# Elementary Sorts and Shuffling <br> CS 121: Data Structures 

## START RECORDING

## Attendance Quiz: Hash Tables

- Scan the QR code, or find today's attendance quiz under the "Quizzes" tab on Canvas
- Password: announced in class


| Key | Index <br> (from hash <br> function) | Value |
| :---: | :---: | :---: |
| Act | 0 | 11 |
| Box | 1 | 22 |
| Cat | 1 | 33 |
| Rat | 2 | 44 |

## Attendance Quiz: Hash Tables

- Write your name and the date
- Draw the data structures of hash tables containing the data shown at the right, inserted in the order shown, for:
- A hash table implemented using separate chaining, with room for five chains
- A hash table implemented using linear probing, with room for five keys/values


### 2.1 Elementary Sorts

- rules of the game
- selection sort
- insertion sort
- shellsort
- shuffling
http://algs4.cs.princeton.edu


### 2.1 Elementary Sorts

- rules of the game
- selection sort

Robert Sedgewick I Kevin Wayne

## - insertion sort

, shellsort

- shuffling
http://algs4.cs.princeton.edu


## Sorting problem

## Ex. Student records in a university.

|  | Chen | 3 | A | $991-878-4944$ | 308 Blair |
| :---: | :---: | :---: | :---: | :---: | :---: |
|  | Rohde | 2 | A | $232-343-5555$ | 343 Forbes |
|  | Gazsi | 4 | B | $766-093-9873$ | 101 Brown |
| item | Furia | 1 | A | $766-093-9873$ | 101 Brown |
|  | Kanaga | 3 | B | $898-122-9643$ | 22 Brown |
|  | Andrews | 3 | A | $664-480-0023$ | 097 Little |

Sort. Rearrange array of $N$ items into ascending order.

| Andrews | 3 | A | $664-480-0023$ | 097 Little |
| :---: | :---: | :---: | :---: | :---: |
| Battle | 4 | C | $874-088-1212$ | 121 Whitman |
| Chen | 3 | A | $991-878-4944$ | 308 Blair |
| Furia | 1 | A | $766-093-9873$ | 101 Brown |
| Gazsi | 4 | B | $766-093-9873$ | 101 Brown |
| Kanaga | 3 | B | $898-122-9643$ | 22 Brown |
| Rohde | 2 | A | $232-343-5555$ | 343 Forbes |

## Sorting applications



Library of Congress numbers

contacts

playing cards: shuffling by sorting

...maybe?

## Sample sort client 1

Goal. Sort any type of data.
Ex 1. Sort random real numbers in ascending order.
seems artificial (stay tuned for an application)

```
public class Experiment
{
    pub1ic static void main(String[] args)
    {
        int N = Integer.parseInt(args[0]);
        Double[] a = new Double[N];
        for (int i = 0; i < N; i++)
                a[i] = StdRandom.uniform();
            Insertion.sort(a);
            for (int i = 0; i < N; i++)
            StdOut.println(a[i]);
```

\% java Experiment 10
0.08614716385210452
0.09054270895414829
0.10708746304898642
0.21166190071646818
0.363292849257276
0.460954145685913
0.5340026311350087
0.7216129793703496
0.9003500354411443
0.9293994908845686

## Sample sort client 2

Goal. Sort any type of data.
Ex 2. Sort strings in alphabetical order.

```
public class StringSorter
{
    public static void main(String[] args)
    {
        String[] a = StdIn.readA11Strings();
        Insertion.sort(a);
        for (int i = 0; i < a.length; i++)
            StdOut.println(a[i]);
    }
}
% more words3.txt
bed bug dad yet zoo ... all bad yes
    % java StringSorter < words3.txt
    a11 bad bed bug dad ... yes yet zoo
    [suppressing newlines]
```


## Sample sort client 3

Goal. Sort any type of data.
Ex 3. Sort the files in a given directory by filename.

```
import java.io.File;
public class FileSorter
{
    public static void main(String[] args)
    {
        File directory = new File(args[0]);
        File[] files = directory.listFiles();
        Insertion.sort(files);
        for (int i = 0; i < files.length; i++)
        StdOut.println(files[i].getName());
    }
}
```

```
% java FileSorter .
Insertion.class
Insertion.java
InsertionX.class
InsertionX.java
Selection.class
Selection.java
She11.class
She11.java
She11X.class
She11X.java
```


## Total order

Goal. Sort any type of data (for which sorting is well defined).

A total order is a binary relation $\leq$ that satisfies:

- Antisymmetry: if both $v \leq w$ and $w \leq v$, then $v=w$.
- Transitivity: if both $v \leq w$ and $w \leq x$, then $v \leq x$.
- Totality: either $v \leq w$ or $w \leq v$ or both.

Ex.

- Standard order for natural and real numbers.
- Chronological order for dates or times.
- Alphabetical order for strings.

No transitivity. Rock-paper-scissors.
No totality. Course prerequisites.

violates transitivity

violates totality

## Callbacks

Goal. Sort any type of data (for which sorting is well defined).
Q. How can sort() know how to compare data of type Double, String, and java.io. File without any information about the type of an item's key?

Callback $=$ reference to executable code.

- Client passes array of objects to sort() function.
- The sort() function calls object's compareTo() method as needed.

Implementing callbacks.

- Java: interfaces.
- C: function pointers.
- C++: class-type functors.
- C\#: delegates.
- Python, Perl, ML, Javascript: first-class functions.


## Callbacks: roadmap

```
client
client
```

```
public class StringSorter
```

public class StringSorter
{
{
public static void main(String[] args)
public static void main(String[] args)
{
{
String[] a = StdIn.readAl1Strings();
String[] a = StdIn.readAl1Strings();
Insertion.sort(a);
Insertion.sort(a);
for (int i = 0; i < a.length; i++)
for (int i = 0; i < a.length; i++)
StdOut.println(a[i]);
StdOut.println(a[i]);
}
}
}

```
}
```


## data-type implementation

```
public class String
implements Comparable<String>
{
    public int compareTo(String b)
    {
        return -1;
        ...
        return +1;
        return 0;
    }
}
```

Comparable interface (built in to Java)

```
public interface Comparable<Item>
{
    public int compareTo(Item that);
}
```

sort implementation

```
public static void sort(Comparable[] a)
{
    int N = a.length;
    for (int i = 0; i < N; i++)
        for (int j = i; j > 0; j--)
        if (a[j].compareTo(a[j-1]) < 0)
        exch(a, j, j-1);
        else break;
}
```


## Comparable API

## Implement compareTo() so that v.compareTo(w)

- Defines a total order.
- Returns a negative integer, zero, or positive integer if $v$ is less than, equal to, or greater than $w$, respectively.
- Throws an exception if incompatible types (or either is null).

less than (return -1)

equal to (return 0)

greater than (return +1 )

Built-in comparable types. Integer, Double, String, Date, File, ...
User-defined comparable types. Implement the Comparable interface.

## Implementing the Comparable interface

Date data type. Simplified version of java.util. Date.

```
public class Date implements Comparable<Date>
{
    private final int month, day, year;
    public Date(int m, int d, int y)
    {
        month = m;
        day = d;
        year = y;
    }
    public int compareTo(Date that)
    {
        if (this.year < that.year ) return -1;
        if (this.year > that.year ) return +1;
        if (this.month < that.month) return -1;
        if (this.month > that.month) return +1;
        if (this.day < that.day ) return -1;
        if (this.day > that.day ) return +1;
        return 0;
    }
}
```


### 2.1 Elementary Sorts

- rules of the game
- selection sort


## Selection sort demo

- In iteration i, find index min of smallest remaining entry.
- Swap a[i] and a[min].

initial


## Selection sort

Algorithm. $\uparrow$ scans from left to right.

Invariants.

- Entries the left of $\uparrow$ (including $\uparrow$ ) fixed and in ascending order.
- No entry to right of $\uparrow$ is smaller than any entry to the left of $\uparrow$.



## Two useful sorting abstractions

Helper functions. Refer to data through compares and exchanges.

Less. Is item v less than w?

```
private static boolean less(Comparable v, Comparable w)
{ return v.compareTo(w) < 0; }
```

Exchange. Swap item in array a[] at index $i$ with the one at index $j$.

```
private static void exch(Comparable[] a, int i, int j)
{
    Comparable swap = a[i];
    a[i] = a[j];
    a[j] = swap;
}
```


## Selection sort inner loop

To maintain algorithm invariants:

- Move the pointer to the right.

$$
i++
$$

- Identify index of minimum entry on right.

```
int min = i;
for (int j = i+1; j < N; j++)
    if (less(a[j], a[min]))
        min = j;
```

- Exchange into position.

```
exch(a, i, min);
```



## Selection sort: Java implementation

```
public class Selection
{
    public static void sort(Comparable[] a)
    {
        int N = a.length;
        for (int i = 0; i < N; i++)
        {
            int min = i;
            for (int j = i+1; j < N; j++)
                if (less(a[j], a[min]))
                        min = j;
            exch(a, i, min);
        }
    }
    private static boolean less(Comparable v, Comparable w)
    { /* as before */ }
    private static void exch(Comparable[] a, int i, int j)
    { /* as before */ }
}
```


## Selection sort: animations



A algorithm position

$\square$in final order not in final order

[^0]
## Selection sort: mathematical analysis

Proposition. Selection sort uses $(N-1)+(N-2)+\ldots+1+0 \sim N^{2} / 2$ compares and $N$ exchanges.


Trace of selection sort (array contents just after each exchange)

Running time insensitive to input. Quadratic time, even if input is sorted. Data movement is minimal. Linear number of exchanges.

### 2.1 Elementary Sorts

-rules of the game

- selection sort
- insertion sort
- shellsort
- shuffling
http://algs4.cs.princeton.edu
- In iteration i, swap a[i] with each larger entry to its left.



## Insertion sort

Algorithm. $\uparrow$ scans from left to right.

Invariants.

- Entries to the left of $\uparrow$ (including $\uparrow$ ) are in ascending order.
- Entries to the right of $\uparrow$ have not yet been seen.



## Insertion sort inner loop

To maintain algorithm invariants:

- Move the pointer to the right.

```
i++;
```



- Moving from right to left, exchange a[i] with each larger entry to its left.

```
for (int j = i; j > 0; j--)
    if (less(a[j], a[j-1]))
        exch(a, j, j-1);
    else break;
```



```
public class Insertion
{
    public static void sort(Comparable[] a)
    {
        int N = a.length;
        for (int i = 0; i < N; i++)
            for (int j = i; j > 0; j--)
                if (less(a[j], a[j-1]))
                exch(a, j, j-1);
            else break;
    }
    private static boolean less(Comparable v, Comparable w)
    { /* as before */ }
    private static void exch(Comparable[] a, int i, int j)
    { /* as before */ }
}
```


## Insertion sort: animations



A algorithm position

in final order
not in final order
http://www.sorting-algorithms.com/insertion-sort

## Insertion sort: mathematical analysis

Proposition. To sort a randomly-ordered array with distinct keys, insertion sort uses $\sim 1 / 4 N^{2}$ compares and $\sim 1 / 4 N^{2}$ exchanges on average.

Pf. Expect each entry to move halfway back.

| a[] |  |  |  |  |  |  |  |  |  |  |  |  | entries in gray do not move |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| i | j | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |  |
|  |  | S | 0 | R | T | E | X | A | M | P | L | E |  |
| 1 | 0 | 0 | S | R | T | E | X | A | M | P | L | E |  |
| 2 | 1 | 0 | R | S | T | E | X | A | M | P | L | E | entry in red is a[j] |
| 3 | 3 | 0 | R | S | T | E | X | A | M | P | L | E |  |
| 4 | 0 | E | 0 | R | S | T | X | A | M | P | L | E |  |
| 5 | 5 | E | 0 | R | S | T | X | A | M | P | L | E |  |
| 6 | 0 | A | E | 0 | R | S | T | X | M | P | L | E | entries in black moved one position right for insertion |
| 7 | 2 | A | E | M | 0 | R | S | T | X | P | L | E |  |
| 8 | 4 | A | E | M | 0 | P | R | S | T | X | L |  |  |
| 9 | 2 | A | E | L | M | 0 | P | R | S | T | X |  |  |
| 10 | 2 | A | E | E | L | M | 0 | P | R | S | T | X |  |
|  |  | A | E | E | L | M | 0 | P | R | S | T | X |  |

Trace of insertion sort (array contents just after each insertion)

## Insertion sort: trace

a[]



## Insertion sort: analysis

Best case. If the array is in ascending order, insertion sort makes $N-1$ compares and 0 exchanges.
A E E L M O PR S TX

Worst case. If the array is in descending order (and no duplicates), insertion sort makes $\sim 1 / 2 N^{2}$ compares and $\sim 1 / 2 N^{2}$ exchanges.
X T S R P OMLFEA

### 2.1 Elementary Sorts

-rules of the game

- selection sort


## Algorithms

Robert Sedgewick I Kevin Wayne

- insertion sort
- shellsort
- shuffling
http://algs4.cs.princeton.edu


## Shellsort overview

Idea. Move entries more than one position at a time by $h$-sorting the array.
an $h$-sorted array is $h$ interleaved sorted subsequences


Shellsort. [Shell 1959] $h$-sort array for decreasing sequence of values of $h$.

| input | S | H | E | L | L | S | 0 | $R$ | T | E | X | A | $M$ | $P$ | $L$ | $E$ |
| :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- | :--- |
| 13-sort | P | H | E | L | L | S | 0 | R | T | E | X | A | M | S | L | E |
| 4-sort | L | E | E | A | M | H | L | E | P | S | 0 | L | T | S | X | R |
| 1-sort | A | E | E | E | H | L | L | L | M | 0 | P | R | S | S | T | X |

## h-sorting demo

In iteration i, swap a[i] with each larger entry h positions to its left.


## h-sorting

How to $h$-sort an array? Insertion sort, with stride length $h$.


Why insertion sort?

- Big increments $\Rightarrow$ small subarray.
- Small increments $\Rightarrow$ nearly in order. [stay tuned]

Shellsort example: increments 7, 3, 1

| input |  |  |  |  |  |  |  |  |  |  |  | ort |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| S | 0 | R | T | E | X | A | M | P | L | E | A | E | L | E | 0 | P | M | S | X | R | T |
|  |  |  |  |  |  |  |  |  |  |  | A | E | L | E | 0 | P | M | S | X | R | T |
|  |  |  |  |  |  |  |  |  |  |  | A | E | L | E | 0 | P | M | S | X | R | T |
| 7-so |  |  |  |  |  |  |  |  |  |  | A | E | E | L | 0 | P | M | 5 | X | R | T |
| S | 0 | R | T | E | X | A | M | P | L | E | A | E | E | L | 0 | P | M | S | X | R | T |
| M | 0 | R | T | E | X | A | S | P | L | E | A | E | E | L | 0 | P | M | S | X | R | T |
| M | 0 | R | T | E | $x$ | A | S | P | L | E | A | E | E | L | M | 0 | P | 5 | X | R | T |
| M | 0 | L | T | E | X | A | S | P | R | E | A | E | E | L | M | 0 | P | S | X | R | T |
| M | 0 | L | E | E | X | A | S | P | R | T | A | E | E | L | M | 0 | P | S | X | R | T |
|  |  |  |  |  |  |  |  |  |  |  | A | E | E | L | M | 0 | P | R | S | X | T |
| 3-so |  |  |  |  |  |  |  |  |  |  | A | E | E | L | M | 0 | P | R | S | T | X |
| M | 0 | L | E | E | X | A | S | P | R | T |  |  |  |  |  |  |  |  |  |  |  |
| E | 0 | L | M | E | X | A | S | P | R | T |  |  |  |  |  |  |  |  |  |  |  |
| E | E | L | M | 0 | X | A | S | P | R | T | res |  |  |  |  |  |  |  |  |  |  |
| E | E | L | M | 0 | X | A | S | P | R | T | A | E | E | L | M | 0 | P | R | S | T | X |
| A | E | L | E | 0 | X | M | S | P | R | T |  |  |  |  |  |  |  |  |  |  |  |
| A | E | L | E | 0 | X | M | S | P | R | T |  |  |  |  |  |  |  |  |  |  |  |
| A | E | L | E | 0 | P | M | S | X | R | T |  |  |  |  |  |  |  |  |  |  |  |
| A | E | L | E | 0 | P | M | S | X | R | T |  |  |  |  |  |  |  |  |  |  |  |
| A | E | L | E | 0 | P | M | S | X | R | T |  |  |  |  |  |  |  |  |  |  |  |

## Shellsort: Java implementation

```
public class Shell
{
    pub1ic static void sort(Comparable[] a)
    {
        int N = a.length;
        int h = 1; < < 3x+1 increment
        while (h < N/3) h = 3*h + 1; // 1, 4, 13, 40, 121, 364, ..\longleftarrow% sequence
        while (h >= 1)
        { // h-sort the array.
            for (int i = h; i < N; i++)
            {
                for (int j = i; j >= h && less(a[j], a[j-h]); j -= h)
                exch(a, j, j-h);
            }
                h = h/3;
        }
    }
    private static boolean less(Comparable v, Comparable w)
    { /* as before */ }
    private static void exch(Comparab7e[] a, int i, int j)
    { /* as before */ }
}

\section*{Shellsort: visual trace}
input


40-sorted

\section*{}

13-sorted

4-sorted

result

\section*{Shellsort: animations}
\begin{tabular}{|c|c|c|c|c|}
\hline \multirow{4}{*}{Play All} & \multirow[t]{4}{*}{Random
\(\square\)} & Nearly Sorted & Reversed & Few Unique \\
\hline & & & & \(\overline{\overline{\underline{\#}}}\) \\
\hline & & & ] &  \\
\hline & & & & \\
\hline
\end{tabular}

A algorithm position
h-sorted
current subsequence
other elements
http://www.sorting-a1gorithms.com/she11-sort

Shellsort: which increment sequence to use?

Powers of two. \(1,2,4,8,16,32, \ldots\)
No.

Powers of two minus one. \(1,3,7,15,31,63, \ldots\)
Maybe.
\(\rightarrow 3 x+1.1,4,13,40,121,364, \ldots\)
OK. Easy to compute.

Sedgewick. 1, 5, 19, 41, 109, 209, 505, 929, \(2161,3905, \ldots\)
Good. Tough to beat in empirical studies.
```

merging of (9\times4i) - (9 < 2i) +1
and 4i- (3 < 2i) +1

```

\section*{Shellsort: intuition}

Proposition. An \(h\)-sorted array remains \(h\)-sorted after \(g\)-sorting it.


Challenge. Prove this fact-it's more subtle than you'd think!

Shellsort: analysis

Proposition. The order of growth of the worst-case number of compares used by shellsort with the \(3 \mathrm{x}+1\) increments is \(N^{3 / 2}\).

Property. The expected number of compares to shellsort a randomlyordered array using \(3 x+1\) increments is....
\begin{tabular}{|c|c|c|c|c|}
\hline\(N\) & compares & \(2.5 \mathrm{~N} \ln \mathrm{~N}\) & \(0.25 \mathrm{~N} \mathrm{In}^{2} \mathrm{~N}\) & N 1.3 \\
\hline 5,000 & 93 K & 106 K & \(\mathbf{9 1 K}\) & 64 K \\
\hline 10,000 & 209 K & 230 K & \(\mathbf{2 1 3 K}\) & 158 K \\
\hline 20,000 & 467 K & 495 K & \(\mathbf{4 9 0 K}\) & 390 K \\
\hline 40,000 & 1022 K & \(\mathbf{1 0 5 9 K}\) & 1122 K & 960 K \\
\hline 80,000 & 2266 K & \(\mathbf{2 2 5 8 K}\) & 2549 K & 2366 K \\
\hline
\end{tabular}

Remark. Accurate model has not yet been discovered (!)

\section*{Why are we interested in shellsort?}

Example of simple idea leading to substantial performance gains.

Useful in practice.
- Fast unless array size is huge (used for small subarrays).
- Tiny, fixed footprint for code (used in some embedded systems).
- Hardware sort prototype.

R, bzip2, /linux/kernel/groups.c

Simple algorithm, nontrivial performance, interesting questions.
- Asymptotic growth rate?
- Best sequence of increments? \(\longleftarrow\) open problem: find a better increment sequence
- Average-case performance?

Lesson. Some good algorithms are still waiting discovery.

\section*{Elementary sorts summary}

Today. Elementary sorting algorithms.
\begin{tabular}{|c|c|c|c|}
\hline algorithm & best & average & worst \\
\hline selection sort & \(N^{2}\) & \(N^{2}\) & \(N^{2}\) \\
\hline insertion sort & \(N\) & \(N^{2}\) & \(N^{2}\) \\
\hline Shellsort (3x+1) & \(N \log N\) & \(?\) & \(N^{3 / 2}\) \\
\hline goal & \(N\) & \(N \log N\) & \(N \log N\) \\
\hline
\end{tabular}
order of growth of running time to sort an array of \(\mathbf{N}\) items

Next time. \(N \log N\) sorting algorithms (in worst case).

\section*{Shuffling Disclaimer}
- The shuffling we will talk about today is very different than the shuffling described in the homework
- In the homework, we use "in-shuffles" and "outshuffles," which do not incorporate randomness
- In this lecture, we will talk about randomizing the order of a deck, which does incorporate randomness

\subsection*{2.1 Elementary Sorts}
-rules of the game
- selection sort

Algorithms

Robert Sedgewick | Kevin Wayne
- insertion sort
- shellsort
- shuffling

How to shuffle an array
Goal. Rearrange array so that result is a uniformly random permutation. all permutations equally likely

How to shuffle an array
Goal. Rearrange array so that result is a uniformly random permutation. all permutations equally likely


\section*{Shuffle sort}
- Generate a random real number for each array entry.
- Sort the array.
columns in a spreadsheet
\begin{tabular}{|c|c|c|c|c|c|c|c|c|}
\hline  & \begin{tabular}{|cc|}
\hline 3 & \(\%\) \\
\hline \multirow{2}{*}{} \\
& \(\%\) \\
& \(\%\) \\
\hline
\end{tabular} &  & \begin{tabular}{|cc|}
\hline \(5 \%\) & \(\%\) \\
\(\%\) & \\
\(\%\) & \(\%\) \\
\hline
\end{tabular} & \[
\begin{array}{|cc|}
\hline 6 \% & \% \\
\% & \% \\
\% & \psi_{9}^{+} \\
\hline
\end{array}
\] &  &  &  & \[
10 \mathrm{Cog}
\] \\
\hline & & & & & 0.48 & 0.141 & 0.42 & \\
\hline
\end{tabular}

\section*{Shuffle sort}
- Generate a random real number for each array entry.
- Sort the array.
\useful for shuffling
columns in a spreadsheet
\begin{tabular}{|c|c|c|c|c|c|c|c|c|}
\hline  & \[
\begin{array}{|cc|}
\hline 6 \Leftrightarrow & \% \\
\% & \% \\
\% & \% \\
\hline
\end{array}
\] &  &  &  &  &  & \begin{tabular}{|cc|}
\hline \(5 \%\) & \(\%\) \\
\hline\(\%\) & \\
\(\%\) & \\
\(\%\) & \(\%\) \\
\hline
\end{tabular} & \begin{tabular}{|lll|}
\hline 3 & \(\%\) \\
\hline
\end{tabular} \\
\hline . 14 & 0.1576 & 0.4218 & 0.4854 & 0.8003 & 0.9157 & 0.9572 & 0.9649 & 0.97 \\
\hline
\end{tabular}

\section*{Shuffle sort}
- Generate a random real number for each array entry.
- Sort the array.
useful for shuffling
columns in a spreadsheet


Proposition. Shuffle sort produces a uniformly random permutation.

\section*{War story (Microsoft)}

\title{
Microsoft antitrust probe by EU. Microsoft agreed to provide a randomized ballot screen for users to select browser in Windows 7.
}
http://www.browserchoice.eu

\section*{Select your web browser(s)}

A fast new browser from Google. Try it now!

\section*{Safari}

Safari for Windows from Apple, the world's most innovative browser.

Your online security is Firefox's top priority. Firefox is free, and made to help you get the most out of the

The fastest browser on Earth. Secure, powerful and easy to use, with excellent privacy protection.

Designed to help you take control of your privacy and browse with confidence. Free from Microsoft.

appeared last
50\% of the time

\section*{War story (Microsoft)}

Microsoft antitrust probe by EU. Microsoft agreed to provide a randomized ballot screen for users to select browser in Windows 7.

Solution? Implement shuffle sort by making comparator always return a random answer.

Problem: Breaks reflexivity, antisymmetry, and transitivity!
```

public int compareTo(Browser that)
{
double r = Math.random();
if (r < 0.5) return -1;
if (r > 0.5) return +1;
return 0;
}

```

Knuth shuffle demo
- In iteration i, pick integer r between 0 and i uniformly at random.
- Swap a[i] and a[r].


\section*{Knuth shuffle}
- In iteration i, pick integer r between 0 and i uniformly at random.
- Swap a[i] and a[r].


Proposition. [Fisher-Yates 1938] Knuth shuffling algorithm produces a uniformly random permutation of the input array in linear time.

\section*{Knuth shuffle}
- In iteration i, pick integer r between 0 and i uniformly at random.
- Swap a[i] and a[r].
common bug: between 0 and \(\mathrm{N}-1\) correct variant: between i and N - 1
```

public class StdRandom
{
public static void shuffle(Object[] a)
{
int N = a.length;
for (int i = 0; i < N; i++)
{
int r = StdRandom.uniform(i + 1);
exch(a, i, r);
}
}
}

```

\section*{Broken Knuth shuffle}
Q. What happens if integer is chosen between 0 and \(N-1\) ?
A. Not uniformly random!
\begin{tabular}{|c|c|c|}
\hline permutation & Knuth shuffle & broken shuffle \\
\hline A B C & \(1 / 6\) & \(4 / 27\) \\
\hline A C B & \(1 / 6\) & \(5 / 27\) \\
\hline B A C & \(1 / 6\) & \(5 / 27\) \\
\hline B C A & \(1 / 6\) & \(5 / 27\) \\
\hline C A B & \(1 / 6\) & \(4 / 27\) \\
\hline C B A & \(4 / 27\) \\
\hline
\end{tabular}

\section*{War story (online poker)}

Texas hold'em poker. Software must shuffle electronic cards.


How We Learned to Cheat at Online Poker: A Study in Software Security http://www.datamation.com/entdev/article.php/616221

\section*{War story (online poker)}

Shuffling algorithm in FAQ at www.planetpoker.com
```

for i := 1 to 52 do begin
r := random(51) + 1; « between 1 and 51
swap := card[r];
card[r] := card[i];
card[i] := swap;
end;

```

Bug 1. Random number \(r\) never \(52 \Rightarrow 52^{\text {nd }}\) card can't end up in \(52^{\text {nd }}\) place.
Bug 2. Shuffle not uniform (should be between 1 and i).
Bug 3. random() uses 32 -bit seed \(\Rightarrow 2^{32}\) possible shuffles.
Bug 4. Seed \(=\) milliseconds since midnight \(\Rightarrow 86.4\) million shuffles.
" The generation of random numbers is too important to be left to chance.
- Robert R. Coveyou

\section*{War story (online poker)}

Best practices for shuffling (if your business depends on it).
- Use a hardware random-number generator that has passed both the FIPS 140-2 and the NIST statistical test suites.
- Continuously monitor statistic properties: hardware random-number generators are fragile and fail silently.
- Use an unbiased shuffling algorithm.


RANDOM.ORG

\section*{War story (online poker)}

\section*{Best practices for shuffling (when programming).}
- Are there security concerns?
- Use your language's secure random number generation capabilities
- SecureRandom in Java
- secrets in Python
- Otherwise, pseudorandom numbers might be acceptable
- Random in Java
- random in Python
- When possible, use well-vetted libraries to perform shuffles, etc.

Bottom line. Shuffling a deck of cards is hard!```


[^0]:    http://www.sorting-algorithms.com/selection-sort

