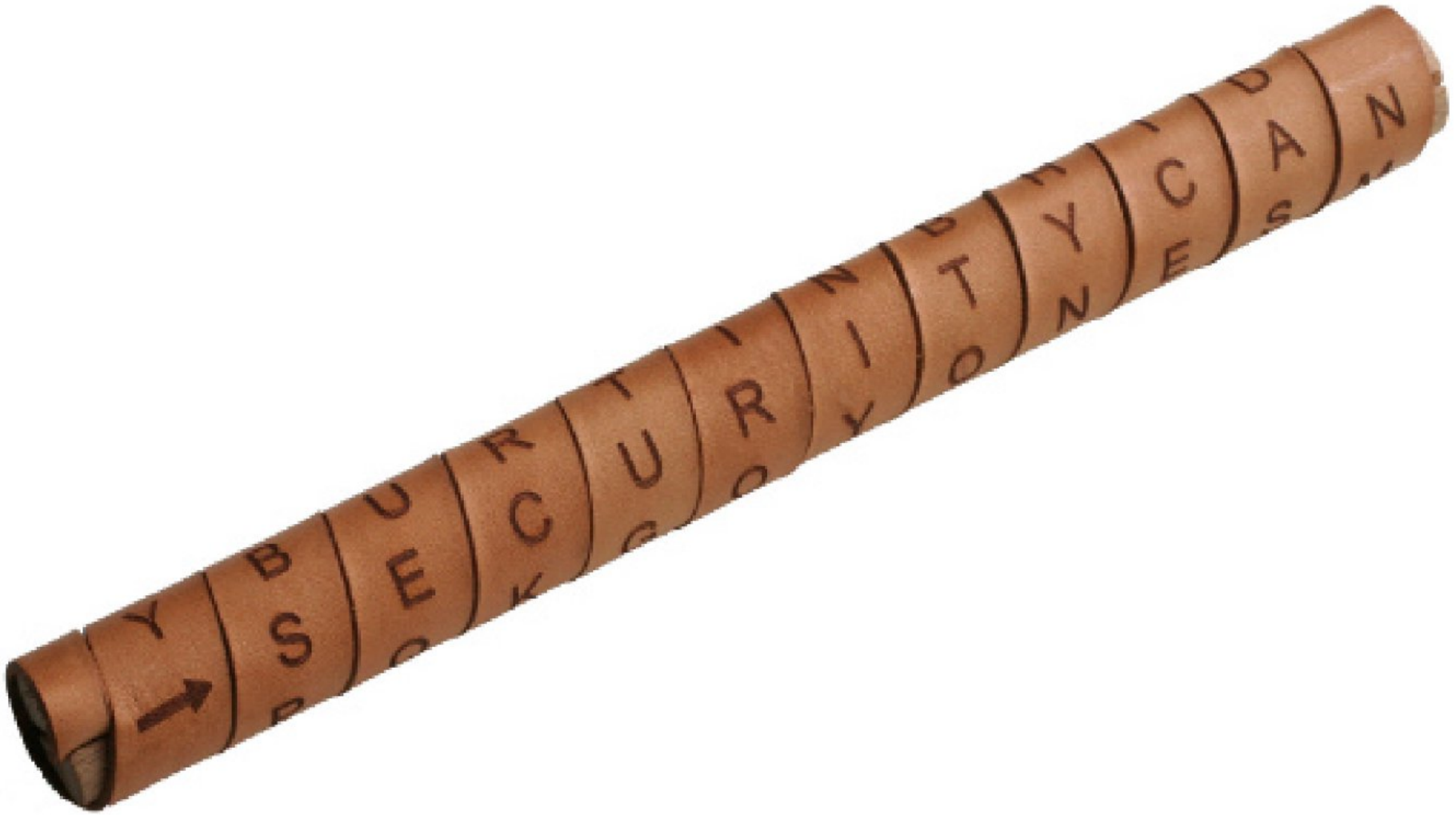
Transposition Techniques

IT3122 Computer Security

2025.09.19

Scytale of Sparta



Transposition Cipher

- Mapping is achieved by performing some sort of permutation on the plaintext letters.
- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.
- The transposition cipher can be made significantly more secure by performing more than one stage of transposition.

Rail Fence Technique

- The plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- E.g., to encipher the message `THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG` with a rail fence of depth 2, write the following:

```
T E U C B O N O J M S V R H L Z D G
 H Q I K R W F X U P O E T E A Y O
```

The encrypted message is

```
teucbonojmsvrhlzdghqikrwfxupoeteayo
```

Columnar Transposition

- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- E.g.:

```
Key:          4 3 1 2 5 6 7
Plaintext:    T H E Q U I C
              K B R O W N F
              O X J U M P S
              O V E R T H E
              L A Z Y D O G
Ciphertext: erjezqouryhbxvatkooluwmtdinphocfseg
```

Attacking Columnar Transposition

- Cryptanalysis involves laying out the ciphertext in a matrix and playing around with column positions.
- Digram and trigram frequency tables can be useful.

Reference

- W. Stallings, “Transposition Techniques,” in *Cryptography and Network Security, Principles and Practice*, 8th Edition, 2023, pp. 105–106.