This exercise consists of two parts:

1. Study G-Schreiber cipher design. Describe known plain-text attack against its internal settings:
1)0-1 distribution on the wheels,
2) wheels initial state,
3) cabling permutation.

The analysis is based on two observations: if the cipher-text 5-bit group is 11111 or 00000 at some moment, then the
5-bit group at the switches input is 11111 or 00000 respectively as well. So one can reconstruct the first 5 bits on the plug for those moments. Therefore the cabling to the first 5 plug positions and 0-1 distribution on related wheels are easily reconstructed by testing periodicity: the period of the bit sequence from a wheel with n =47,53,..,73 positions is n.

You know switches input/ output at almost any moment now. Learn about control 5-bit group if switches input/ output comprise single 1 or single 0, that is of weight 1 or 4. Reconstruct the rest of the cabling and 0-1 distribution on related wheels .

Remark the bits representing plain-text/cipher-text characters are numbered from left to right. So, for instance, the left most bit of a 5-bit group representing a plain-text character is XORed with the left most bit on the plug. The bottom bit of the output (see the picture) is the left most bit of a 5-bit combination representing the cipher-text character. Also have a look at the Maple implementation provided.

2. For the plain-text, Latin alphabet 60 times, 1560 characters, a related cipher-text for the first 1560-10=1550 characters is given below. The plain-text was encoded by teleprinter code CCITT2 in Letter Shift, provided in the Lecture Notes and then got encrypted. Cipher-text 5-bit groups are encoded by their positions in CCITT2 code, e.g., 11000 is encoded by 1, 10011 is encoded by 2 and so on. Exemplary program for encryption with G-Schreiber including the code is provided. Find all internal settings of the cipher.

Continue encryption and provide (with a description) the cipher-text(10 numbers) for the rest of the plaintext(10 characters) as an answer. The deadline is Monday, February 14, midnight. Remark that to be admitted

to the exam you should gain at least 60%(upper “D”) for each of the mandatory exercises. Each mandatory exercise is at most 10% of the final grade. Very good luck!

Plain-text= ABCDEGHIJKLMNOPQRSTUVWXY…
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher-text=

20, 16, 29, 28, 16, 12, 30, 4, 11, 30, 7, 14, 12, 10, 24, 1, 5, 8, 19, 20, 3, 26, 25, 11, 4, 22, 15, 13, 31, 25, 25, 4, 13, 12, 16, 16, 20, 8, 11, 19, 10, 4, 20, 5, 21, 18, 30, 31, 9, 15, 6, 31, 9, 17, 24, 12, 22, 25, 8, 24, 17, 14, 18, 5, 25, 4, 29, 8, 24, 25, 21, 30, 23, 27, 28, 31, 12, 22, 23, 6, 19, 6, 13, 30, 5, 18, 13, 18, 2, 29, 7, 13, 6, 30, 17, 24, 16, 24, 23, 2, 5, 2, 9, 14, 15, 8, 2, 18, 31, 22, 18, 28, 10, 7, 31, 25, 31, 30, 18, 16, 26, 8, 13, 8, 3, 2, 1, 5, 31, 11, 31, 4, 30, 14, 25, 5, 25, 5, 8, 17, 14, 9, 30, 12, 6, 18, 1, 3, 18, 28, 18, 25, 6, 5, 23, 28, 19, 21, 21, 21, 14, 4, 23, 4, 18, 1, 31, 30, 14, 8, 3, 12, 27, 15, 30, 22, 10, 23, 15, 29, 22, 14, 29, 20, 13, 23, 15, 17, 32, 27, 32, 21, 13, 20, 7, 19, 6, 24, 16, 24, 7, 30, 30, 17, 19, 22, 28, 21, 22, 20, 9, 12, 12, 3, 13, 17, 14, 20, 1, 24, 2, 19, 16, 10, 20, 3, 11, 11, 10, 9, 20, 15, 10, 20, 3, 9, 30, 29, 6, 2, 18, 32, 15, 30, 31, 20, 10, 3, 16, 28, 4, 13, 19, 28, 1, 20, 7, 30, 4, 17, 27, 1, 24, 28, 8, 31, 6, 21, 24, 11, 24, 4, 11, 30, 19, 1, 24, 9, 9, 14, 13, 16, 7, 3, 6, 7, 32, 9, 15, 22, 8, 21, 30, 28, 20, 11, 25, 5, 31, 30, 26, 8, 1, 31, 29, 25, 22, 26, 22, 13, 30, 24, 30, 12, 25, 25, 1, 26, 21, 11, 1, 32, 23, 3, 25, 2, 29, 14, 29, 10, 21, 4, 17, 28, 32, 11, 28, 4, 2, 10, 21, 21, 4, 30, 23, 17, 32, 15, 17, 7, 28, 9, 30, 25, 7, 32, 1, 8, 7, 3, 4, 22, 13, 15, 7, 13, 16, 13, 8, 13, 20, 16, 7, 10, 31, 13, 31, 29, 30, 4, 5, 23, 8, 27, 21, 9, 23, 2, 25, 16, 31, 29, 29, 18, 17, 31, 9, 21, 29, 24, 10, 5, 3, 15, 18, 24, 30, 14, 23, 26, 17, 30, 10, 31, 11, 27, 20, 30, 27, 6, 9, 28, 12, 21, 3, 26, 4, 10, 25, 3, 26, 28, 14, 19, 2, 24, 25, 26, 8, 29, 9, 1, 2, 19, 5, 8, 19, 10, 5, 7, 9, 18, 19, 18, 5, 16, 10, 9, 8, 24, 3, 14, 16, 3, 5, 28, 32, 23, 13, 10, 14, 12, 28, 6, 11, 23, 21, 8, 24, 24, 22, 3, 9, 7, 32, 15, 10, 19, 9, 23, 14, 26, 17, 32, 30, 28, 24, 2, 25, 1, 28, 10, 28, 4, 27, 31, 12, 14, 24, 9, 15, 7, 29, 21, 10, 26, 2, 1, 5, 5, 8, 13, 18, 11, 6, 8, 16, 14, 18, 9, 19, 28, 24, 25, 16, 18, 5, 21, 13, 2, 15, 17, 25, 31, 10, 25, 8, 23, 9, 15, 24, 25, 2, 32, 4, 29, 27, 19, 28, 26, 27, 32, 15, 14, 7, 14, 21, 9, 31, 17, 21, 19, 28, 11, 23, 17, 2, 10, 10, 9, 5, 27, 27, 27, 18, 8, 3, 27, 29, 10, 13, 4, 23, 31, 18, 9, 32, 2, 30, 10, 6, 9, 28, 11, 22, 30, 14, 8, 17, 16, 28, 27, 15, 19, 10, 27, 1, 11, 25, 30, 16, 7, 23, 12, 30, 15, 26, 15, 12, 29, 6, 7, 23, 2, 9, 24, 19, 17, 17, 13, 8, 20, 24, 31, 26, 28, 4, 24, 25, 3, 16,

22, 17, 1, 14, 27, 5, 13, 29, 25, 7, 31, 29, 23, 13, 28, 10, 9, 17, 19, 27, 6, 3, 24, 16, 14, 32, 16, 19, 10, 8, 22, 5, 12, 23, 8, 5, 29, 19, 23, 7, 23, 18, 28, 7, 24, 5, 1, 18, 24, 7, 18, 9, 30, 5, 6, 16, 23, 27, 14, 13, 14, 13, 31, 25, 10, 29, 18, 29, 22, 5, 21, 3, 25, 19, 27, 3, 26, 2, 19, 4, 31, 9, 15, 19, 23, 27, 14, 1, 30, 21, 16, 1, 4, 16, 13, 16, 25, 1, 25, 16, 17, 22, 31, 21, 31, 22, 24, 9, 2, 26, 25, 15, 2, 14, 6, 16, 15, 24, 25, 18, 19, 17, 14, 2, 15, 6, 25, 12, 23, 20, 21, 1, 8, 19, 15, 24, 32, 8, 10, 15, 2, 7, 3, 9, 12, 15, 3, 25, 6, 21, 29, 2, 25, 17, 19, 9, 29, 20, 30, 1, 5, 21, 9, 20, 25, 15, 17, 3, 11, 9, 13, 31, 14, 29, 26, 11, 5, 13, 8, 22, 32, 17, 26, 13, 8, 7, 16, 28, 1, 15, 5, 13, 19, 16, 8, 17, 20, 4, 7, 14, 23, 11, 26, 31, 14, 27, 11, 22, 5, 26, 12, 3, 17, 24, 15, 19, 28, 21, 12, 19, 14, 4, 8, 8, 27, 2, 11, 21, 9, 11, 29, 1, 11, 1, 3, 22, 25, 4, 29, 23, 14, 23, 6, 15, 1, 21, 29, 2, 21, 32, 29, 7, 5, 15, 28, 25, 22, 28, 3, 18, 2, 30, 9, 24, 6, 13, 25, 26, 19, 23, 8, 17, 2, 13, 7, 29, 27, 20, 19, 13, 17, 29, 23, 23, 4, 5, 24, 31, 15, 12, 7, 15, 25, 32, 13, 11, 3, 9, 21, 24, 19, 26, 18, 1, 27, 20, 22, 27, 30, 6, 12, 11, 29, 1, 1, 7, 11, 28, 14, 30, 14, 27, 12, 21, 22, 29, 15, 3, 14, 5, 29, 30, 18, 20, 19, 7, 24, 6, 29, 6, 24, 31, 24, 19, 5, 13, 26, 22, 17, 31, 18, 2, 1, 32, 13, 20, 2, 12, 2, 19, 11, 2, 27, 4, 9, 4, 21, 15, 22, 18, 14, 19, 9, 1, 6, 21, 18, 25, 17, 28, 7, 22, 13, 15, 11, 11, 10, 6, 21, 20, 3, 12, 19, 23, 8, 5, 25, 15, 15, 2, 14, 25, 7, 20, 29, 12, 25, 16, 17, 4, 24, 22, 14, 29, 4, 9, 14, 16, 7, 6, 26, 1, 7, 5, 10, 32, 3, 24, 4, 32, 7, 31, 18, 24, 32, 5, 6, 28, 2, 24, 4, 10, 11, 24, 29, 9, 29, 16, 27, 25, 12, 19, 14, 7, 31, 19, 31, 18, 26, 16, 17, 24, 26, 8, 18, 14, 21, 22, 10, 3, 15, 25, 23, 16, 7, 2, 6, 23, 11, 19, 19, 23, 26, 28, 23, 10, 29, 3, 30, 18, 12, 23, 19, 25, 24, 21, 7, 7, 21, 28, 3, 7, 20, 5, 19, 27, 3, 20, 14, 28, 30, 7, 14, 20, 23, 21, 5, 14, 23, 25, 2, 2, 5, 16, 19, 2, 3, 8, 23, 30, 32, 29, 11, 24, 19, 2, 12, 13, 31, 27, 24, 4, 8, 9, 25, 21, 10, 27, 12, 4, 25, 29, 18, 4, 26, 31, 19, 5, 21, 25, 14, 15, 13, 23, 31, 8, 5, 5, 18, 24, 6, 12, 24, 3, 15, 4, 11, 16, 14, 3, 1, 20, 9, 20, 1, 26, 1, 14, 26, 5, 25, 24, 28, 26, 3, 31, 29, 2, 29, 31, 1, 2, 3, 8, 23, 8, 27, 29, 23, 14, 18, 16, 17, 1, 15, 6, 7, 13, 21, 28, 13, 13, 9, 1, 26, 10, 17, 27, 25, 25, 8, 11, 3, 1, 1, 18, 23, 29, 27, 18, 18, 19, 21, 26, 21, 1, 10, 13, 22, 7, 16, 5, 1, 16, 15, 6, 9, 2, 30, 8, 8, 29, 16, 30, 7, 13, 14, 16, 14, 32, 29, 1, 18, 6, 20, 28, 11, 3, 6, 20, 16, 16, 18, 28, 30, 31, 25, 7, 11, 19, 11, 3, 13, 2, 27, 26, 3, 9, 4, 24, 28, 20, 19, 8, 17, 10, 10, 28, 5, 32, 27, 3, 6, 6, 2, 8, 8, 11, 2, 31, 27, 29, 15, 31, 28, 14, 25, 5, 24, 10, 18, 25, 11, 5, 17, 8, 28, 6, 29, 12, 1, 5, 7, 14, 14, 11, 30, 12, 30, 9, 22, 21, 5, 13, 19, 26, 29, 19, 3, 32, 28, 11, 10, 14, 3, 13, 25, 17, 14, 18, 7, 11, 19, 11, 15, 21, 22, 9, 19, 15, 4, 26, 8, 6, 9, 15, 15, 30, 12, 23, 14, 29, 21, 30, 20, 18, 21, 25, 25, 32, 5, 12, 9, 22, 27, 11, 20, 13, 30, 22, 29, 24, 19, 19, 12, 15, 25, 20, 21, 32, 3, 4, 13, 11, 31, 21, 32, 2, 9, 3, 27, 11, 27, 16, 21, 22, 15, 28, 14, 23, 28, 20, 28, 16, 22, 8, 5, 29, 28, 31, 18, 23, 5, 13, 20, 27, 29, 31, 29, 7, 8, 21,

24, 18, 9, 27, 19, 15, 9, 11, 8, 24, 6, 26, 32, 13, 6, 23, 2, 2, 23, 11, 16, 25, 32, 24, 20, 28, 23, 10, 3, 21, 12, 31, 16, 27, 7, 22, 8