6.6 Number representation

6.7 Fast exponentiation

6.8 Introduction to cryptography

6.7 Representation of Integers

In our everyday life we use decimal notation to express integers

Note: decimal notation and decimal numbers are two different terms.

The other ones you probably have heard of are: binary, HEX (hexadecimal), and maybe octal.

6.7 Representation of Integers

In our everyday life we use decimal notation to express integers

Note: decimal notation and decimal numbers are two different terms.

The other ones you probably have heard of are: binary, HEX (hexadecimal), and maybe octal.

[Theorem]
Let $b \in \mathbf{Z}^+$ and $b > 1$. Then if n is a positive integer, it can be expressed uniquely in the form $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

A proof of this theorem can be constructed using mathematical induction (not presented here)

$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$ is called base b expansion of n

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 10 gives decimal notation.

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 10 gives decimal notation.

Example: 567 stands for 5 hundreds + 6 tens + 7 ones

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 10 gives decimal notation.

Example: 567 stands for 5 hundreds + 6 tens + 7 ones

$567 = 5 * 10^2 + 6 * 10^1 + 7 * 10^0 =$
$= 500 + 60 + 7$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 10 gives decimal notation.

Example: 567 stands for 5 hundreds + 6 tens + 7 ones

$$567 = 5 * 10^2 + 6 * 10^1 + 7 * 10^0 =$$
$$= 500 \quad + 60 \quad + 7$$

<ins>digits</ins>: 0,1,2,3,4,5,6,7,8,9

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$

binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$

binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.

$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1; n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0; 0 \leq a_i < b$, $i = 0,\ldots,k,$ and $a_k \neq 0.$

Choosing the base b to be 2 gives binary expansions of integers.

<u>digits</u>: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

<u>Solution</u>: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 =$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

<u>digits</u>: *0, 1*
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

<u>Solution</u>: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = \ 1 +$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

<u>digits</u>: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

<u>Solution</u>: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = \ 1 + 0 \cdot 2$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = \ 1 + 0 \cdot 2 + 0 \cdot 2^2 +$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 +$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 =$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 = 1 + 8 + 16 + 64 + 128 + 512$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$

binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.

$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 = 1 + 8 + 16 + 64 + 128 + 512 = 729_{10}$

Answer: $(10\ 1101\ 1001)_2 = 729_{10}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$
$10\ 11\ 12\ 13\ 14\ 15$

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16}$ =

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

<u>digits</u>: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*

10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

<u>Solution</u>: using the highlighted formula and starting from the right, i.e.

$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 +$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

<u>digits</u>: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

<u>Solution</u>: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = \; 11 + 0 \cdot 16 +$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

<u>digits</u>: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

<u>Solution</u>: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 + 15 \cdot 16^2 + 13 \cdot 16^3 + 3 \cdot 16^4 =$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$
$10\ 11\ 12\ 13\ 14\ 15$

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 + 15 \cdot 16^2 + 13 \cdot 16^3 + 3 \cdot 16^4 = 11 + 3840 + 53248 + 196608$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$
$10\ 11\ 12\ 13\ 14\ 15$

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 + 15 \cdot 16^2 + 13 \cdot 16^3 + 3 \cdot 16^4 = 11 + 3840 + 53248 + 196608 = 253707_{10}$

Answer: $(3DF0B)_{16} = 253707_{10}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0, \ldots, k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*

10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

$4678 \div 16 = 292$ R 6

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

<u>digits</u>: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

<u>Solution</u>: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

$4678 \div 16 = 292 \text{ R } 6$
$292 \div 16 = 18 \text{ R } 4$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

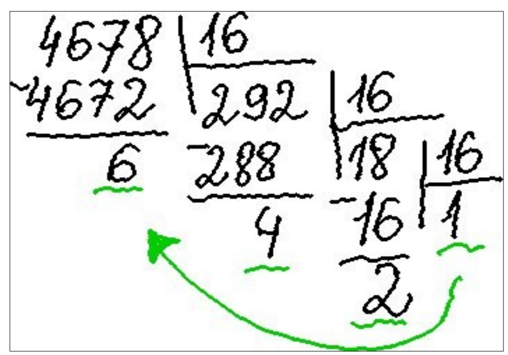
digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

$4678 \div 16 = 292$ R 6
$292 \div 16 = 18$ R 4
$18 \div 16 = 1$ R 2

or



Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0, \ldots, k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

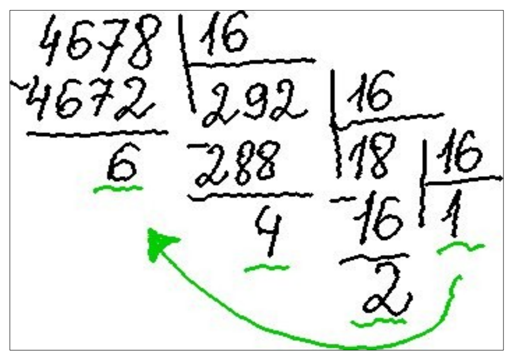
digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

$4678 \div 16 = 292$ R 6
$292 \div 16 = 18$ R 4
$18 \div 16 = 1$ R 2

or



Now, starting from the end (from the last quotient): $(1\ 2\ 4\ 6)_{16}$

Answer: $(4678)_{10} = (1246)_{16}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

<u>digits</u>: $0, 1, 2, 3, 4, 5, 6, 7$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

<u>digits</u>: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

<u>digits</u>: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

<u>Solution</u>:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 =$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7$

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

<u>digits</u>: $0, 1, 2, 3, 4, 5, 6, 7$

Example: Find the decimal expansion of $(1347)_8$

<u>Solution</u>:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

<u>Answer</u>: $(1347)_8 = 743$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7$

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Example: Find the octal expansion of $(47)_{10}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7$

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Example: Find the octal expansion of $(47)_{10}$

Solution:
$47 \div 8 = 5$ R 7

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7$

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 \;=\; 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

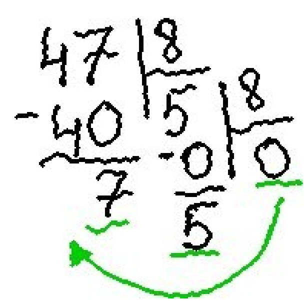
Example: Find the octal expansion of $(47)_{10}$

Solution:

$47 \div 8 = 5$ R 7

$5 \div 8 = 0$ R 5

or



Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: $0, 1, 2, 3, 4, 5, 6, 7$

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 \;=\; 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Example: Find the octal expansion of $(47)_{10}$

Solution:
$47 \div 8 = 5$ R 7
$5 \div 8 = 0$ R 5

or

$$\begin{array}{r|l} 47 & 8 \\ \hline -40 & 5 \\ \hline 7 & \end{array} \qquad \begin{array}{r|l} 5 & 8 \\ \hline -0 & 0 \\ \hline 5 & \end{array}$$

Answer: $(057)_8 = (57)_8$

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of "conversions", but be very careful when using it. There are lots of nuances.

Example:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11	1010	1001	1111
3	A	9	F

therefore,
$(11\ 1010\ 1001\ 1111)_2 = (3A9F)_{16}$

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

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

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed),

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of "conversions", but be very careful when using it. There are lots of nuances.

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

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of "conversions", but be very careful when using it. There are lots of nuances.

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

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of "conversions", but be very careful when using it. There are lots of nuances.

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

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A

Hexadecimal Expansion (HEX)

There is a nice table allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

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

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A 9

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of "conversions", but be very careful when using it. There are lots of nuances.

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

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A 9 F

therefore,
$(11\ 1010\ 1001\ 1111)_2 = (3A9F)_{16}$

In cryptography it is important to be able to find b^n efficiently, where b, n are large integers.

We can use an algorithm that employs the binary expansion of the exponent n. To compute b^n, the algorithm computes b, b^2, $(b^2)^2$,$(b^4)^2$, ... till some point, and then multiplies all of them.

In cryptography it is important to be able to find b^n efficiently, where b, n are large integers.

We can use an algorithm that employs the binary expansion of the exponent n. To compute b^n, the algorithm computes b, b^2, $(b^2)^2$,$(b^4)^2$, ... till some point, and then multiplies all of them.

Input: Positive integers x and y.
Output: x^y

```
procedure fastExponentiation(x,y)
p := 1    // p holds the partial result.
s := x    // s holds the current (x^2)^j
r := y    // r is used for binary expansion of y

While ( r > 0 )
      If ( r mod 2 = 1 ), p := p·s
      s := s·s
      r := r div 2
End-while
Return(p)
```

Example: Find 7^{16}

p = 1, s = 7, r = 16

```
p := 1
s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s
   s := s·s
   r := r div 2
End-while
Return(p)
```

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

7^2

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
      p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49 7^2
r = 16 div 2 = 8

p = 1, s = 49, r = 8

```
p := 1
s := x
r := y

while ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s
   s := s·s
   r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49 7^2
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401 $(7^2)^2$
r = 8 div 2 = 4

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401 7^4
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

```
p := 1
s := x
r := y

while ( r > 0 )
    If ( r mod 2 = 1 )
        p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401 **7^4**
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801 **$(7^4)^2$**
r = 4 div 2 = 2

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
      p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 5 764 801, r = 2

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801 $\quad 7^8$
r = 4 div 2 = 2

```
p := 1
s := x
r := y

while ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801 **7^8**
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 **$(7^8)^2$**
r = 2 div 2 = 1

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
        p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 7^{16}
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

```
p := 1
s := x
r := y

while ( r > 0 )
    If ( r mod 2 = 1 )
        p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 7^{16}
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

1 mod 2 = 1
p = 1 * 33 232 930 569 601
s = 33 232 930 569 601^2 = ...
r = 1 div 2 = 0

```
p := 1
s := x
r := y

while ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s
   s := s·s
   r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 7^{16}
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

1 mod 2 = 1
p = 1 * 33 232 930 569 601 7^{16}
s = 33 232 930 569 601^2 = ...
r = 1 div 2 = 0

```
p := 1
s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s
   s := s·s
   r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

1 mod 2 = 1
p = 1 * 33 232 930 569 601 7^{16}
s = 33 232 930 569 601^2 = ...
r = 1 div 2 = 0

```
p := 1
s := x
r := y

while ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Return(33 232 930 569 601)

Modular Exponentiation

Example: Find 7^{16}

What does the algorithm do?

$16 = (1\ 0000)_2 = 1 * 2^4 + 0 * 2^3 + 0 * 2^2 + 0 * 2^1 + 0 * 2^0$

Therefore $7^{16} = 7^{1*2^4+0*2^3+0*2^2+0*2^1+0*2^0} = 7^{2^4} * \underset{\substack{\uparrow \\ \text{4th iter.}}}{7^0} * \underset{\substack{\uparrow \\ \text{3rd iter.}}}{7^0} * \underset{\substack{\uparrow \\ \text{2nd iteration}}}{7^0} * \underset{\substack{\uparrow \\ \text{1st iteration}}}{7^0}$

Modular Exponentiation

In cryptography it is important to be able to find b^n ***mod*** m efficiently, where b, n, and m are large integers.

As we have discussed, it is impractical to first compute b^n and then find its remainder when divided by m, because b^n will be a huge number.

Modular Exponentiation

In cryptography it is important to be able to find b^n ***mod*** m efficiently, where *b, n*, and *m* are large integers.

As we have discussed, it is impractical to first compute b^n and then find its remainder when divided by *m*, because b^n will be a huge number.

```
Input: Positive integers x and y.
Output: x^y mod n

p := 1   //p holds the partial result.
s := x   //s holds the current (x^2)^j
r := y   //r is used to compute the binary expansion of y

While ( r > 0 )
      If ( r mod 2 = 1 )
            p := p·s mod n
      s := s·s mod n
      r := r div 2
End-while

Return(p)
```

modifications from fast exponentiation are shown in pink

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1*, hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Modular Exponentiation

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Modular Exponentiation

Example: Find 7^{644} ***mod*** *645*

$644 = (10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

p = 1, s = 466, r = 161

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

p = 1, s = 466, r = 161

161 mod 2 = 1, *hence p is updated*
p = 1 * 466 mod 645 = 466
s = 466^2 mod 645 = 436
r = 161 div 2 = 80

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Modular Exponentiation

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1*, hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1*, hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

p = 1, s = 466, r = 161

161 mod 2 = 1*, hence p is updated*
p = 1 * 466 mod 645 = 466
s = 466^2 mod 645 = 436
r = 161 div 2 = 80

p = 466, s = 436, r = 80

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find *7^{644}* ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1*, hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1*, hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1*, hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1*, hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

p = 466, s = 436, r = 20

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

p = 466, s = 436, r = 20

20 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 20 div 2 = 10

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1*, hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1*, hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

p = 466, s = 436, r = 20

20 mod 2 != 1*, hence p is not updated*
s = 436^2 mod 645 = 466
r = 20 div 2 = 10

p = 466, s = 466, r = 10

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 466, r = 10

10 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
r = 10 div 2 = 5

p = 466, s = 436, r = 5

5 mod 2 = 1, *hence p is updated*
p = 466 * 436 mod 645 = 1
s = 436^2 mod 645 = 466
r = 5 div 2 = 2

p = 1 , s = 466, r = 2

2 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
r = 2 div 2 = 1

p = 1, s = 436, r=1

```
p := 1, s := x
r := y

while ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 436, r=1

1 mod 2 = 1, hence p is updated
p = 1 * 436 mod 645 = 436
s = 436^2 mod 645 = 466
r = 1 div 2 = 0

p = 436, s = 466, r = 0

STOP

Return(436)

7^{644} ***mod*** *645 = 436*

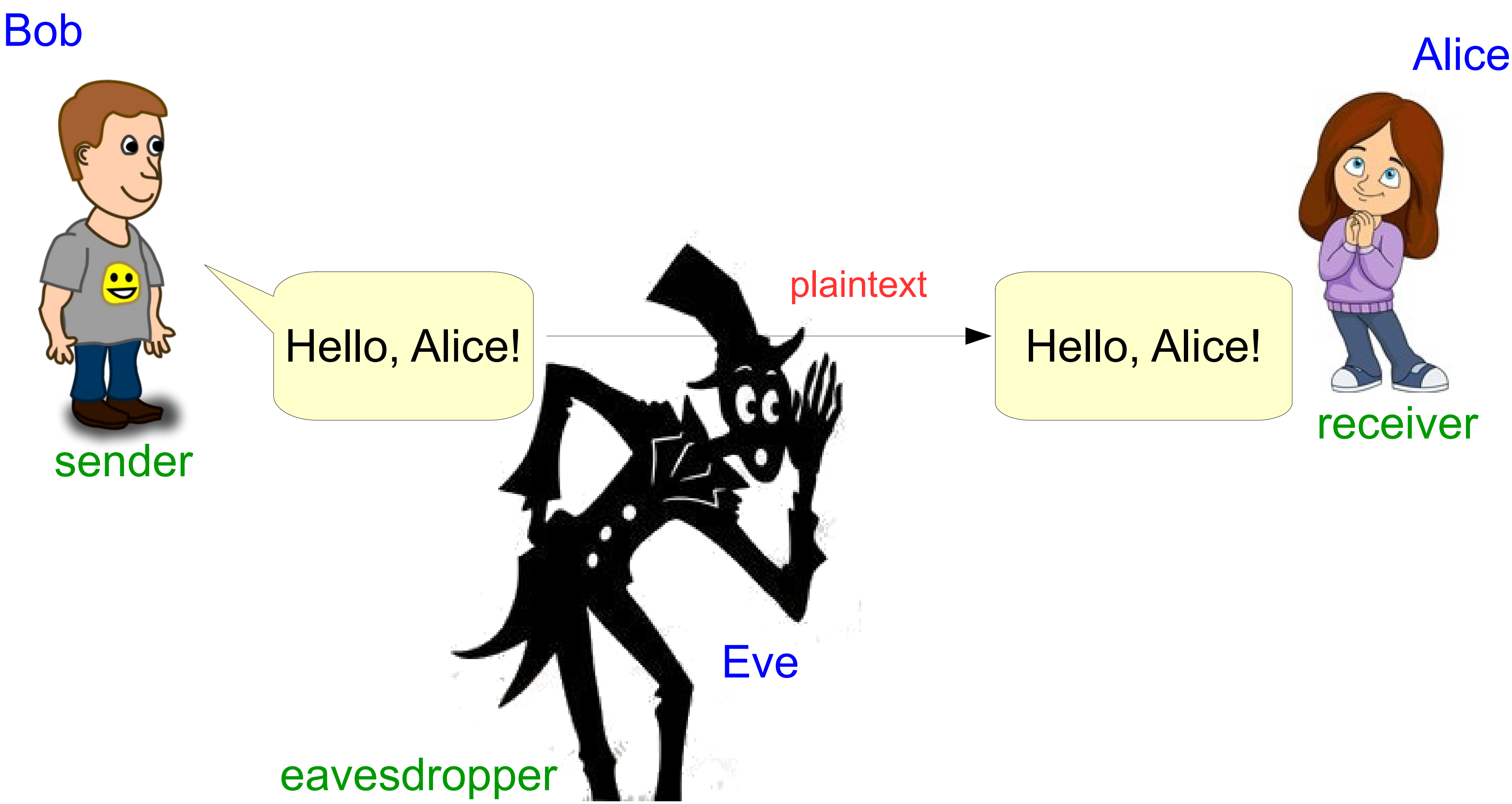
```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
        p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

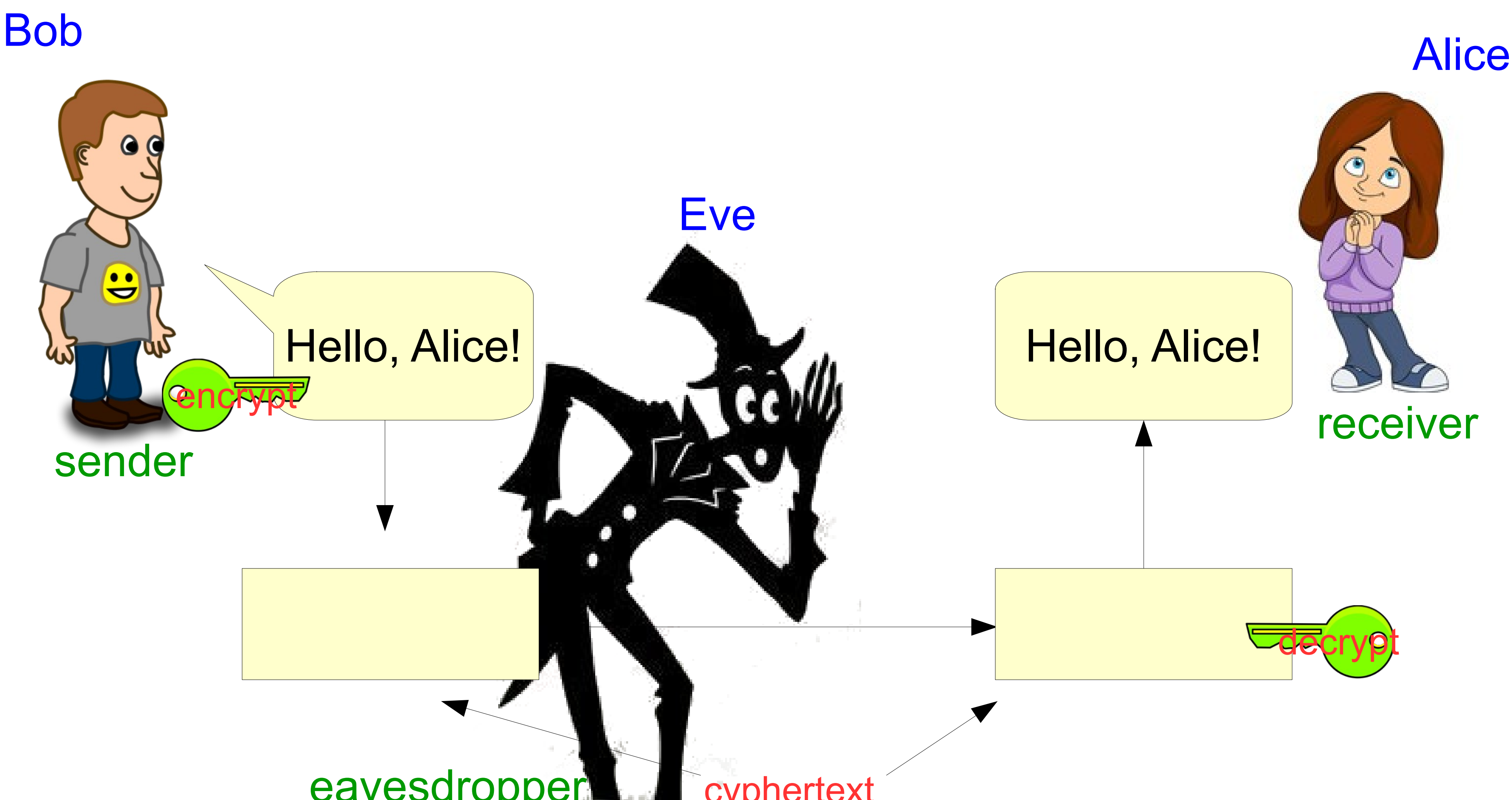
6.8 Introduction to cryptography

Cryptography is science of protecting and authenticating data and communication.
One important aspect: sending messages securely in the presence of eavesdroppers who can learn the transmitted information.



6.8 Introduction to cryptography

Cryptography is science of protecting and authenticating data and communication.
One important aspect: sending messages securely in the presence of eavesdroppers who can learn the transmitted information.



6.8 Introduction to cryptography

Often we transmit text messages. Therefore, we convert text message into an integer, then the "message" is encrypted and sent.

There are many possible ways to do the conversion.

Example: assume that the message contains only uppercase letters, space characters, and periods

A	01	N	14	_	27
B	02	O	15	.	28
C	03	P	16		
D	04	Q	17		
E	05	R	18		
F	06	S	19		
G	07	T	20		
H	08	U	21		
I	09	V	22		
J	10	W	23		
K	11	X	24		
L	12	Y	25		
M	13	Z	26		

not onto, but
has to be one-to-one

6.8 Introduction to cryptography

Often we transmit text messages. Therefore, we convert text message into an integer, then the “message” is encrypted and sent.

There are many possible ways to do the conversion.

Example: assume that the message contains only uppercase letters, space characters, and periods

A	01	N	14	_	27
B	02	O	15	.	28
C	03	P	16		
D	04	Q	17		
E	05	R	18		
F	06	S	19		
G	07	T	20		
H	08	U	21		
I	09	V	22		
J	10	W	23		
K	11	X	24		
L	12	Y	25		
M	13	Z	26		

H E L L O   A L I C E .

0805121215011209030528

integer plaintext

6.8 Introduction to cryptography

Often we transmit text messages. Therefore, we convert text message into an integer, then the "message" is encrypted and sent.

There are many possible ways to do the conversion.

Example: assume that the message contains only uppercase letters, space characters, and periods

A	01	N	14	_	27
B	02	O	15	.	28
C	03	P	16		
D	04	Q	17		
E	05	R	18		
F	06	S	19		
G	07	T	20		
H	08	U	21		
I	09	V	22		
J	10	W	23		
K	11	X	24		
L	12	Y	25		
M	13	Z	26		

H E L L O A L I C E .

$\downarrow$

0805121215011209030528

The mapping of text messages to numbers described above gives a function from strings of length n to integers with *2n* digits.

The translation of text messages to numbers need not be secure.

6.8 Introduction to cryptography

Modern cryptosystems rely on **number theory** in which the encryption and decryption procedures are mathematical functions whose input and output are integers.

To encrypt a plaintext message: compute a mathematical function with the *integer plaintext* m as the input and the *ciphertext* c as the output.

To decrypt: is to compute the inverse of the encryption process.
Given a *ciphertext* c, the decryption process must produce the unique *plaintext* m whose encryption is c.

Let
M: set of all possible plaintexts, $\mathbf{M} \subset \mathbf{Z}$
C: set of all ciphertexts
then
Encryption is a function: $\mathbf{M} \rightarrow \mathbf{Z}$, with range **C**

6.8 Introduction to cryptography

A simple cryptosystem

Assume that the set of all possible plaintexts come from $\mathbf{Z_N}$ for some integer N.

Alice and Bob share a secret number $k \in \mathbf{Z_N}$.

The security of their encryption scheme rests on the assumption that no one besides them knows the number k.

6.8 Introduction to cryptography

A simple cryptosystem

Assume that the set of all possible plaintexts come from $\mathbf{Z}_N$ for some integer N.
Alice and Bob share a secret number $k \in \mathbf{Z}_N$.

The security of their encryption scheme rests on the assumption that no one besides them knows the number *k*.

To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k) \textbf{ mod } N$

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k) \textbf{ mod } N$

6.8 Introduction to cryptography

A simple cryptosystem

Assume that the set of all possible plaintexts come from $\mathbf{Z}_N$ for some integer N.
Alice and Bob share a secret number $k \in \mathbf{Z}_N$.

The security of their encryption scheme rests on the assumption that no one besides them knows the number *k*.

To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k)$ **mod** N

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k)$ **mod** N

Simple encryption scheme requirements:

If $m_1 \neq m_2$ and $m_1, m_2 \in \mathbf{Z}_N$ then $(m_1 + k)$ **mod** N $\neq$ $(m_2 + k)$ **mod** N
(i.e. no two distinct *plaintexts* map to same *ciphertext*)

If $m \in \mathbf{Z}_N$ then (((m + k) **mod** N) - k) mod N = m
(i.e. decryption scheme is inverse of encryption scheme)

6.8 Introduction to cryptography

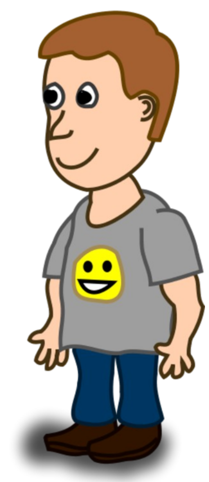
To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k)$ **mod** N

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k)$ **mod** N

Example: let N = 1028

Alice wants to send a “message” 978 to Bob.

Bob



k = 678

Alice

message =
“978”

k = 678

6.8 Introduction to cryptography

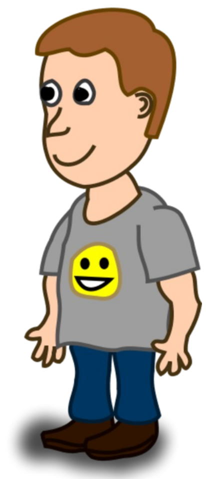
To encrypt a *plaintext* $m \in \mathbf{Z_N}$: compute $c = (m+k)$ **mod** N

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k)$ **mod** N

Example: let N = 1028

Alice wants to send a “message” 978 to Bob.

Bob



k = 678

Alice

k = 678

message = “978”

c = (978+678) mod 1028 = 628

?????
628???

6.8 Introduction to cryptography

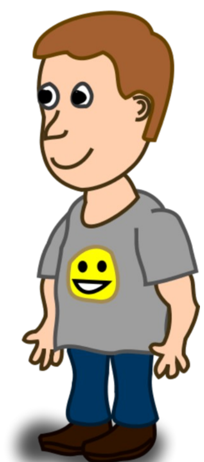
To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k)$ **mod** N

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k)$ **mod** N

Example: let N = 1028

Alice wants to send a “message” 978 to Bob.

Bob



message = “978”

Alice

k = 678

message = “978”

c = (978+678) mod 1028 = 628

?????
628???

M = (628-678) mod 1028 = -50 mod 1028 = 978

k = 678

6.8 Introduction to cryptography

To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k)$ **mod** N

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k)$ **mod** N

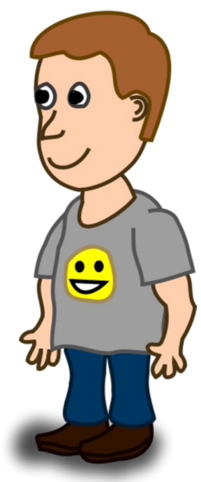
Example: let N = 1028

Alice wants to send a “message” 978 to Bob.

Alice

What is our private key?

Bob



The simple encryption scheme presented here is an example of ***private key*** cryptography. In a private key cryptosystem,

Alice and Bob must meet in advance (or communicate over a reliably secure channel) to decide on the value of a secret key.

6.8 Introduction to cryptography

A simple cryptosystem

Assume that the set of all possible plaintexts come from $\mathbf{Z}_N$ for some integer N.

Alice and Bob share a secret number $k \in \mathbf{Z}_N$.

The security of their encryption scheme rests on the assumption that no one besides them knows the number *k*.

To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k) \textbf{ mod } N$

To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k) \textbf{ mod } N$

The simple cryptosystem described here is not very secure.

1. if Eve can ever get ahold of one *plaintext* and its corresponding *ciphertext*, she can determine *k* and decrypt all further *plaintexts* from Alice to Bob.

6.8 Introduction to cryptography

A simple cryptosystem

Assume that the set of all possible plaintexts come from $\mathbf{Z}_N$ for some integer N.
Alice and Bob share a secret number $k \in \mathbf{Z}_N$.

The security of their encryption scheme rests on the assumption that no one besides them knows the number *k*.

To encrypt a *plaintext* $m \in \mathbf{Z}_N$: compute $c = (m+k)$ **mod** N
To decrypt a *cyphertext* $c \in \mathbf{C}$: compute $m = (c-k)$ **mod** N

The simple cryptosystem described here is not very secure.

2. English text has many well understood patterns.
For example the letters "ing" often occur in sequence but the letters "qx" almost never do. Eve will know something about the pattern of likely messages based on the patterns of English text. If she is allowed to see a large enough number of encrypted messages, she can match the pattern of ciphertexts with the pattern of likely plaintexts and infer k.