Exercises: Substitution Ciphers

Spreadsheet Exercise

To begin with, download the Excel spreadsheet: `01a-caesar.xlsx`. We will use some basic functions to allow us to encrypt short messages using the Caesar cipher.

1. In Cell B1, enter 15 characters of text, all in lower case.
2. In Cell B2 enter a shift value for the Caesar cipher - this is an integer between 0 and 25.
3. In Cell B3, use the LEN function to check the length of the text you have entered. To enter a formula, you need to start with an equals sign. So you will enter '=LEN(B1)' in this cell.
4. Now use the MID function to split your text apart:
   - In Cell B5, enter '=MID(B1,B4,1)'.
   - The dollar signs mean that when we drag the function into new cells, it will always point at Cell B1.
   - Instead of typing the entries, you can also click on the appropriate cell.
   - Tapping the 'F4' key on your keyboard will automatically add dollar signs.
5. Hover over the bottom right of Cell B5 until your cursor becomes a black cross. Hold and drag this over to Cell P5. You should find that your text appears in single letters across the sheet.
6. We will use the CODE function to turn these letters into numbers. In Cell B6, enter '=CODE(B5)'. This will return a number between 97 and 122. Drag this across to Cell P6.
7. The formulae in Row 7 should remain untouched and will update once the previous formulae above have been created. (The numbers are being adjusted so that they are in the range 0-25, instead of the ANSI range of 97-122.)

8. Now we will apply our Caesar cipher using the MOD function. Enter '=MOD(B8+B2,26)' in Cell B8. Drag this across to Cell P9.

9. The formulae in Row 9 are to add back on the code value of 'a' to bring the numbers back into the range 97-122.

10. Now to turn the numbers back into letters, we use the CHAR function. Enter '=CHAR(B9)' in Cell B10, and drag across to Q10.

11. To put the ciphertext back together, we can use the CONCAT function. Enter '=CONCAT(B10:P10)' in Cell B11.

12. (Optional) Can you extend your spreadsheet so that it can handle larger pieces of text? You could also investigate the IFERROR function in order to remove errors when you use shorter pieces of text.

Exercises

1. Using Caesar encryption modulo 26 with key 16,

   (a) encrypt `stop`

   (b) decrypt `THEF`.

   Be careful with capital and lower case letters here. The spreadsheet we have made can only deal with lower case letters, so when entering ciphertext to decrypt you should enter these in lower case.

2. Decipher the following word, which has been subject to a Caesar shift: `TZITLDJKRETVJ`.

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

3. (a) Using the cipher given above, encode the message `yourcodenameisredfox`.

   (b) Using the same cipher, decode the message `ERHOBVNGOHHMGEVNBYRE`.

Solutions

1. (a) Since the key is 16, we need to convert letters to numbers (the table on p.30 of the notes may be useful) and add 16 to each to encode (modulo 26):

$$\begin{aligned} s = 19 \qquad & 19 + 16 = 35 \equiv 9 \bmod 26 \mapsto I \\ t = 20 \qquad & 20 + 16 = 36 \equiv 10 \bmod 26 \mapsto J \\ o = 15 \qquad & 15 + 16 = 31 \equiv 5 \bmod 26 \mapsto E \\ p = 16 \qquad & 16 + 16 = 32 \equiv 6 \bmod 26 \mapsto F \end{aligned}$$

   So the encoded message is IJEF.

(b) To decrypt, we need to subtract 16 (modulo 26):

$$T = 20 \qquad 20 - 16 = 4 \mapsto d$$

$$H = 8 \qquad 8 - 16 = -8 \equiv 18 \bmod 26 \mapsto r$$

$$E = 5 \qquad 5 - 16 = -11 \equiv 15 \bmod 26 \mapsto o$$

$$F = 6 \qquad 6 - 16 = -10 \equiv 16 \bmod 26 \mapsto p$$

So the decoded message is DROP.

2. Trying each of the different shift amounts between 1 and 26 for the first few letters mainly gives invalid letter combinations, but eventually it can be seen that a shift by 9 spaces ($T = 20 \mapsto 20 + 9 = 29 \equiv 3 \bmod 26 \mapsto C$) gives the decoded word `CIRCUMSTANCES`.

3. (a) To encode, we need to find the letter in the top row of the given table, and write down the corresponding letter from the bottom row. yourcodenameisredfox encodes to `AVPIUVTHNKZHBGIHTLVD`.

   (b) To decode, we must find each letter of the ciphertext in the bottom row, and write down the corresponding letter from the top row. `ERHOBVNGOHHMGEVNBYRE` decodes to `thelionsleepstonight`.