Problem 2

DPEPN LDECZYZXJ XPLYD EZZ XLYJ

DPNCPEP

using stastical analysis:

EZZ

Two ending letters are Z, i.e. letters must be same.
Three digit letters that ends with two similar words "too".

Besides possibility of getting (digits) letters in a sentence shows % of getting e is 7.80.

so EZZ - too

so which means key = 15/11

finally decoded string:

" SETEC ASTRONOMY MEANS TOO MANY SECRETS "

Problem 3

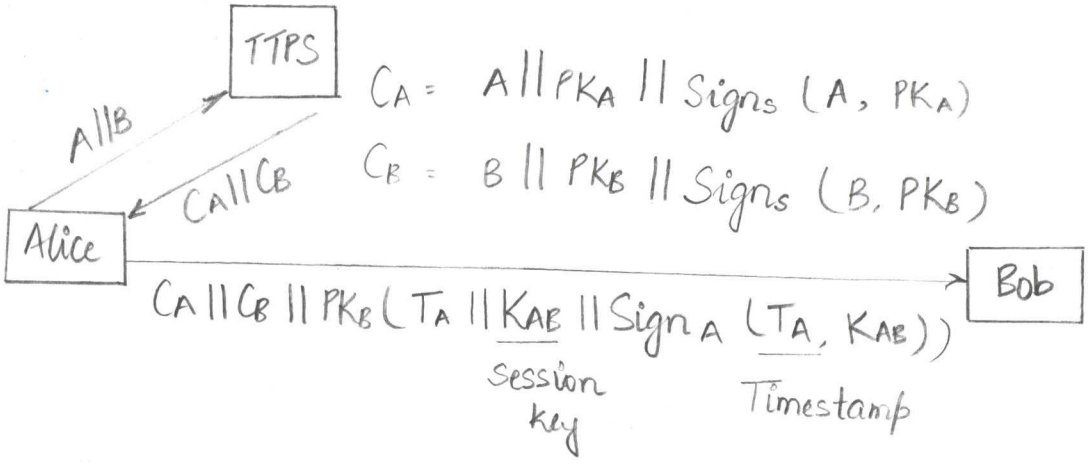
public key (e,n) is (7, 1551)

(d,n) is (631, 1551)

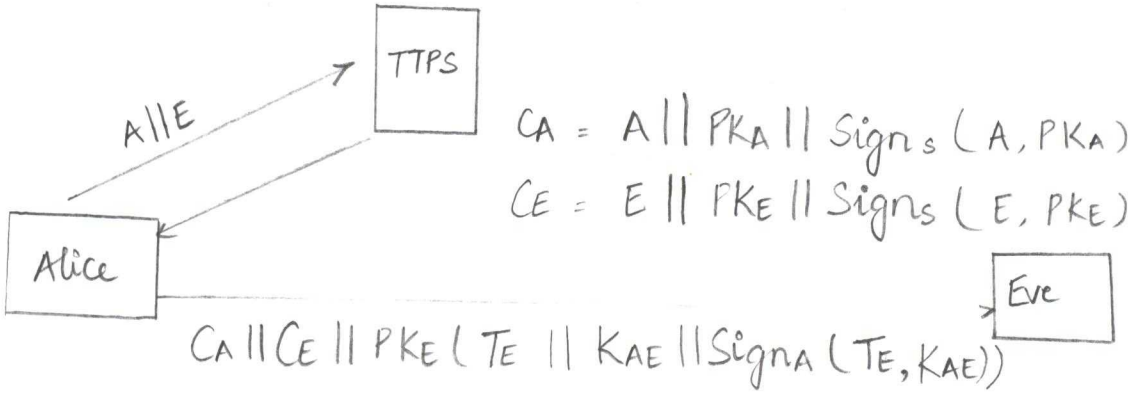
encryption result

O - 7
K - 675
S - 1097
T - 237
A - 758
T - 237
E - ~~738~~ 537
C - 496
O - 7
W - 978
B - 594
O - 7
Y - 1211
S - 1097

Problem 4

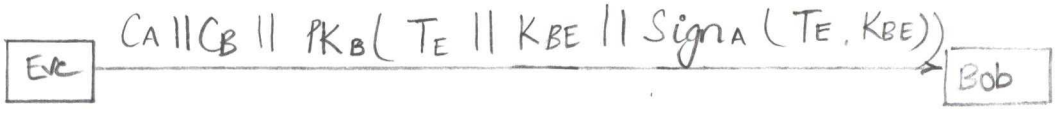


Imagine Alice speaks to Eve after



Eve can decrypt the message send by Alice and can save the signed message from Alice along with session and timestamp.

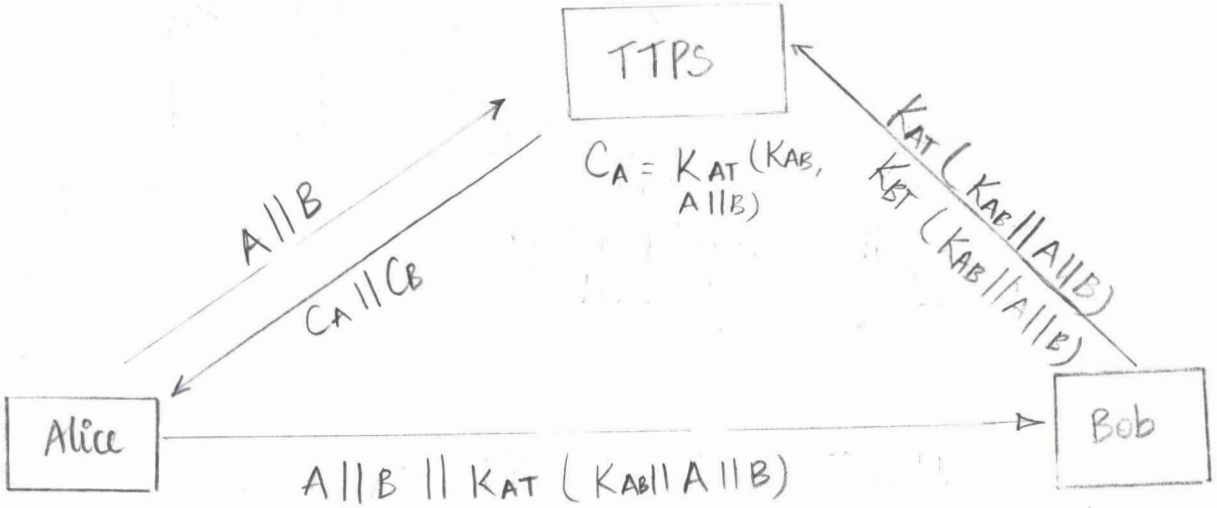
Now eve has been storing messages coming from TTPS to Alice. Eve now has C_B so it can send the message to Bob, pretending to be Alice.



Eve plans to use the same timestamp as when talking to Alice, before pretending to be Alice

Fix

Bob should verify if the message is being sent by Alice so Alice should send TTPS that it wants to communicate to B. TTPS should return back session ID, wrapped in with Alice-TTP publickey, and a message for Bob, with session key as well wrapped in public key of Bob and TTPS.



This fix should work as only keys are shared between TTPS and Alice and TTPS and Bob respectively. Therefore Eve cannot know what the shared key is between TTPS and Bob Alice. Taking into consideration that a session key would be used only once per session.

Problem 5 :

$C_1 \rightarrow S$: $PK_S(PK_{C_1}, PK_{C_2}, K_C, time) \,||\, Sign_{C_1}(PK_{C_1}, PK_{C_2}, K_C, time)$

$S \rightarrow C_1$: $Sign_S(PK_{C_1}, PK_{C_2}, K_C, time)$

$C_1 \rightarrow C_2$: $num \,||\, C_1 \,||\, C_2 \,||\, K_{C_1T}(r_1 \,||\, num \,||\, C_1 \,||\, C_2)$

$C_2 \rightarrow S$: $num \,||\, C_1 \,||\, C_2 \,||\, K_{C_1T}(r_1 \,||\, num \,||\, C_1 \,||\, C_2) \,||\, K_{C_2T}(r_2 \,||\, num \,||\, C_1 \,||\, C_2)$

$S \rightarrow C_2$: $num \,||\, K_{C_1T}(r_1 \,||\, PK_S) \,||\, K_{C_2T}(r_2 \,||\, PK_S)$

$C_2 \rightarrow C_1$: $num \,||\, K_{AT}(r_1 \,||\, K_S)$