# CSC165 fall 2019

rooted trees / what's next

Danny Heap csc165-2019-09@cs.toronto.edu BA4270 (behind elevators) Web page: http://www.teach.cs.toronto.edu/~heap/165/F19/

Using Course notes: trees

(日)、(四)、(日)、(日)、

æ

### distinguish a root

add notions of distance, hierarchy/direction to trees by

rooted tree: a tree with

exactly one vertex labelled (distinguished) as root, if the tree has at least one vertex

 OR no vertices (a convenience for proofs and algorithms)

(日)、(四)、(日)、(日)、

ъ











- arity (branching factor)
- height, denote as height(G)

ience Y OF TORONTO

æ

<ロト <四ト <注入 < モト

- every rooted tree with  $n \ge 2$  vertices has height at least 2
- ▶ some rooted tree with  $n \ge 2$  vertices has height exactly 2
- every rooted tree with n vertices has height no more than n

(日)、

ъ

 $\blacktriangleright$  some rooted tree with *n* vertices has height exactly *n* 

#### binary rooted trees

maximum degree  $3 \equiv$  maximum of 2 children  $\forall h \in \mathbb{N}, \forall G = (V, E) (G \text{ rooted, binary tree } \land height(G) \leq h) \Rightarrow |V| \leq 2^{h} - 1$ 



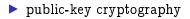
### later topics...

prove correctness

analyze recursive runtime

computability

intractability





## problem with keys... e.g. Vigenere cipher



key: thewalrusandthecarpenter
cleartext: ifsevenmaidswithsevenmopssweptforhalfayear

NIVERSITY OF TORONTO

イロト 不得下 イヨト イヨト

if seven maids with seven mops swept for half a year the walr us and the carpenter the walr us and the car

how do you securely exchange keys?

# public/private

share public key with the world keep private key secret

allows:

authentication

encryption



#### RSA

need: text $\rightarrow$ integer, integer $\rightarrow$ text reversible padding scheme

- 1. randomly choose large primes p and q
- 2. n = pq (key length is n in bits...)

3. 
$$L = (p - 1)(q - 1)$$

- 4. choose 1 < e < L so that gcd(e, L) = 1
- 5. compute inverse,  $d \equiv e^{-1} \pmod{L}$ , i.e.  $de \equiv 1 \pmod{L}$ (notes Example 2.19 works for co-prime!)

(日)、(四)、(日)、(日)、

```
publish: e, n
keep private d, p, q, L.
m = \text{text} \rightarrow \text{integer}(\text{message})
encrypt: c \equiv m^e \pmod{n}
decrypt: message = integer \rightarrow \text{text}(c^d) \pmod{n}
```

#### it works... how? Use results from this course... mostly

▲日 → ▲圖 → ▲ 画 → ▲ 画 →

E 990

• (problem set #2, Q2(a)):  $m^{ed} \equiv m \pmod{pq} \equiv m \pmod{n}$ .

#### Notes

