Problem 4. «Weak key schedule for DES»

Alice is a novice cryptographer. She figured out how the DES encryption algorithm works and decided to implement it in order to exchange secret messages with Bob. She used the simplest ECB mode. But in her implementation, Alice made a mistake: inside the function F in addition of data with a round secret subkey, she forgot to change the index. So, in her implementation, in each round, the data is added modulo 2 with the first round key. Carol really wants to know what Alice and Bob are exchanging messages about. She even managed to get hold of a couple of files once. The Book.txt file contains an open message, and the Book_Cipher.txt file contains the corresponding encrypted text. Help Carol to find the secret encryption key and read the message she intercepted (the message is in hexadecimal format):

```
86991641D28259604412D6BA88A5C0A6471CA722
2C52482BF2D0E841D4343DFB877DC8E0147F3D5F
20FC18FF28CB5C4DA8A0F4694861AB5E98F37ADB
C2D69B35779D9001BB4B648518FE6EBC00B2AB10
```

Some explanations. Description of DES algorithm can be found in the web, see for inst. https://csrc.nist.gov/files/pubs/fips/46/final/docs/nbs.fips.46.pdf Consider an example. We are talking about the correct implementation of DES, where all 16 round subkeys are used correctly. For example, if we take the plaintext 8787878787878787, and encrypt it with the DES key 0E329232EA6D0D73, we end with the ciphertext 0000000000000000. If the ciphertext is decrypted with the same secret DES key 0E329232EA6D0D73, the result is the original plaintext 8787878787878787. In the Book.txt file, each character corresponds to one byte of information according to the ASCII table. Since the DES algorithm processes 64 bits at a time, the first 8 characters of «Three Ri» will be used as the input message, which corresponds to the hexadecimal sequence 5468726565205269. It should be noted that moving the carriage return to a new line in the file also takes two bytes 0D0A.