Unit 34
Keyword substitution cipher

The *keyword substitution cipher*, also called the *keyed substitution cipher*, or simply the *keyword cipher*, is a monoalphabetic substitution cipher in which the key alphabet is constructed from a keyword. The keyword is placed at the beginning of the key, its repeated letters are removed, and then the remainder of English letters are added to the key. The three most common ways of filling the key are these:

- Add the remaining letters in alphabetical order. For example, if the keyword is AUTOMOBILE, then the key alphabet is (remember to drop the repeated O)

  AUTOMBILECDFGHJKNPQRSVWXYZ

- Start adding letters from the alphabetically next after the last letter of the keyword. For the keyword AUTOMOBILE, we start with the next letter after E, which is F. When we reach Z we place the remaining missing letters C and D.

  AUTOMBILEFGHJKNPQRSVWXYZCD

- Start adding letters from the next letter after the alphabetically last letter of the keyword. The keyword AUTOMOBILE has U as its alphabetically last letter. So we fill in starting with V.

  AUTOMBILEVWXYZCDFGHJKNPQRS

Here are some other variations. They can be used alone or in combinations.

- Fill in the remaining letters after the keyword in reverse alphabetical order.
- Put the keyword at the end of the key.
- Use a keyword for the plaintext alphabet rather than the ciphertext alphabet.
- Use keywords for both the plaintext and ciphertext alphabets.

Reading and references

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, revised and updated 1996, pages 103-104.

Programming tasks

1. Create a function that returns a permutation of the alphabet from a keyword. Use an optional parameter to determine whether the remaining letters are added in order starting from the beginning of the alphabet or from the last letter of the keyword. The return type of this function should be the data type that you defined in Task 1 of Unit 18.

2. Implement the cipher. Allow for the user to choose a key-filling method.

3. Write a function to generate an alphabet key if the keyword is used in the plaintext alphabet rather than the ciphertext alphabet.

4. Write a function to generate an alphabet key if keywords are used in both the plaintext and ciphertext alphabets. Note that you can combine tasks 1, 3, and 4 into one function if you like. Make a new version of your cipher that can handle keywords for both alphabets.

Exercises

1. Encipher this text with the keyword `KNIGHTS`. Use the first key-filling method that we discussed above.

   > Before Cai was born, Cynyr made the prophesy that his son would have a frozen heart and be extremely stubborn. He added the prediction that no one would be able to endure fire or water as well as his son.

2. Decipher this text with the keyword `ROUNDTABLE`. Use the second key-filling method that we discussed above.

   ```
   AVLIDWDPDAVLIDWDPDXBLSBDPQBRGGLAJHVQSLDINVPDQJVSSDPGZRGJIDS
   JNPRAHZGLTDJVSBRVISDNDWDPHJPDOZKRGDRUUVQLIAQKDUSPDQJTNDRNFI
   LABSQLURIIJSGDRWDSBDDKLSZHZNDQKRLPAXLIDWDPD
   ```

3. This ciphertext is an example from Gaines’s book. It uses a keyword for both the plaintext and ciphertext alphabets. In the plaintext, `J` is used as a space between words. Break it by hand and reconstruct both alphabets to obtain the two keywords.

   ```
   ROVLL ABTLD LBCQM PXLBA FBTCT ATCOR LTOLC RHPDT XLYOA
   ELBXP HLXBT XXQLD RGLTK XRLGD BKLDP PLOHL YOAEL KOMXB
   LHOEL VCRRC RJLTK DTLRC INXPL LLTKX LRCIN XPLVD BLVOR
   LPORJ LDJOL FYLIO PORXP LMDEN XELKC TTLVK OLOHH XEXGL
   TOLIO QMEOQ CBXLH OELTV OLIXR TBLBC RIXLK XLVDB LDFPX
   LTOLB XRGLT KXLBO PATCO RLFYL EXTAE RLQDC PLLBT CPPLC
   TLVOA PGLFX LVOET KLDRO TKXEL RCINX PLTOL HCRGL OATLT
   KXLNX YLLTK CBLQA BTLFX LTKXL XWMPD RDTCO RLOHL TKXLE
   XHXEX RIXLT OLDLI EOORX ELDRG LTKXL XQMKD BCBLO RLDLG
   DTXLL MLBLT KXLTV OLIXR TBLKD BLROT LYXTL FXXRL MDCGL
   ```