

**EBU6010**

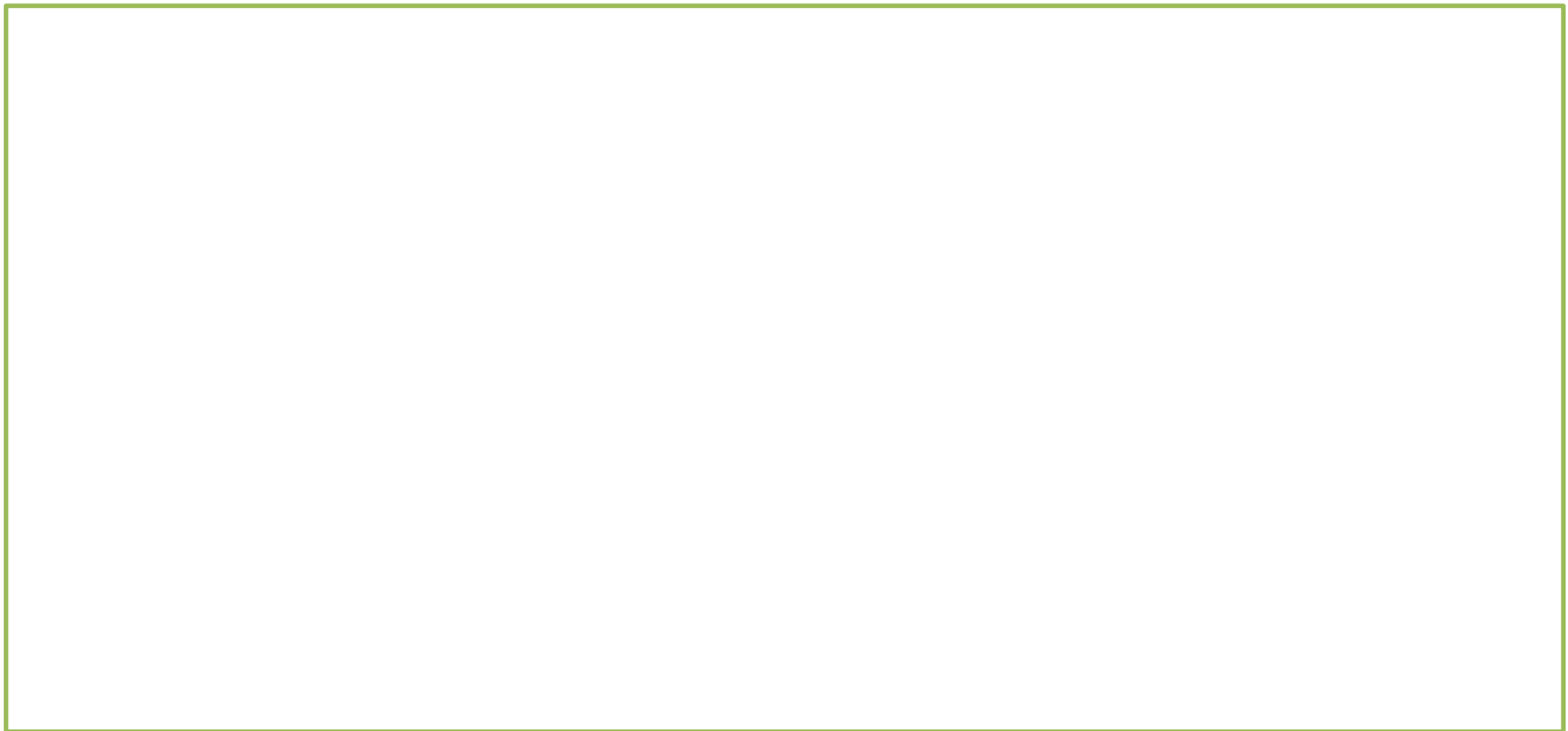
Tutorial 3

2023

**1) What is a replay attack?**

**2) What is Kerberos system? What security services does it provide?**

**3) A simple way for a server to authenticate a client, is to ask for a password. In Kerberos this authentication is not used, why? How does Kerberos authenticate the server and the clients?**



**4) What are the four requirements for Kerberos? What mechanisms are used within Kerberos systems to achieve those requirements?**

Requirement	Mechanism

## 5) What is a public-key certificate?

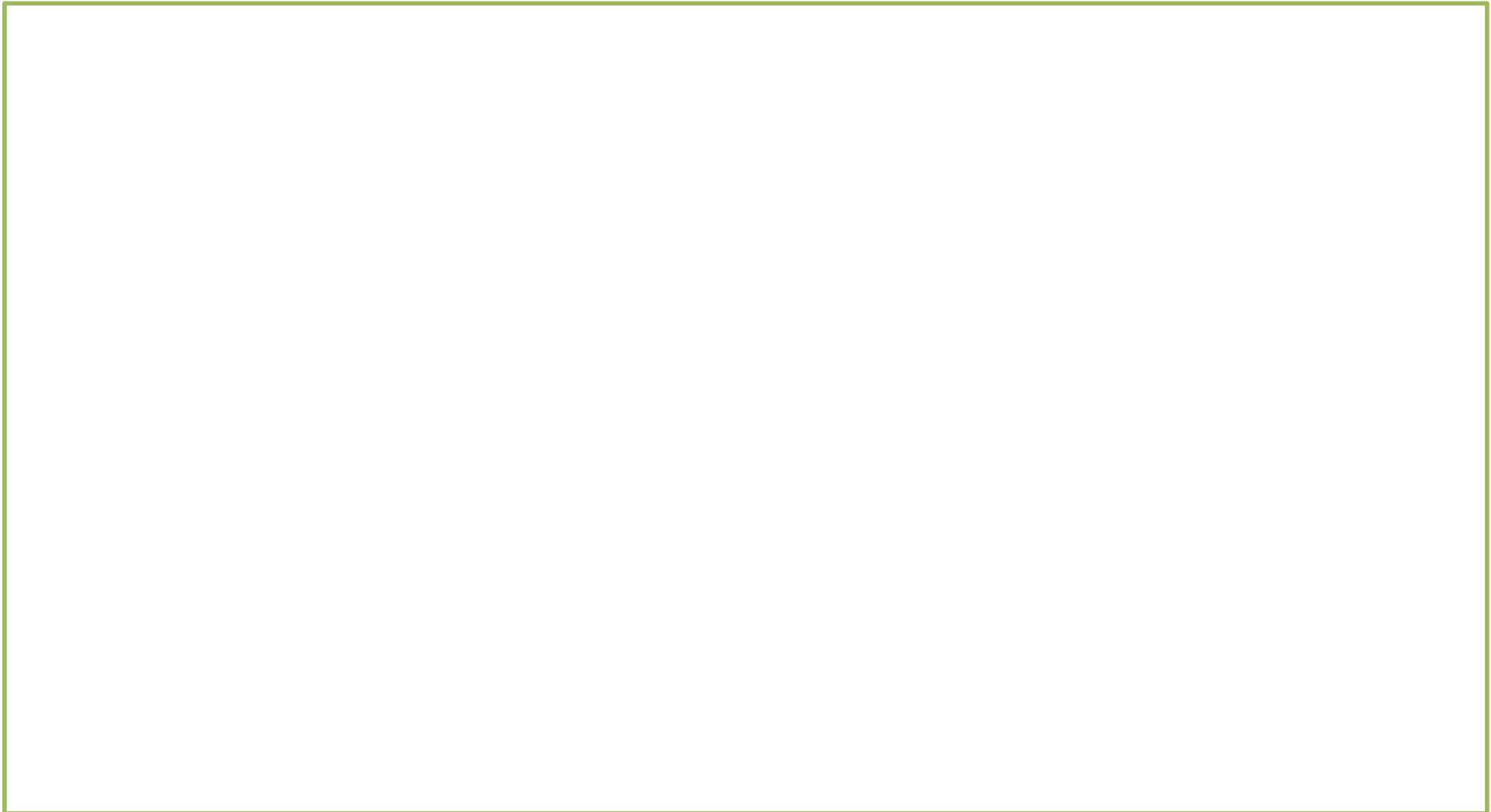


**6) Define the X.509 standard. How is an X.509 certificate revoked?**

## 7) What is IPsec? Why is it significant?



**7) What are the two modes of operations in IPsec? How can they achieve protection against traffic analysis?**



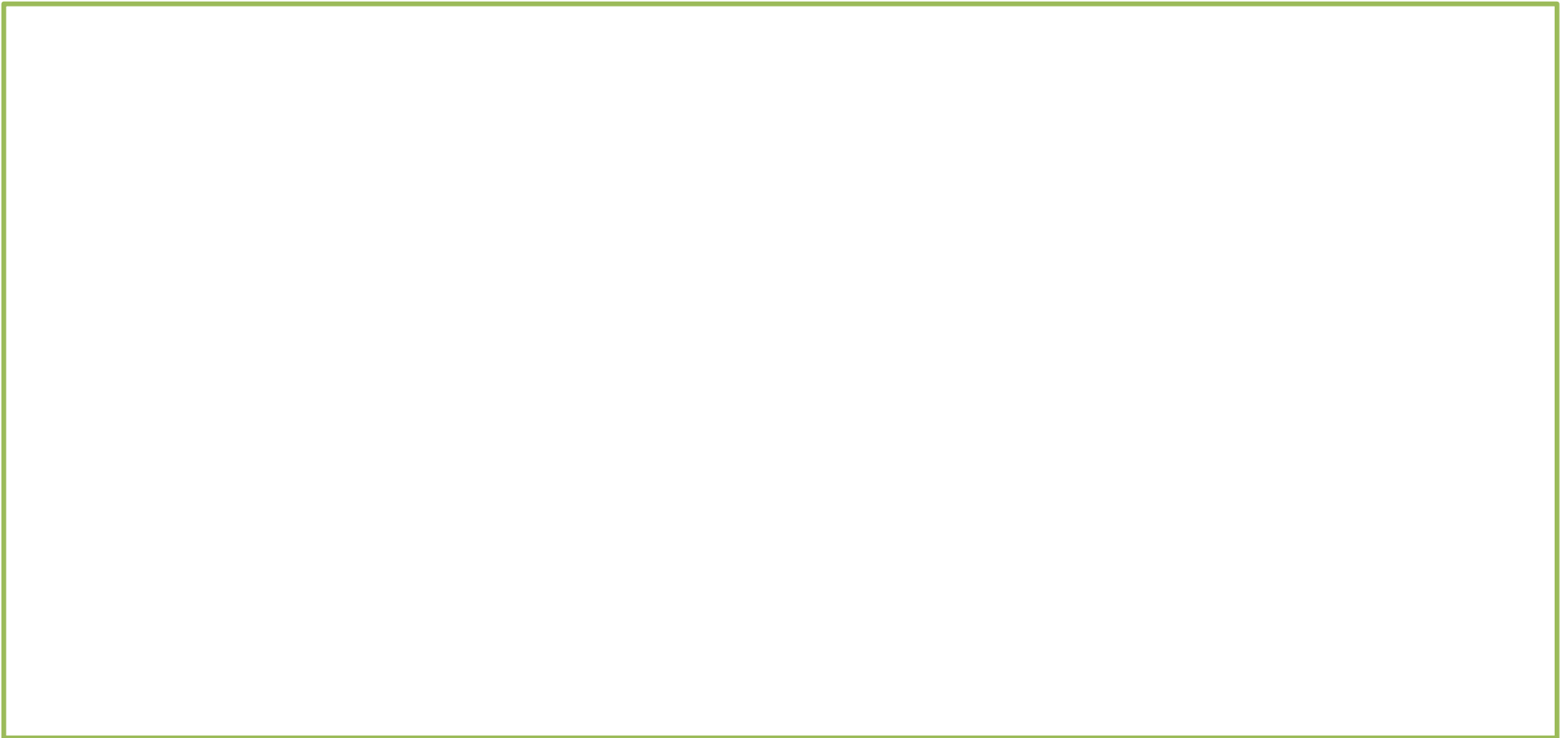


**9) List the services provided by IPSec.**

**10) In IPSec, what is the domain of interpretation (DOI)?**

**11) In IPSec, what is the difference between transport mode and tunnel mode?**

**12) What are the parameters used to characterise the nature of a particular SA?**

A large, empty rectangular box with a thin green border, occupying the lower half of the slide. It is intended for a user to write their answer to the question above it.

**13) What are the roles of the Oakley key determination protocol and ISAKMP in IPsec?**

Questions?