Digital Signature Schemes:

Finding your best fit.

Andrea M. Stojanovski

Goal:

- Create a question and answer interface to help a user pick a scheme for a specific primitive

Primitive: Digital Signature Scheme

Schemes:

1. Hashed RSA
2. Schnorr
3. DSA
4. EC DSA
5. Tree-based Lamport
6. El-gamal
7. DSS

How to pick a Digital Signature Scheme?

Choice criteria → Digital Signature schemes ↓	Security Assumption	Runtime	Key and signature size	Quantum computing safety
Hashed RSA	RSA + Random oracle	Efficient	Short	Not safe
Schnorr	DL	Efficient	Short	Safe
DSA	Related to DL over Zp	Efficient	Short	Not safe
EC DSA	Related to DL over EC	Very efficient	Very short	Not safe
Tree-based Lamport	One-way Hash Function	Very efficient	Very short	Not safe
El-gamal	Related to DL over EC	Less efficient	Short	Not safe
DSS	Related to DSA	Efficient	Very short	Not safe

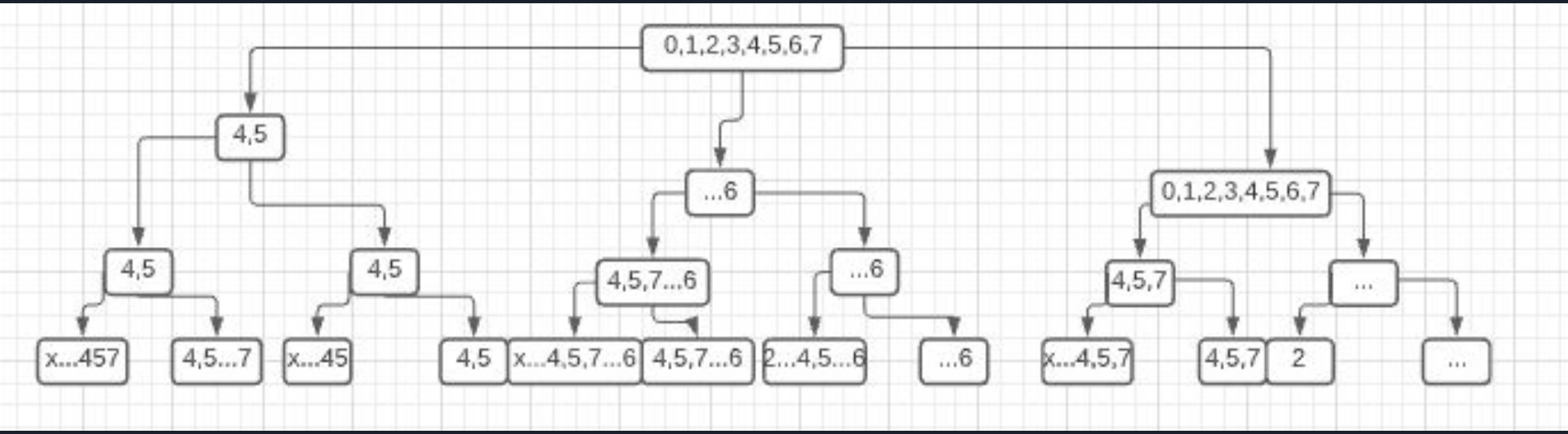
Designing questions:

- Criteria:
  - Security Assumptions
  - Runtime
  - Key and signature size
  - Quantum computing safety

Questions:

```python
def q1():
    print("Importance of runtime efficiency of scheme:")
    print("A. Not important / Unsure")
    print("B. Important")
    print("C. Very important")
    runtime = input()
    return runtime

def q2():
    # ask about key and signature length
    print("Select importance of short key and signature length:")
    print("A. Important")
    print("B. Not a priority / Unsure")
    keyandsig = input()
    return keyandsig

def q3():
    print("Importance of quantum computing safety:")
    print("A. Important")
    print("B. Not important / Unsure")
    quantum = input()
    return quantum
```

Score tree:



Not a decision tree

Scoring:

Python dictionaries:

- Mutable
- Sort

```
schemes = {  # dictionary of schemes
    "Hashed RSA": 0,
    "Schnorr": 0,
    "DSA": 0,
    "EC DSA": 0,
    "Tree-based Lamport": 0,
    "El-Gamal": 0,
    "DSS": 0,
    "ED DSA": 0}
```

Certain questions would warrant 2 points (ex: efficiency)

Ex:

```
Information on security assumptions of Digital Signature Schemes:
Hashed RSA: RSA + Random oracle
Schnorr: DL
DSA: Related to DL over ZP
EC DSA: Related to DL over EC
Tree-based Lamport: One-way Hash Functions
El-gamal: Related to Dl over EC
DSS:
Importance of runtime efficiency of scheme:
A. Not important / Unsure
B. Important
C. Very important
A
Select importance of short key and signature length:
A. Important
B. Not a priority / Unsure
A
Importance of quantum computing safety:
A. Important
B. Not important / Unsure
B
Two matches were found!
EC DSA or Tree-based Lamport best fit the given specifications
Alternative options include (in order of most preferred):
DSS Hashed RSA Schnorr DSA El-Gamal

Process finished with exit code 0
```

Ex:

```
Information on security assumptions of Digital Signature Schemes:
Hashed RSA: RSA + Random oracle
Schnorr: DL
DSA: Related to DL over ZP
EC DSA: Related to DL over EC
Tree-based Lamport: One-way Hash Functions
El-gamal: Related to Dl over EC
DSS:
Importance of runtime efficiency of scheme:
A. Not important / Unsure
B. Important
C. Very important
A
Select importance of short key and signature length:
A. Important
B. Not a priority / Unsure
A
Importance of quantum computing safety:
A. Important
B. Not important / Unsure
B
Two matches were found!
EC DSA or Tree-based Lamport best fit the given specifications
Alternative options include (in order of most preferred):
DSS Hashed RSA Schnorr DSA El-Gamal

Process finished with exit code 0
```

Ex:

```
Information on security assumptions of Digital Signature Schemes:
Hashed RSA: RSA + Random oracle
Schnorr: DL
DSA: Related to DL over ZP
EC DSA: Related to DL over EC
Tree-based Lamport: One-way Hash Functions
El-gamal: Related to Dl over EC
DSS:
Importance of runtime efficiency of scheme:
A. Not important / Unsure
B. Important
C. Very important
A
Select importance of short key and signature length:
A. Important
B. Not a priority / Unsure
A
Importance of quantum computing safety:
A. Important
B. Not important / Unsure
A
None of the schemes fit your exact specifications.
Alternative options include (in order of most preferred):
EC DSA Tree-based Lamport DSS Hashed RSA Schnorr DSA El-Gamal

Process finished with exit code 0
```

Ex:

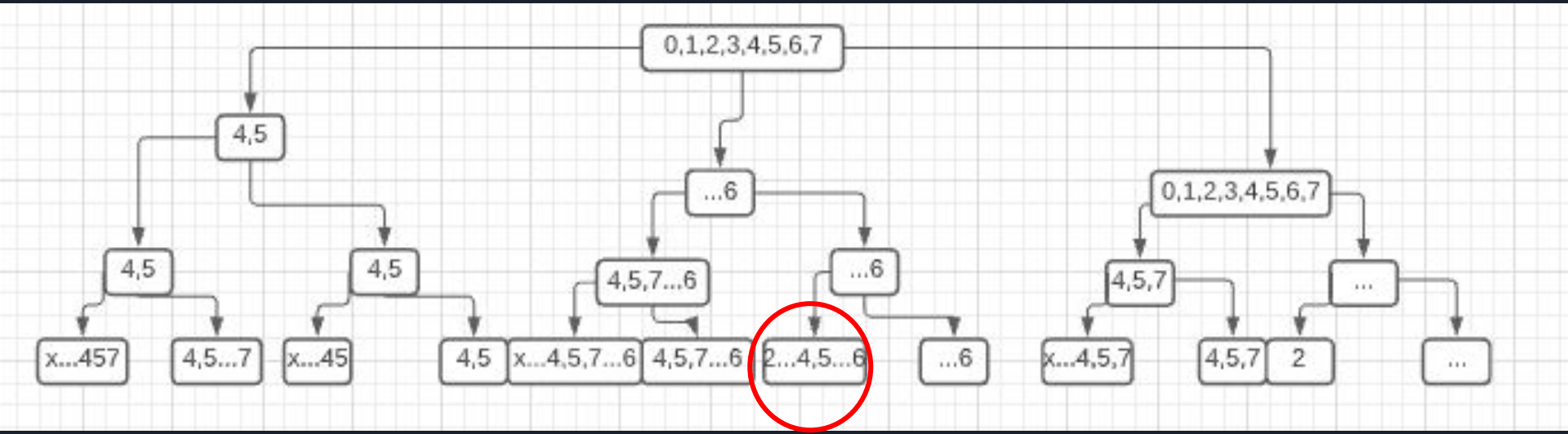
```
Information on security assumptions of Digital Signature Schemes:
Hashed RSA: RSA + Random oracle
Schnorr: DL
DSA: Related to DL over ZP
EC DSA: Related to DL over EC
Tree-based Lamport: One-way Hash Functions
El-gamal: Related to Dl over EC
DSS:
Importance of runtime efficiency of scheme:
A. Not important / Unsure
B. Important
C. Very important
A
Select importance of short key and signature length:
A. Important
B. Not a priority / Unsure
A
Importance of quantum computing safety:
A. Important
B. Not important / Unsure
A
None of the schemes fit your exact specifications.
Alternative options include (in order of most preferred):
EC DSA Tree-based Lamport DSS Hashed RSA Schnorr DSA El-Gamal

Process finished with exit code 0
```

Evaluation:

- All questions must be answered to receive an answer
- Users are provided with a list (in order) of alternatives
  - Alternatives will not satisfy all criteria (or be as “perfect”)

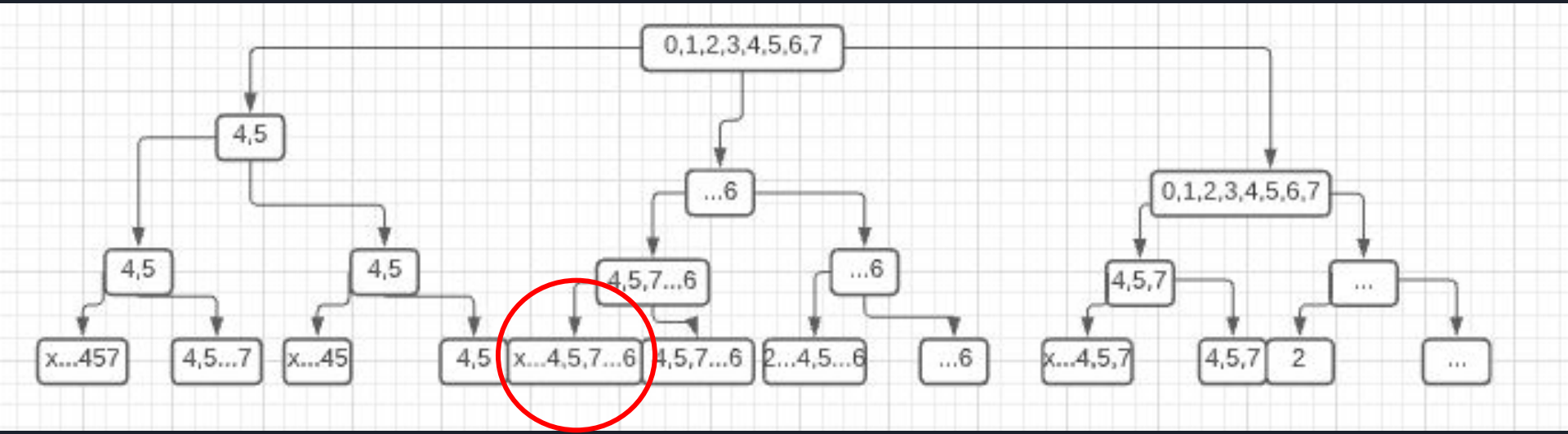
- Suggestions are not random
  - Order is intentional and then lists the remaining items (see in tree)

Score tree:



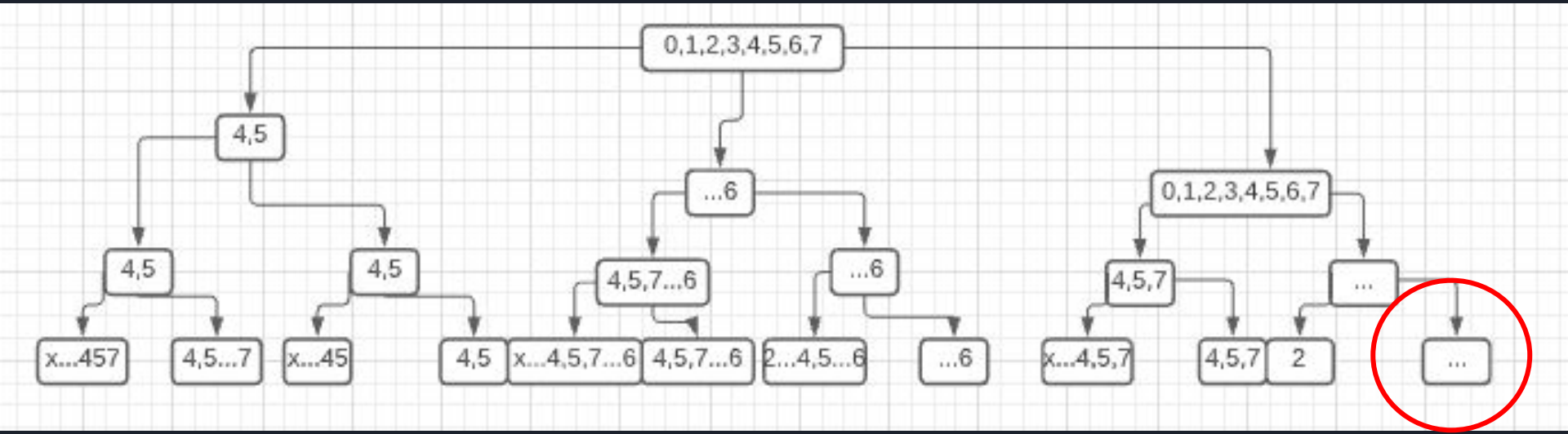
Not a decision tree

Score tree:



Not a decision tree

Score tree:



Not a decision tree

Alternative approaches / Improvements

- Machine learning:
  - Creating data set of criteria and selected scheme
  - Graph answers to show data (allows user to more easily see data)
- No decision tree to not eliminate too many options
- Create more questions (?)
- Allow users to “hard” select answers
  - This make recommendations that are not “perfect” based on answer, however provides “best” and “next best” recommendations