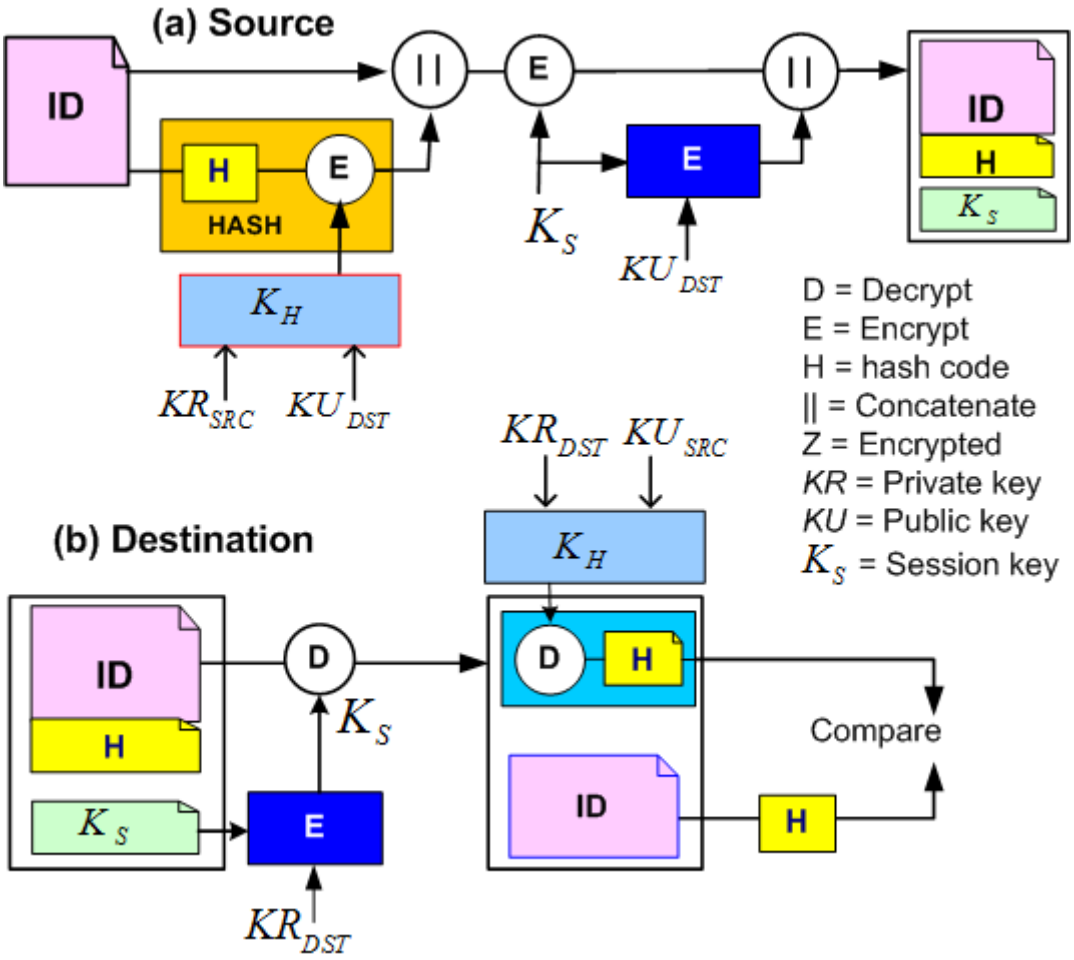
CE 340 Cryptography & Network Security: Assignment 2 Addendum

Title: Secure Authentication
Date to delivery: 29.12.2022, 17:00

PART 2:
Now write a set of functions in a source file, which will implement a hybrid authentication system with digital signature shown in the following figure. The program, **secAuth.py** will read the sender's ID from **ID.txt** file, which contains full citizen registration data (kimlik bilgilerinin tamamı), sign it and send to destination. The destination will then verify the ID of the source. Please, note that K_H is defined as $K_H = XOR(KR_x, KU_x)$.



What to deliver?

1) Execution trace (e.g., screenshots) of each operation
2) Source files and user guide zipped and sent as e-mail attachment
3) Make sure that you can present the project in the classroom