0. Motivation and topics

Cryptography scientific study of techniques for securing digital information, transactions, and distributed computations.

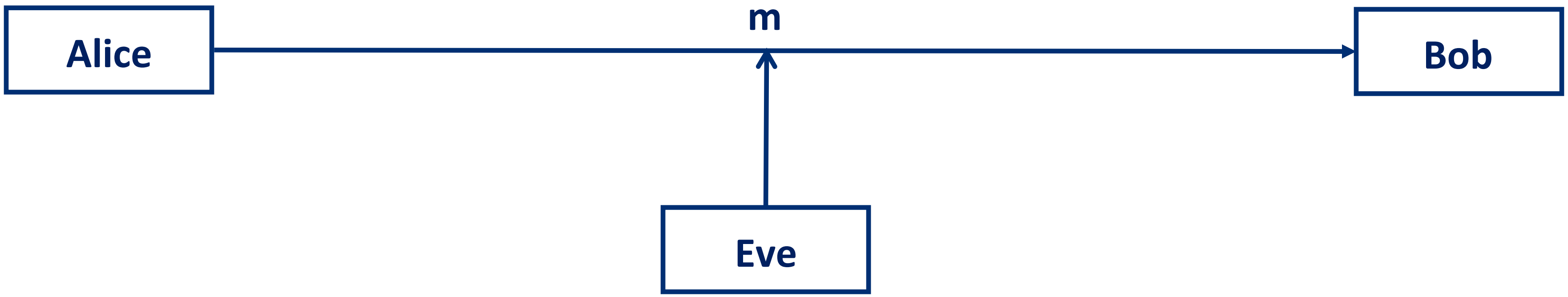
4 main goals

- confidentiality
- integrity
- authenticity
- non-repudiation

Course concentrates on confidentiality and encryption schemes.

Second part of semester: Course on Cryptographic Protocols discusses the other three topics

Scenario and encryption schemes



Scenario and encryption schemes

Definition 0 A private or symmetric encryption scheme consists of three algorithms Gen, Enc, Dec.

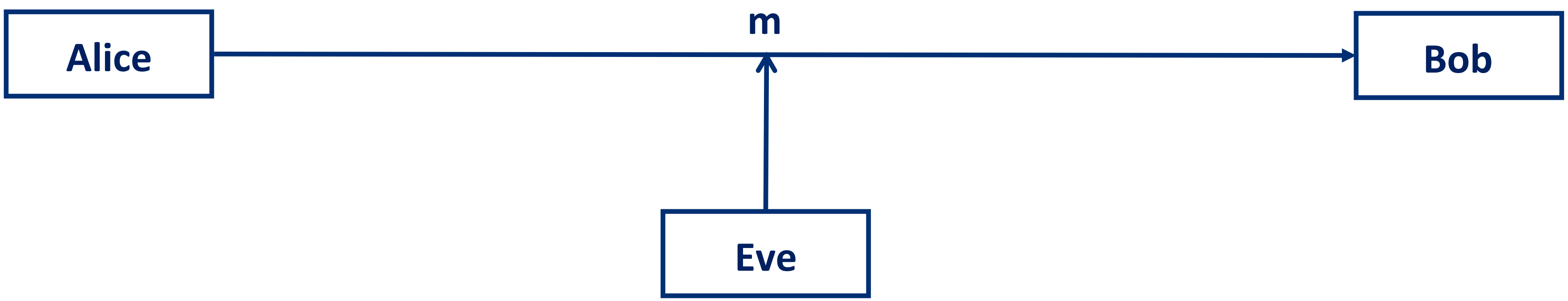
1. The key generation algorithm outputs a key k, according to some distribution on the key space K.

2. The encryption algorithm Enc, on input a key k and a plaintext message m from message space P, outputs a ciphertext c, $\mathrm{Enc}_k(m) =: c$.

3. The decryption algorithm Dec, on input a key k and a ciphertext c from a cipher space C, outputs a plaintext message m, $\mathrm{Dec}_k(c) =: m$.

$$\forall k \in K, m \in P : \mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

Scenario and encryption schemes

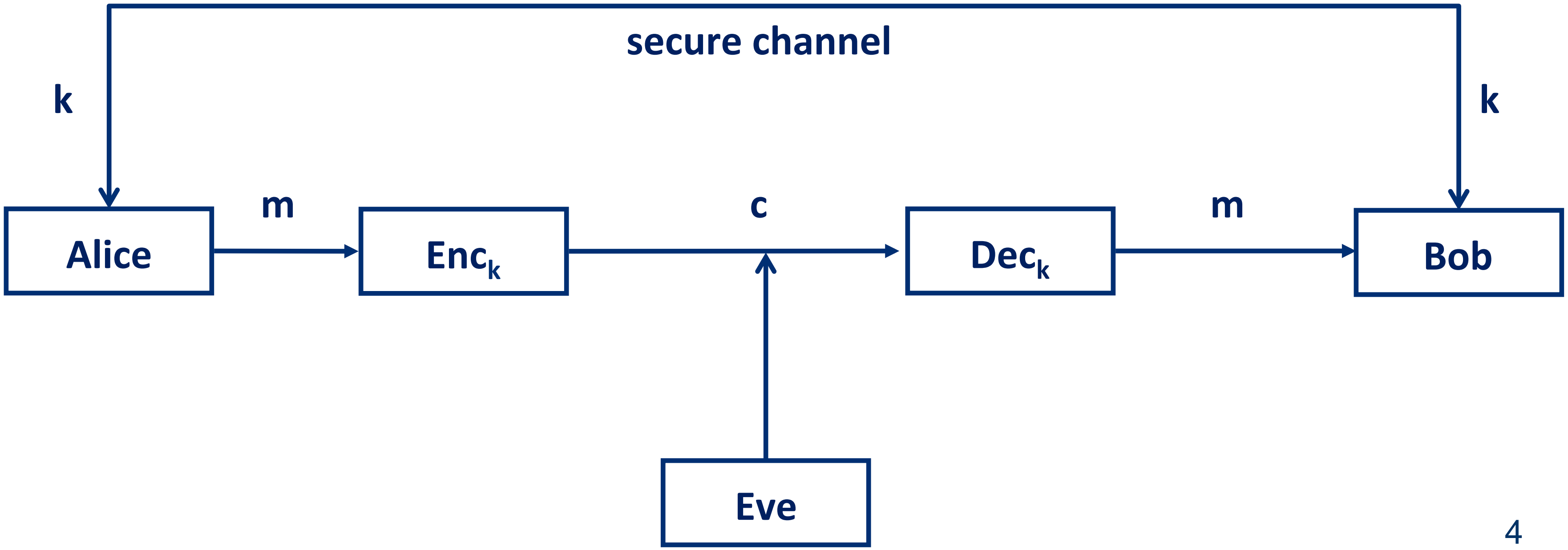


Alice

m

Bob

Eve



secure channel

k

k

Alice

m

Enc_k

c

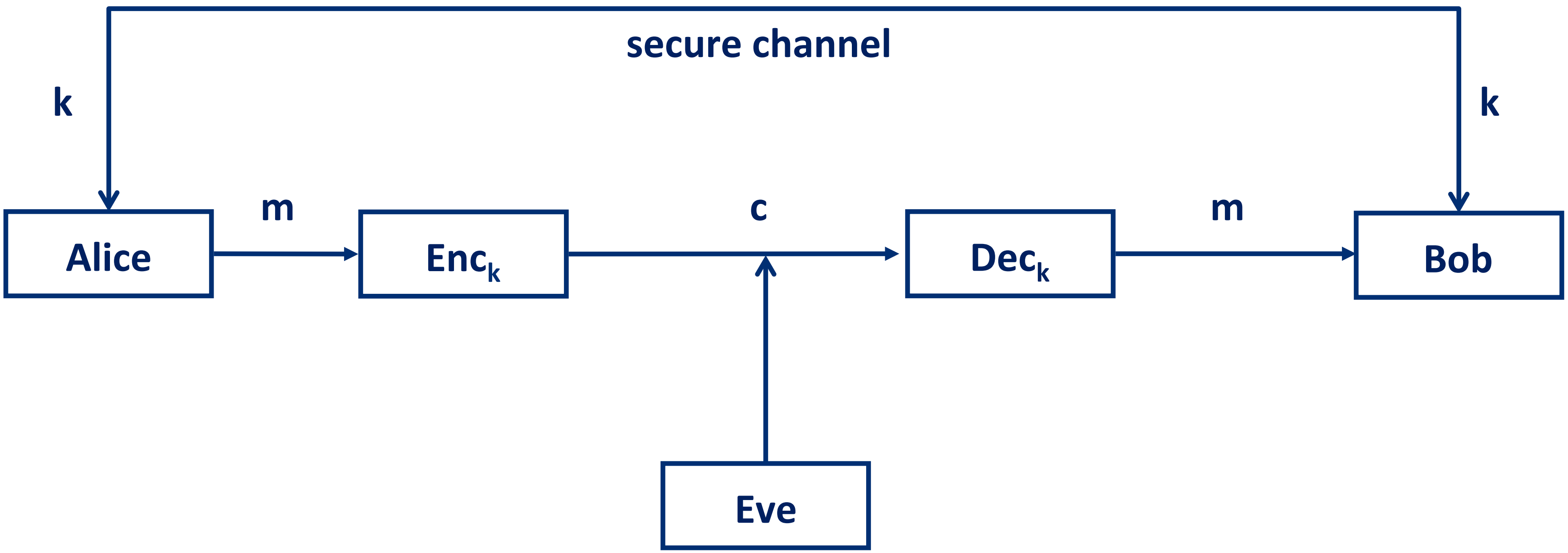
Dec_k

m

Bob

Eve

Scenario and encryption schemes



Security Eve seeing c should learn almost nothing about m.

What does this mean exactly?

How can we achieve this?

$\}$ ➔ This course!

Basic principles

0. Principle (Kerckhoff) The encryption scheme must not be required to be secret and must be able to fall into the hands of the adversary without inconvenience.

1. Principle One must formulate a rigorous and precise definition of security for a given cryptographic problem.

2. Principle If the security of a cryptographic construction relies on an unproven assumption, this must be stated precisely.

3. Principle Cryptographic constructions require rigorous proofs of security with respect to the security definition and the underlying assumptions.

Assumptions

1. Concrete assumptions „The following mathematical/ computational problem is hard to solve.“

➔ factoring, discrete logarithms

2. General assumptions „Computationally hard problems of the following type exist.“

➔ languages in $\mathrm{NP} \setminus \mathrm{P}$ exist, one-way functions exist.

mostly follow 2. ➔ foundations of cryptography

Prerequisites

- elementary probability theory
- algorithm theory
- basic complexity theory
- very basic number theory

Organization

Information about this course

http://cs.uni-paderborn.de/cuk/lehre/veranstaltungen/ss-2017/cryptography-provable-security/

Here you find

- **handouts**
- **slides**
- **literature**
- **announcements**

Schedule

- **Lectures are Tuesdays 11am – 1pm, 2pm – 4pm**
- **Tutorials are Tuesdays 4pm – 6pm**