Protocole : BATAKAR

Initial knowledge :

We assume that Alice and Bob will communicate using a server

I- Notation

We denote by :
$C(m,k) \longleftrightarrow$ The cipher message of m with the key k.
$K_{AS} \longleftrightarrow$ The secret key that Alice share with the server.
$K_{BS} \longleftrightarrow$ The secret/key that Bob share with the server..
A$\longleftrightarrow$ Alice
B$\longleftrightarrow$ Bob
S$\longleftrightarrow$ Server
H$\longleftrightarrow$ A hash map

II- Protocol description

Alice

A send to S the message : $< A, C(< B, K >, K_{AS}) >$

Server

S receive it, see that it's coming from A (Because of the first part of the message), he decipher the second part and found a secret K and a destination B. He then send to B :

$$C(< A, K >, K_{BS})$$

Bob

B receive the message and decipher it, know's that it's coming from Alive and get to find the secret K.
B then compute the hash of the secret K : $H(K)$ and send to S

$$< B, C(< A, H(K) >, K_{BS}) >$$

Server

S receive the message, first see's that it's coming from Bob (Because of the first part of the message) then decipher the second part and found a secret H(K) and a destination A.
S send to A :

$$C(< B, H(K) >, K_{AS})$$

Alice

A decipher the message and discovers that it's coming from Bob, then she compute the Hash of the secret K she sent before and verify if it's equal to H(k) that she received.

II-Complexity :

Alice-server : 50+9
Server-Bob : 50+3
Bob-Server : 50+9+5
Server-Alice : 50+3