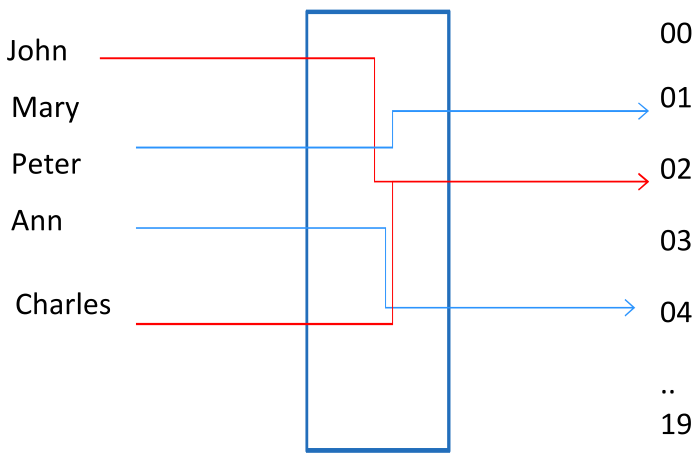
Hash functions

- A ***hash function*** is an algorithm that maps data of arbitrary length to data of afixed length.
- The values returned by a hash function are called **hash values** or **hash codes.**

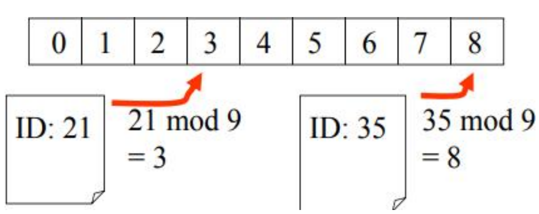
For Example :

Hash function



- **Problem:** Given a large collection of records, how can we store and find a recordquickly?
- **Solution:** Use a hash function calculate the location of the record based on therecord's ID.
- **Example 1:** A common hash function is
  - $h(k) = k$ **mod** m,

where m is the number of available storage locations.



An example of a hash function that maps integers (including verylarge ones) to a subset of integers 0, 1, .. m-1 is:

- **h(k) = k mod m**

Example 2: Assume we have a database of employees, each with a unique ID – a social security number that consists of 8 digits. We want to store the records in a smaller table with m entries. Using h(k) function we can map a social security number in the database of employees to indexes in the table.

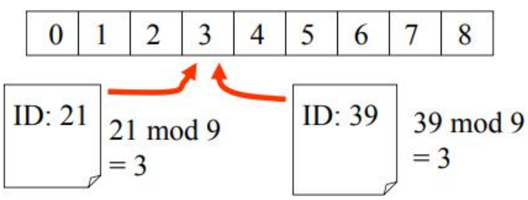
Assume: h(k) = k mod 111

Then:

h(064212848) = 064212848 mod 111 = 14

h(037149212) = 037149212 mod 111 = 65

- **Problem:** two documents mapped to the same location



- **Solution :** move the next available location

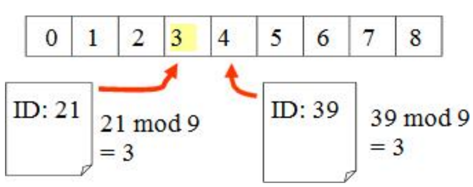
– Method is represented by a sequence of hash functions to

Try

$h_0(k) = k$ **mod** m $h_1(k) = (k+1)$ **mod** m

...

$h_m(k) = (k+m)$ **mod** m



There are many other ways to resolve collisions that are discussed in the references on hashing functions given at the end of the book.

Cryptology

Encryption of messages.

- **Caesar cipher:**
- Shift letters in the message by 3, last three letters mapped to the first 3 letters, e.g. A is shifted to D, X is shifted to A

How to represent the idea of a shift by 3?

- There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order.
- **Coding of letters:**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$
- **Encrypt message:**

– **I LIKE DISCRETE MATH**

– **L 0LNH GLYFUHVH PDVK.**

How to decode the message ?

  - $\mathbf{f^{-1}(p) = (p-3) \bmod 26}$

4.2 Integer Representations and Algorithms

Representations of Integers

- In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 965, we mean
  $965 = 9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.
- We can represent numbers using any base b, where b is a positive integer greater than 1.
- The bases $b = 2$ (*binary*), $b = 8$ (*octal*), and $b = 16$ (*hexadecimal*) are important for computing and communications
- The ancient Mayans used base 20 and the ancient Babylonians used base 60.

Base *b* Representations

- We can use positive integer b greater than 1 as a base

Theorem 1: Let b be a positive integer greater than 1. Then if n isa positive integer, it can be expressed uniquely in the form:

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

where k is a nonnegative integer, $a_0, a_1, \dots a_k$ are nonnegative integers less than b, and $a_k \neq 0$. The a_j, $j = 0,\dots,k$ are called the base-b digits of therepresentation.

- The representation of n given in **Theorem 1** is called the ***base b expansionof n*** and is denoted by $(a_k a_{k-1} \dots a_1 a_0)_b$.

We usually omit the subscript 10 for base 10 expansions.

Binary Expansions

- Most computers represent integers and do arithmetic with binary (base 2) expansions of integers.
- In these expansions,the only digits used are 0 and 1.

Example 1:

What is the decimal expansion of the integer that has$(1\ 01011111)_2$ as its binary expansion?

Solution:

$(1\ 0101\ 1111)_2 = 1\cdot2^8 + 0\cdot2^7 + 1\cdot2^6 + 0\cdot2^5 + 1\cdot2^4 + 1\cdot2^3$

$+ 1\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 = 351.$

Example 2: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?

Solution: $(11011)_2 = 1\cdot2^4 + 1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 1\cdot2^0 = 27$

Octal Expansions

- The octal expansion (base 8) uses the digits {0,1,2,3,4,5,6,7}.

Example 3: What is the decimal expansion of the number with octalexpansion $(7016)_8$?

Solution: $7\cdot8^3 + 0\cdot8^2 + 1\cdot8^1 + 6\cdot8^0 = 3598$

Example 4: What is the decimal expansion of the number with octal expansion $(111)_8$?

Solution: $1\cdot8^2 + 1\cdot8^1 + 1\cdot8^0 = 64 + 8 + 1 = 73$

Hexadecimal Expansions

- The hexadecimal expansion uses 16 digits: {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}.
  - The letters A through F represent the decimal numbers 10 through 15.

Example 5: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution:

$2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = 175627$

Example 6: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?

Solution: $14\cdot16^1 + 5\cdot16^0 = 224 + 5 = 229$

Base Conversion

- To construct the base b expansion of an integer n:
  - Divide n by b to obtain a quotient and remainder.

    $$n = bq_0 + a_0 \quad 0 \le a_0 \le b$$

  - The remainder, a_0 , is the rightmost digit in the base b expansion of n. Next, divide q_0 by $b.q_0$

    $$b.q_0 = bq_1 + a_1 \quad 0 \le a_1 \le b$$

  - The remainder, a_1, is the second digit from the right in the base b expansion of n.
  - Continue by successively dividing the quotients by b, obtaining the additional base b digits as the remainder.
  - The process terminates when the quotient is 0.

Example 7: Find the octal expansion of $(12345)_{10}$

Solution: Successively dividing by 8 gives:

$12345 = 8 \cdot 1543 + 1$

$1543 = 8 \cdot 192 + 7$

$192 = 8 \cdot 24 + 0$

$24 = 8 \cdot 3 + 0$

$3 = 8 \cdot 0 + 3$

– The remainders are the digits from right to left yielding $(30071)_8$.