Exercise 28.

a) Given the following challenge-response mutual authentication protocol

1) $A \rightarrow B : r_A$
2) $B \rightarrow A : E_K(r_A, r_B)$
3) $A \rightarrow B : r_B$

Explain how an eavesdropper $E$ can authenticate to $A$ without knowing the symmetric key $K$. This attack is called reflection attack.

b) Given the following challenge-response protocol based on digital signature

1) $A \rightarrow B : r_A$
2) $B \rightarrow A : r_B, S_B(r_B, r_A, A)$
3) $A \rightarrow B : r'_A, S_A(r'_A, r_B, B)$

Explain how an eavesdropper $E$ can authenticate to $B$ without signing any message with his own identity. This attack is called interleaving attack.

Exercise 29.

We want to study the vulnerabilities of the Kerberos protocol

a) A ticket has a limited validity period. Explain what are the advantages and drawbacks to have a short validity period or a long validity period.

b) How can an eavesdropper mount a replay attack which is not prevented by the time stamp $t_A$. Give a countermeasure.

Exercise 30.

Consider the equation

$$Y^2 = X^3 + X + 1.$$ 

Show that this equation describes an elliptic curve over the field $\mathbb{F}_7$.

a) Determine all points in $E(\mathbb{F}_7)$ and compute the trace $t$ of $E$.

b) Show that $E(\mathbb{F}_7)$ is cyclic and find a generator.