III)

Example The factorization of 660 is

$$\begin{array}{r|ll} 660 & 2 & \\ 330 & 2 & \\ 165 & 3 & 2 \nmid 165 \\ 55 & 5 & 3 \nmid 55 \\ 11 & 11 & \\ 1 & & \end{array}$$

Then we have $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$.

Primes (IV)

IT University of Copenhagen

Theorem If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

So an integer is prime if it is not divisible by any prime less than or equal to its square root.

Example Is 253 prime?

Since $\sqrt{253} \simeq 16$, we only need to check whether 253 is divisible by $2, 3, 5, 7, 11$ or 13 (all prime numbers less than or equal to 16). We see that $11 \mid 253$, so 253 is not prime.

Exercise Is 101 prime?

Since $\sqrt{101} \simeq 10$, we only need to check whether 101 is divisible by 2, 3, 5 or 7. Since it is not divisible by any of them, 101 is prime.

Primes (V)

IT University of Copenhagen

Theorem There are infinitely many primes.

This means that the sequence

$$2, 3, 5, 7, 11, 13, \ldots$$

never ends.

More and more primes are still being discovered.

Least Common Multiple

Given two positive integers a and b, the smallest positive integer that is a multiple of **both** a and b is the least common multiple, denoted by $\text{lcm}(a, b)$.

Given $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then

$$\text{lcm}(a, b) = p_1^{\max\{a_1, b_1\}} \cdot p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

Example

a) $\text{lcm}(4, 5) = \text{lcm}(2^2, 5) = 20.$

b) $\text{lcm}(1260, 378) = \text{lcm}(2^2 \cdot 3^2 \cdot 5 \cdot 7, 2 \cdot 3^3 \cdot 7) = 2^2 \cdot 3^3 \cdot 5 \cdot 7 = 3780.$

Greatest Common Divisor (I)

Given two integers, a and b, not both zero, the largest integer d such that $d \mid a$ and $d \mid b$ is the greatest common divisor of a and b, denoted by $\gcd(a, b)$.

To find the gcd of two integers, we can find all the positive integers that are divisors of **both** a and b, and then take the largest one.

Given $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$, then

$$\gcd(a, b) = p_1^{\min\{a_1, b_1\}} \cdot p_2^{\min\{a_2, b_2\}} \cdots p_n^{\min\{a_n, b_n\}}.$$

Exercise Find the greatest common divisor of 12 and 30.

Since $12 = 2^2 \cdot 3$, and $30 = 2 \cdot 3 \cdot 5$, then $\gcd(12, 30) = 2 \cdot 3 = 6$.

Greatest Common Divisor (II)

IT University of Copenhagen

Two integers a and b are relatively prime if $\gcd(a, b) = 1$.

Equivalently, a set of integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ for any pair of integers, a_i and a_j, in the set.

Exercise Are the integers $12, 35$ and 11 pairwise relatively prime?

Since $12 = 2^2 \cdot 3 = 12$, $35 = 5 \cdot 7$ and $11 = 11 \cdot 1$, we have

$$\gcd(12, 35) = 1,\ \gcd(12, 11) = 1, \quad \text{and} \quad \gcd(11, 35) = 1.$$

Therefore, they are pairwise relatively prime.

The Euclidean Algorithm (I)

IT University of Copenhagen

Lemma Let $a = bq + r$, where a, b, q and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Given the prime factorizations of two integers, computing their greatest common divisor is inefficient.
The Euclidean Algorithm is a more efficient method to compute it.

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ **is** $x\}$

The Euclidean Algorithm (II)

Example Find the gcd of 20 and 97 using the Euclidean algorithm.

$$\begin{aligned} 97 &= 4 \cdot 20 + 17 \\ 20 &= 1 \cdot 17 + 3 \\ 17 &= 5 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{array}{r|l} & 4 \\ \hline 20 & 97 \\ & 80 \\ \hline & 17 \end{array} \qquad \begin{array}{r|l} & 1 \\ \hline 17 & 20 \\ & 17 \\ \hline & 3 \end{array} \qquad \begin{array}{r|l} & 5 \\ \hline 3 & 17 \\ & 15 \\ \hline & 2 \end{array} \qquad \begin{array}{r|l} & 1 \\ \hline 2 & 3 \\ & 2 \\ \hline & 1 \end{array}$$

$$\begin{array}{r|l} & 2 \\ \hline 1 & 2 \\ & 2 \\ \hline & 0 \end{array}$$

$$\gcd(97, 20) = \gcd(20, 17) = \gcd(17, 3) = \gcd(3, 2) = \gcd(2, 1) = 1.$$

The Euclidean Algorithm (III)

IT University of Copenhagen

Exercise Find the $\gcd$ of 210 and 45 using the Euclidean algorithm.

$$\begin{aligned} 210 &= 4 \cdot 45 + 30 \\ 45 &= 1 \cdot 30 + 15 \\ 30 &= 2 \cdot 15 + 0 \end{aligned}$$

$$\begin{array}{r|l} & 4 \\ \hline 45 & 210 \\ & 180 \\ \hline & 30 \end{array} \qquad \begin{array}{r|l} & 1 \\ \hline 30 & 45 \\ & 30 \\ \hline & 15 \end{array} \qquad \begin{array}{r|l} & 2 \\ \hline 15 & 30 \\ & 30 \\ \hline & 0 \end{array}$$

$\gcd(210, 45) = \gcd(45, 30) = \gcd(30, 15) = 15.$

Outline

IT University of Copenhagen

Modular Arithmetic (I)

IT University of Copenhagen

We have already introduced the notation a **mod** m to represent the remainder when an integer a is divided by the positive integer m.

We now introduce a different notation that indicates that two integers have the same remainder when they are divided by the positive integer m.

Given two integers a and b, and a positive integer m, we say that a is congruent to b modulo m if $m \mid (a - b)$.

Some notation:

$a \equiv b \pmod{m}$ means that a is congruent to b modulo m.

$a \not\equiv b \pmod{m}$ means that a and b are not congruent modulo m.

We say that $a \equiv b \pmod{m}$ is a congruence and that m is its modulus.

Example Is 25 congruent to 7 modulo 3?
We see that 3 divides $25 - 7 = 18$. Therefore, $25 \equiv 7 \pmod{3}$.

Modular Arithmetic (II)

IT University of Copenhagen

Theorem Let m be a positive integer.

$$\begin{array}{lcl} a \equiv b \pmod{m} & & a + c \equiv b + d \pmod{m} \\ \text{and} & \Rightarrow & \text{and} \\ c \equiv d \pmod{m} & & ac \equiv bd \pmod{m} \end{array}$$

Be careful!

- If $ac \equiv bc \pmod{m}$, the congruence $a \equiv b \pmod{m}$ may be false.

Corollary Given two integers a and b, and a positive integer m, we have

$$\begin{aligned} (a + b) \bmod m &= (a \bmod m) + (b \bmod m) \bmod m \\ ab \bmod m &= (a \bmod m)(b \bmod m) \bmod m \end{aligned}$$

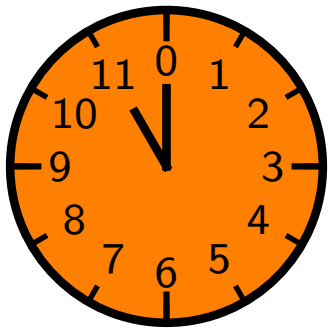
Example

- $(7 + 5) \bmod 3 = (7 \bmod 3) + (5 \bmod 3) \bmod 3 = (1 + 2) \bmod 3 = 0.$
- $7 \cdot 5 \bmod 3 = (7 \bmod 3) \cdot (5 \bmod 3) \bmod 3 = (1 \cdot 2) \bmod 3 = 2.$

Modular Arithmetic III

Example The hours of a clock are elements modulo 12.
We will replace the 12 at the top of the clock with a 0. Starting at noon, the hour hand of a clock points in order to the following:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 0, \ldots$$



Computing $a^k \bmod n$

Example Compute $14^{11} \bmod 142$.

First write the exponent as a sum of powers of 2:

$$11 = 2^3 + 2 + 1 = 8 + 2 + 1.$$

Next compute 14^{2^k} for $k = 0, 1, 2, 3$.

$$\begin{aligned}
14 \bmod 143 &= 14.\\
14^2 \bmod 143 &= 196 \bmod 143 = 53.\\
14^4 \bmod 143 &= 53^2 \bmod 143 = 2809 \bmod 143 = 92.\\
14^8 \bmod 143 &= 92^2 \bmod 143 = 8464 \bmod 143 = 27.
\end{aligned}$$

Then, since

$$14^{11} = 14^{8+2+1} = 14^8 \cdot 14^2 \cdot 14.$$

We have

$$\begin{aligned}
14^{11} \bmod 143 &= (14^8 \bmod 143) \cdot (14^2 \bmod 143) \cdot (14 \bmod 143) \bmod 143\\
&= (27 \cdot 53 \cdot 14) \bmod 143\\
&= 20034 \bmod 143 = 14.
\end{aligned}$$

Inverse Modulo n

IT University of Copenhagen

For any integers a and n, the value s such that

$$as \equiv 1 \pmod{n}.$$

is called the inverse of a modulo n.

Example

- The inverse of 4 modulo 5 is 4, since $4 \cdot 4 = 16 \equiv 1 \pmod{5}$.
- The inverse of 2 modulo 5 is 3, since $2 \cdot 3 = 6 \equiv 1 \pmod{5}$.

Some elements do not have an inverse modulo an integer n. For example, there is no number x modulo 4 such that

$$2x \equiv 1 \pmod{4}.$$

For all integers a and n, $\boxed{\text{if } \gcd(a, n) = 1}$, then there exists an integer s such that $as \equiv 1 \pmod{n}$.

Exercise Does 4 have an inverse modulo 7? If so, what is it?

It has, since $\gcd(4, 7) = 1$. The inverse of 4 is 2, so

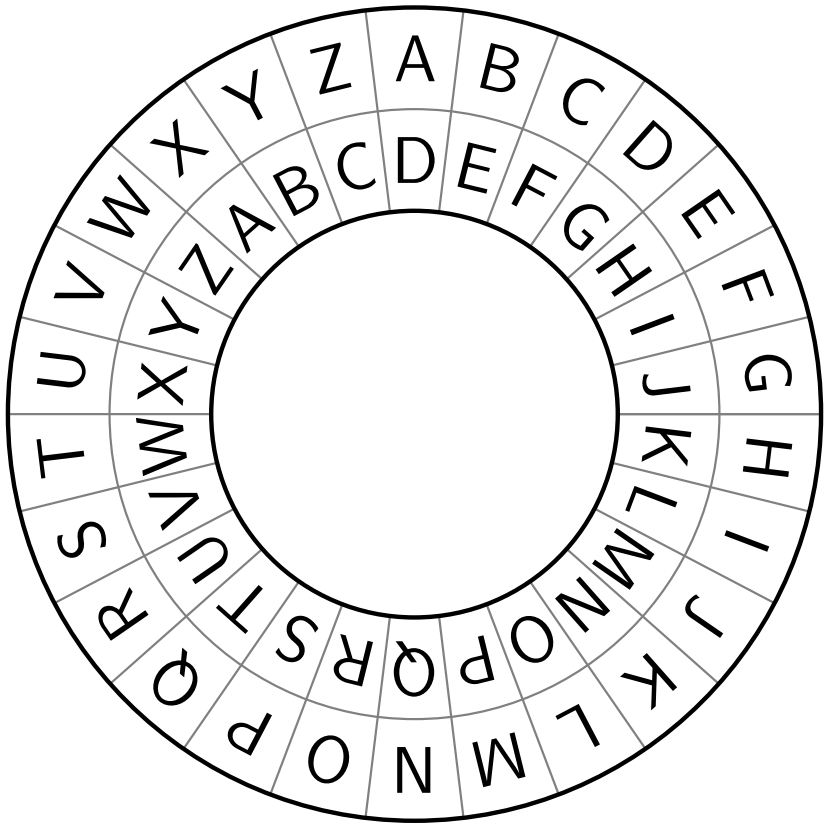
$$4 \cdot 2 = 8 \equiv 1 \pmod{7}.$$

Outline

Classical Cryptography (I)

IT University of Copenhagen

Congruences are also used to encrypt secret messages.
Caesar's encryption shifts each letter three letters forward in the alphabet.



Classical Cryptography (II)

IT University of Copenhagen

Encryption with Caesar's cipher

1. Replace each letter in the message by its numeric equivalence.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

2. Add 3 to this value $(\mathrm{mod}\ 26)$.
3. Replace each resulting integer by the corresponding letter.

Decryption with Caesar's cipher

1. Replace each letter in the encrypted message by its numeric equivalence.
2. Subtract 3 to this value $(\mathrm{mod}\ 26)$.
3. Replace the resulting integer by the corresponding letter.

Classical Cryptography (III)

In general, the function used in Caesar's algorithm is

$$f(p) = (p + k) \pmod{26},$$

where k is the secret key, and p the numerical value corresponding to the letter being encrypted.

Example Encrypt the message "HELLO WORLD" using the key $k = 13$.

H	E	L	L	O		W	O	R	L	D
↓	↓	↓	↓	↓		↓	↓	↓	↓	↓
8	5	12	12	15		23	15	18	12	4
↓	↓	↓	↓	↓		↓	↓	↓	↓	↓
21	18	25	25	2		10	2	5	25	17
↓	↓	↓	↓	↓		↓	↓	↓	↓	↓
U	R	Y	Y	B		J	B	E	Y	Q

RSA Cryptography (I)

IT University of Copenhagen

Developed by three mathematicians: Ronald Rivest, Adi Shamir, and Leonard Adleman.

It is a public key (or asymmetric) cryptosystem: there is a public key and a private key.

Public key: (e, n)

- integer n such that $n = p \cdot q$.
- Positive (and large) integer e such that e is relatively prime to $(p-1)(q-1)$, i.e. $\gcd(e, (p-1)(q-1)) = 1$.

Private key: (p, q, d)

- Two **large** primes p and q.
- Positive integer d such that d is a positive inverse of e modulo $(p-1)(q-1)$, i.e. $ed \equiv 1 \bmod ((p-1)(q-1))$.

RSA cipher exploits the difficulty of performing the prime factorization of numbers.

RSA Cryptography (II)

Everybody knows the public key, so anybody can encrypt a message for Alice. But only Alice has the secret key necessary to decrypt the encrypted messages intended for her.

Bob encrypts a message for Alice

1. Bob encodes every letter of the message the same way as in the Caesar cipher. Let M be the corresponding numerical value to be encrypted.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

2. Bob sends to Alice C, where

$$C = M^e \pmod{n}, \text{ where } n = pq.$$

He will send his message in blocks, one per letter.

Alice decrypts the message coming from Bob

- Alice receives C from Bob, and recovers the original message M by computing

$$M = C^d \pmod{n}, \text{ where } n = pq.$$

RSA cryptography (III)

IT University of Copenhagen

1. Alice chooses two prime numbers, say $p = 11$ and $q = 13$, and computes $pq = 143$.
2. She chooses a positive integer e that is relatively prime to $(p-1)(q-1)$. In this case, $(p-1)(q-1) = 10 \cdot 12 = 120$, so she may take $e = 7$ (note $120 = 2^3 \cdot 3 \cdot 5$).
3. Now she thinks of an integer d such that d is an inverse of e modulo $(p-1)(q-1)$. In this case, $d = 103$. Note that, indeed, $103 \cdot 7 \equiv 1 \bmod 120$.

Public key: $(e, n) = (7, 143)$.
Secret key: $(p, q, d) = (11, 13, 103)$.

Example Given an RSA cipher with public key $(e, n) = (7, 143)$, encrypt the message "NO".

"N" is encoded as $M_1 = 14$ and "O" as $M_2 = 15$.

So the encryption of the message are the following two blocks

$$C_1 = M_1^e \pmod{n} = 14^7 \pmod{143} = 53$$

and

$$C_2 = M_2^e \pmod{n} = 15^7 \pmod{143} = 115.$$

RSA Cryptography (IV)

IT University of Copenhagen

Example Given an RSA cipher with public key $(e, n) = (7, 143)$ and private key $(p, q, d) = (11, 13, 103)$, decrypt the previous ciphertexts.

We compute

$$M_1 = C_1^d \pmod{n} = 53^{103} \pmod{143} = 14$$

and

$$M_2 = C_2^d \pmod{n} = 115^{103} \pmod{143} = 15.$$

We know that 14 corresponds to "N", and 15 to "O".