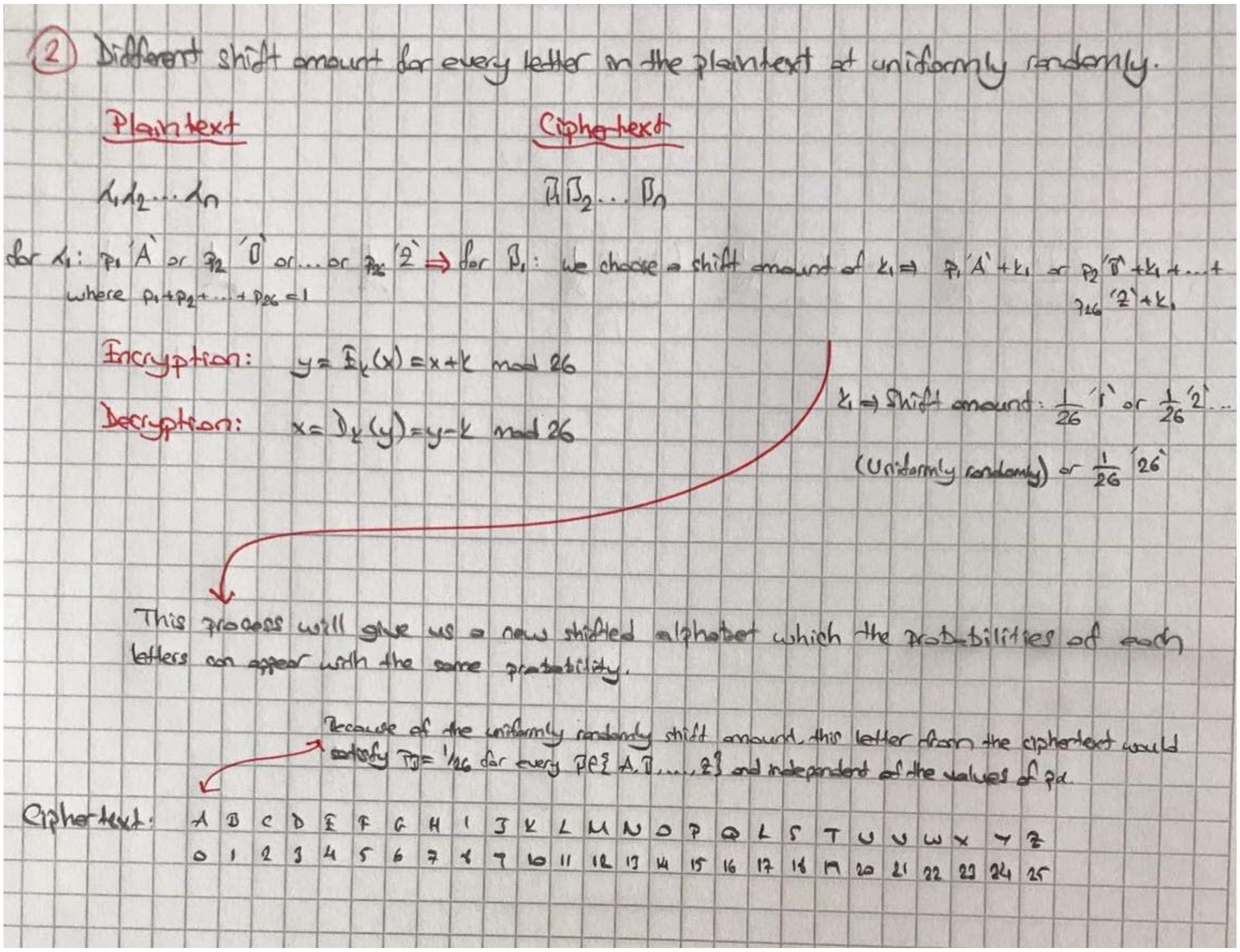
1. FROG : Shift = 18
   COLD : Shift = 21
   (caesar.cpp)

2.



② Different shift amount for every letter in the plaintext at uniformly randomly.

Plaintext

$\alpha_1\alpha_2\ldots\alpha_n$

Ciphertext

$\beta_1\beta_2\ldots\beta_n$

for α_1: p_1 'A' or p_2 'B' or ... or p_{26} 'Z' ⇒ for β_1: we choose a shift amount of k_1 ⇒ p_1 'A' $+ k_1$ or p_2 'B' $+ k_1 + \ldots +$ p_{26} 'Z' $+ k_1$

where $p_1+p_2+\ldots+p_{26}=1$

Encryption: $y = E_k(x) = x+k \mod 26$

Decryption: $x = D_k(y) = y-k \mod 26$

k_1 ⇒ Shift amount: $\frac{1}{26}$ '1' or $\frac{1}{26}$ '2' ...

(Uniformly randomly) or $\frac{1}{26}$ '26'

This process will give us a new shifted alphabet which the probabilities of each letters can appear with the same probability.

Because of the uniformly randomly shift amount, this letter from the ciphertext would satisfy $P_\beta = 1/26$ for every $\beta \in \{A, B, \ldots, Z\}$ and independent of the values of p_α.

Ciphertext:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

3. Most frequent letter in the plaintext is O. Ciphertext was “HR JNAF ERRBH HR STYYSD YTJD “.
   After replacing H with “HO JNAF EOOBH HO STYYSD YTJD” (affine_cipher.cpp)
   β can be any number in Z_{26}. But α values must satisfy gcd(α,26) = 1. So α can be 1,3,5,7,9,11,15,17,19,21,23,25. By using brute force to (α *14+ β)mod26 = 17 we find α=17 and β=13. Plaintext = “SO MANY BOOKS SO LITTLE TIME”

4. We encrypt the trigrams so β can have 26*26*26 values, which is equal to 17576. But α values must satisfy gcd(α,26^3) = 1. So we can use Euler's phi function. φ(17576) = 8112.
   # of α’s: 8112
   # of β’s: 17576
   Key Space = 8112 * 17576 = 142576512

5. Affine cipher defined in the previous question is not secure against the letter frequency analysis because we just make it stronger against letter frequency analysis by increasing the key space. But it is still possible to attack it because there are some trigrams which are more frequently used than other possible trigrams. Some examples for Trigraph Frequency: “the” “and” “tha” “ent” “Ion” “tio” “for” “nde” “has” “nce” “tis” “oft” “men”.

6. I used the table to solve this. The way I used table was that I found the first letter of the key in the column in the most left, then I searched to the right the encrypted message. After I found the encrypted letter I went up and wrote down the decrypted letter. The plaintext I got was: “EVER TRIED EVER FAILED NO MATTER TRY AGAIN FAIL AGAIN FAIL BETTER”.

7. Because of the space characters are not encrypted I searched for same words in the ciphertext such as: FZM, MFL and QE. There are 15, 24 and 225 characters between these words. So the key length must be gcd(15, 24, 225) = 3 or multiples of 3. By using the letter frequency analysis (second method in the book) I found the key “SIM”. After decrypting with the key I got the plaintext.