Coursework 1 - Exercise 5

November 9, 2023

Consider the following protocol (Figure 1) which Alice and Bob use in order to mutually authenticate each other, i.e., convince each other that "they are who they say they are". Assume that Alice and Bob share a secret key K.

In this protocol, Alice first sends an unpredictable random number R_A. In the second step, Bob encrypts this message to prove knowledge of the key K and also sends a random number R_B. In the third step, Alice decrypts $E(K, R_A)$. If the result is not her original number she aborts the protocol otherwise she encrypts R_B and sends it to Bob. Bob performs a similar check and if everything is OK, he's convinced he's talking to Alice.

Find two attacks in which an attacker can impersonate some of them to the other.

(Assume that the key is not compromised, so nobody can use it to create fake messages.)

---

[2]:
```
s(f1)
```

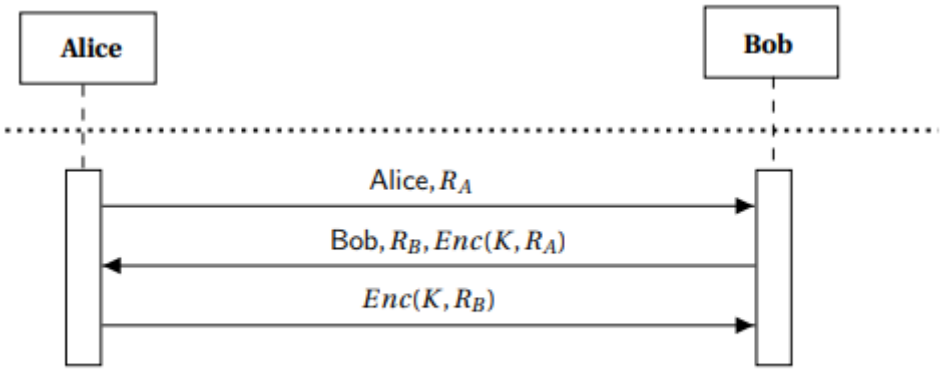
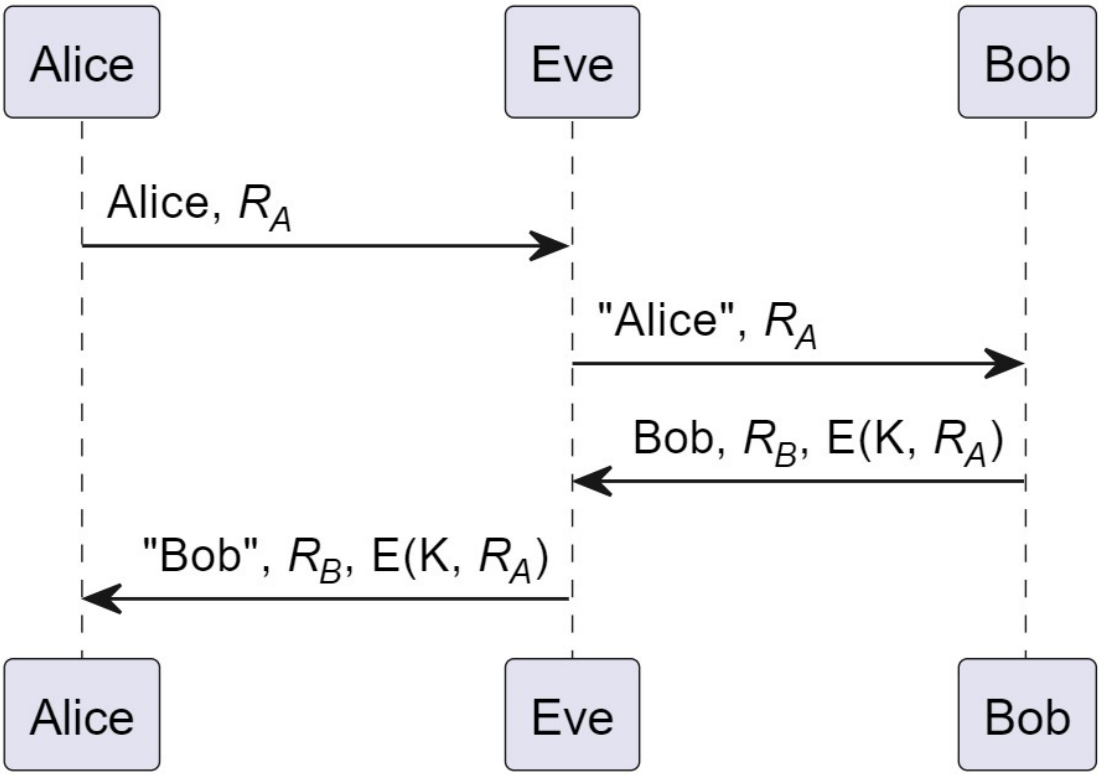


Figure 1: Mutual Authentication Protocol

Attack 1: Bob impersonation

In this attack Eve will intercept the messages sent to Bob and then impersonate Bob by having Bob encrypt the message Alice sent. It will go as follows:

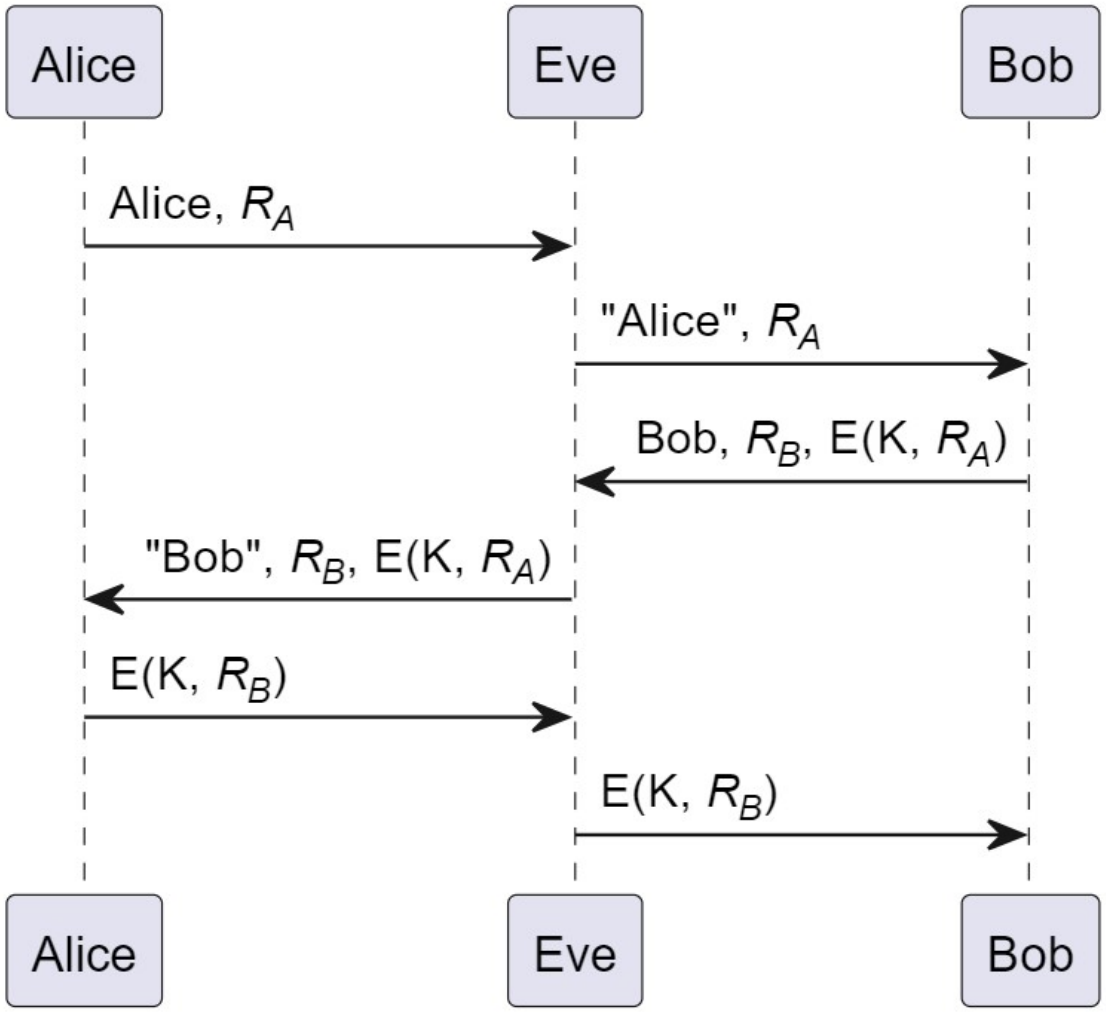
[3]:
```
s(f2)
```



Attack 2: "Man in the middle"

Eve will present herself to Alice as Bob and ask for R_A and then go to Bob and present herself as Alice to Bob and give her Alice's R_A. The communication will be then done through Eve and at the end both Alice and Bob will be trusting Eve. The attack is the same as the previous one but adding the last two steps that makes Bob think that he has been talking with Alice

[4]:
```
s(f3)
```



[1]:
```
from IPython.display import display, Image
def s(f):
    display(Image(filename=f, height=400, width=400))
f1, f2, f3 = "imgs/figure1.png", "imgs/attack1.jpg", "imgs/attack2.jpg"
```