§7.6: Applications: Cæsar cipher

•devo

21 Oct 2005
CMPT14x
Dr. Sean Ho
Trinity Western University

Reminders:

- *journals in folder*
- *Hw (ch6 #28) due*
- *Quiz ch7 today*

TRINITY WESTERN UNIVERSITY

http://cmpt14x.seanho.com/

Quiz ch7 (2 questions, 20 marks, 10 minutes)

```
VAR str1, str2, str3: ARRAY [10..20] OF CHAR;
BEGIN str1 := "Fuji";
    str2 := "Braeburn";
    str3 := "Golden Delicious";
```

- Evaluate each expression, or describe the error:
  - "Fuji" + "Braeburn"
  - str1 + str2
  - LENGTH (str3)
  - Compare (str2, str3) *(* less/greater/equal *)*
  - Compare (str2, "BRAEBURN")
- Write a Length function for strings:

```
PROCEDURE Length (s: ARRAY OF CHAR) : CARDINAL;
```

Quiz ch7 answers: #1

```
VAR str1, str2, str3: ARRAY [10..20] OF CHAR;
BEGIN str1 := "Fuji";
    str2 := "Braeburn";
    str3 := "Golden Delicious";
```

- Evaluate each expression:
  - "Fuji" + "Braeburn"
  - str1 + str2
  - LENGTH (str3)
  - Compare (str2, str3)
  - Compare (str2, "BRAEBURN");
  - "FujiBraeburn"
  - Can't concat vars
  - 11(not 16)
  - less
  - greater

Quiz ch7 answers: #2

- Write a Length function for strings:

```
PROCEDURE Length (s: ARRAY OF CHAR) : CARDINAL;
VAR len : CARDINAL;
BEGIN
    len := 0;
    WHILE (len <= HIGH (s)) AND (s[len] <> “”)
        DO
            INC (len);
        END;
    RETURN len;
END Length;
```

Review / what's on (7.6-7.13)

- Application: pseudo-random number generator
  - Persistent variable (seed) internal to library
  - Initialization in body of implementation file
- Application: substitution cipher
  - Designing public interface (DEF)
  - Using private helper functions
- Application: fractions (time permitting)
  - Designing an ADT as a library

DEF: pseudo-random num library

- We only need Random() as a public procedure:

```
DEFINITION MODULE PseudoRandom;

PROCEDURE Random () : LONGREAL;
    (* returns a random number between 0 and 1 *)

PROCEDURE InitSeed (x : LONGREAL);
    (* initialize the number generator seed *)

END PseudoRandom.
```

- InitSeed provides a way for the user to manually set the seed.

Cryptography example

- Cæsar substitution cipher:
  - Key: e.g., QAZXSWEDCVFRTGBNHYUJMKIOLP
  - Cleartext: input text to encrypt
  - Ciphertext: output encrypted text
  - Encoding: replace each letter in source with corresponding letter from code key
  - Decoding: same, using the decode key
- ROT13 was an example of a substitution cipher
  - Key: NOPQRSTUVWXYZABCDEFGHIJKLM

Write a Substitution cipher library

- What public interface do we want for the library?

```
DEFINITION MODULE Substitution;
TYPE CodeString = ARRAY [0..25] OF CHAR;

PROCEDURE Encode (src: ARRAY OF CHAR;
  VAR dst: ARRAY OF CHAR; key: CodeString);

PROCEDURE Decode (src: ARRAY OF CHAR;
  VAR dst: ARRAY OF CHAR; key: CodeString);

END Substitution.
```

Implementing Substitution

- In the implementation it is handy to have some helper functions for internal use: these will not be exported:

```
IsLetter (ch: CHAR) : BOOLEAN;
    (* check if it's a letter or some other character *)
AlphaPos (ch: CHAR) : CARDINAL;
    (* index of a letter in the range 0..25 *)
DecodeKey (enckey: CodeString; deckey: CodeString);
    (* create a decode key from an encoding key *)
```

- How to implement these?

TODO items

- Lab #6 next week: 7.14 #(22 / 32 / 37)
- 140 Final next week W-Th (two parts)
- Review in-class next Mon