COMP 301/401

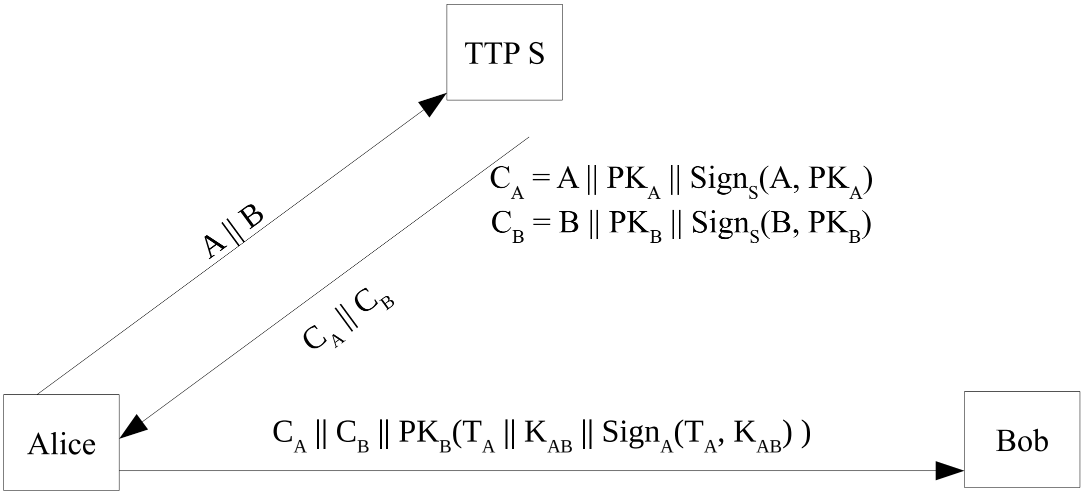
Lab 3

Problem 1
You receive the following ciphertext in the mail *DPEPN LDECZYZXJ XPLYD EZZ XLYJ DPNCPED*. You know that it was enciphered using the Caesar cipher. Can you guess the plaintext? Please explain how you came up with the plaintext.

Problem 2
Consider the following key exchange protocol. Find and describe one vulnerability in this protocol where **Eve can impersonate Alice**.

Terms:

- A is Alice, B is Bob
- S is a Trusted Third Party and knows the public key PK_A of Alice and public key PK_B of Bob
- $Sign_S(...)$ means the signature by entity S
- $PK_B(...)$ means encryption with the public key of B
- K_{AB} is the session key to be shared by A and B
- T_A is a timestamp generated by A to prevent replay attacks (doesn't mean you cannot try to do replay attacks)
- You can assume that at some point Alice talks to Eve (this is important!)


TTP S
$A \| B$
$C_A \| C_B$
$C_A = A \| PK_A \| Sign_S(A, PK_A)$
$C_B = B \| PK_B \| Sign_S(B, PK_B)$
Alice
$C_A \| C_B \| PK_B(T_A \| K_{AB} \| Sign_A(T_A, K_{AB}))$
Bob

Graduate students: Propose a fix for the vulnerability, along with a short explanation why the fix works. For the fix, think about how Bob can be sure that the sender is actually Alice and not Eve.

Problem 3
RangeForce modules

1) Kerberos Overview