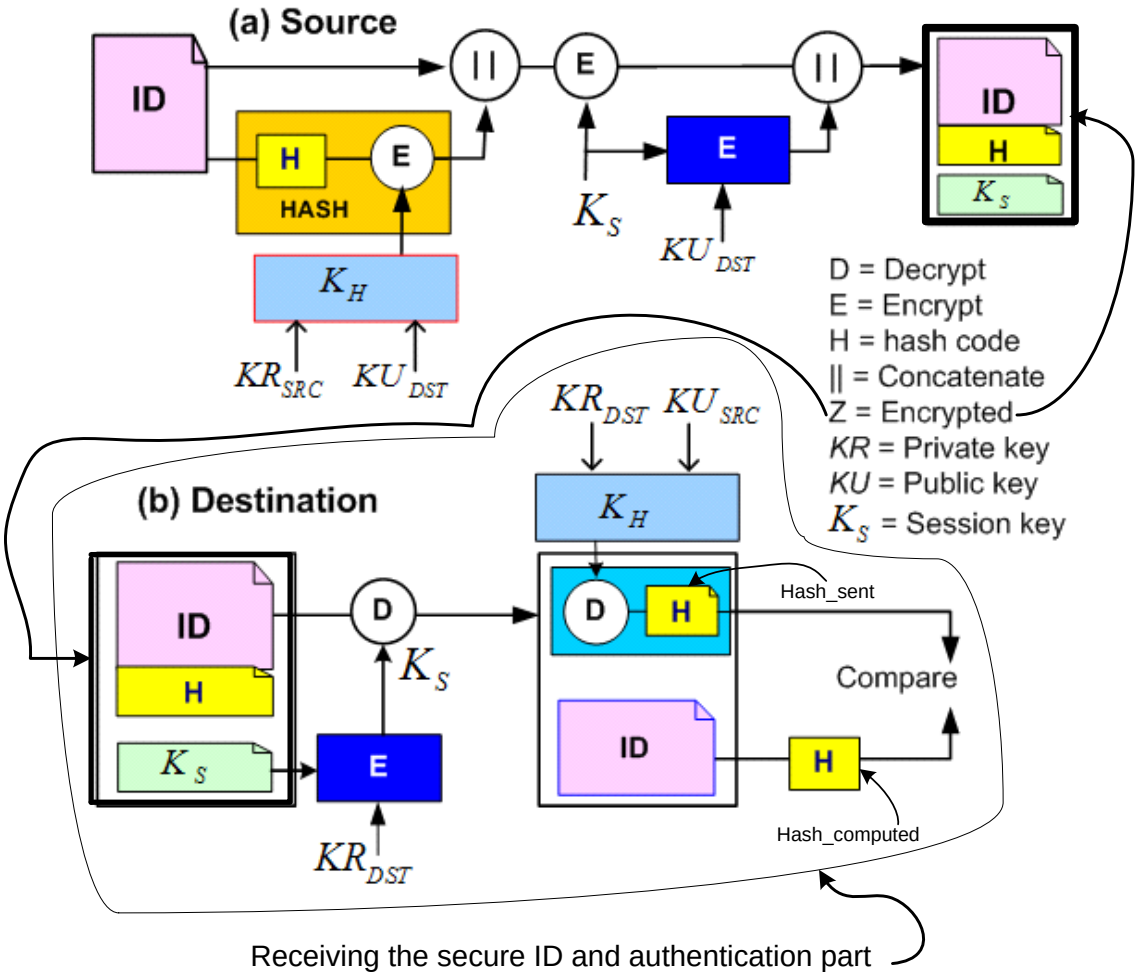
Final Assignment: CE 340 Cryptography & Network Security

Title: Implementation of Secure Authentication Protocol (SAP)
Date to delivery: 09.06.2022, 22:00
Max # of project members is 2

Write a set of **Sage/Python** functions in a python script, which will implement an authentication system with digital signature shown in the following figure. When running the script it will read the **source**'s ID from **ID.txt** file, which contains full citizen registration data (kimlik bilgilerinin tamamı). Please, note that K_H function for the source entity is $K_H = XOR(KR_{SRC}, KU_{DST})$ and for the destination it is $K_H = XOR(KR_{DST}, KU_{SRC})$.



A) Function list for the source:

1. ***H = H(ID):*** Computes and returns the hash value of the source node.
2. ***S = E(H, K_H)***: Encrypts and returns the hash value, which is the signature (***S***) of the source. Note that the encryption is symmetric key.
3. ***CC = conc(X,Y):*** Concatenates ***X*** and ***Y*** and returns the result as ***CC***.
4. ***K_S***: Generate a large integer denoting the session key. The key ***K_S*** must have at least 10 digits.
5. **Z=signID(conc [E(conc(ID,S), K_S)), E(K_S, KU_{DST})])**.
6. **Boolean send(Z, dest_IP):** Sends the signed ID to the destination and returns ***True*** if successful otherwise returns ***False***.

B) You will define the function list for the destination from the block diagram given above, and implement them as appropriate. For example, the verification function is something like

Verify(Hash_sent, Hash_computed): This will compare these (strings) and print "verified" if the input parameters are equal, otherwise it will print "Verification failed"

The report should prove (by screenshot) and explain the verification of the authentication of the source entity done by the destination. You will deliver at least two tests with 2 different IDs and different also with different Keys.

For the public key cryptography you need to use RSA system, which is explained in the slide set (on BB) named as `public_key_crypto.pptx`.

What to deliver?

1) Execution trace (e.g., screenshots) of each operation
2) Source files, report, and user guide zipped and uploaded onto Blackboard
3) Make sure that you can present the project in the classroom on 06.10.2022.