0. Motivation and topics

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

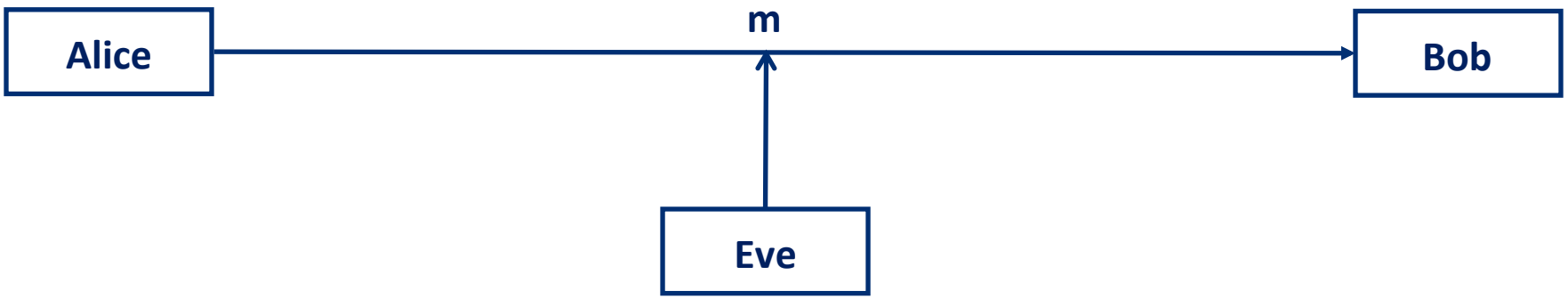
4 main goals

- 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.

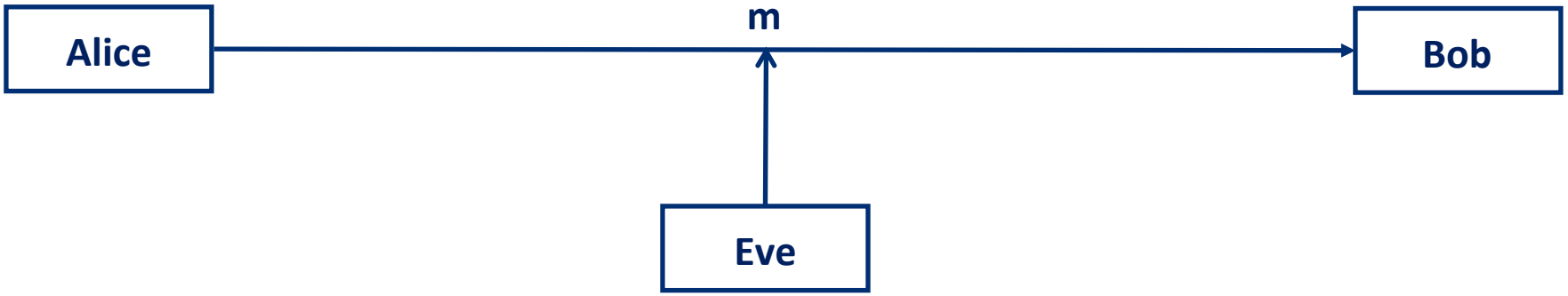
1. The key generation algorithm outputs a key k, according to some distribution on the key space K.

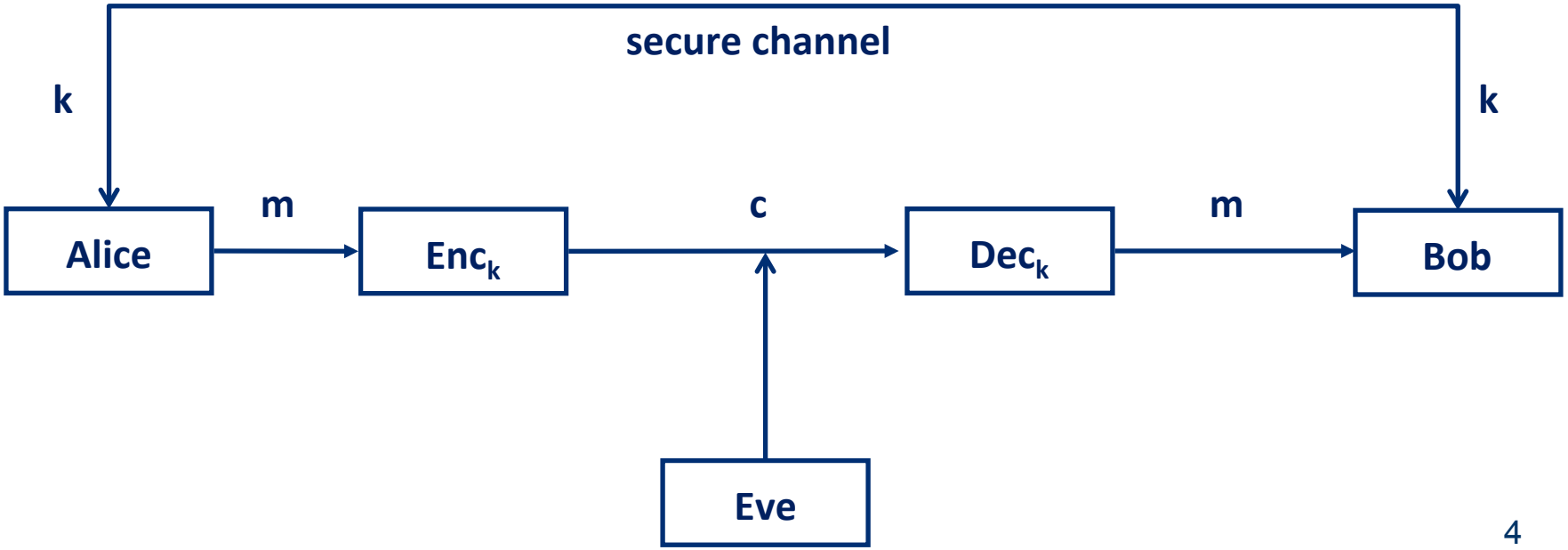
2. The encryption algorithm Enc, on input a key k and a plaintext message m from message space P, outputs a ciphertext c, $Enc_k(m) =: c$.

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

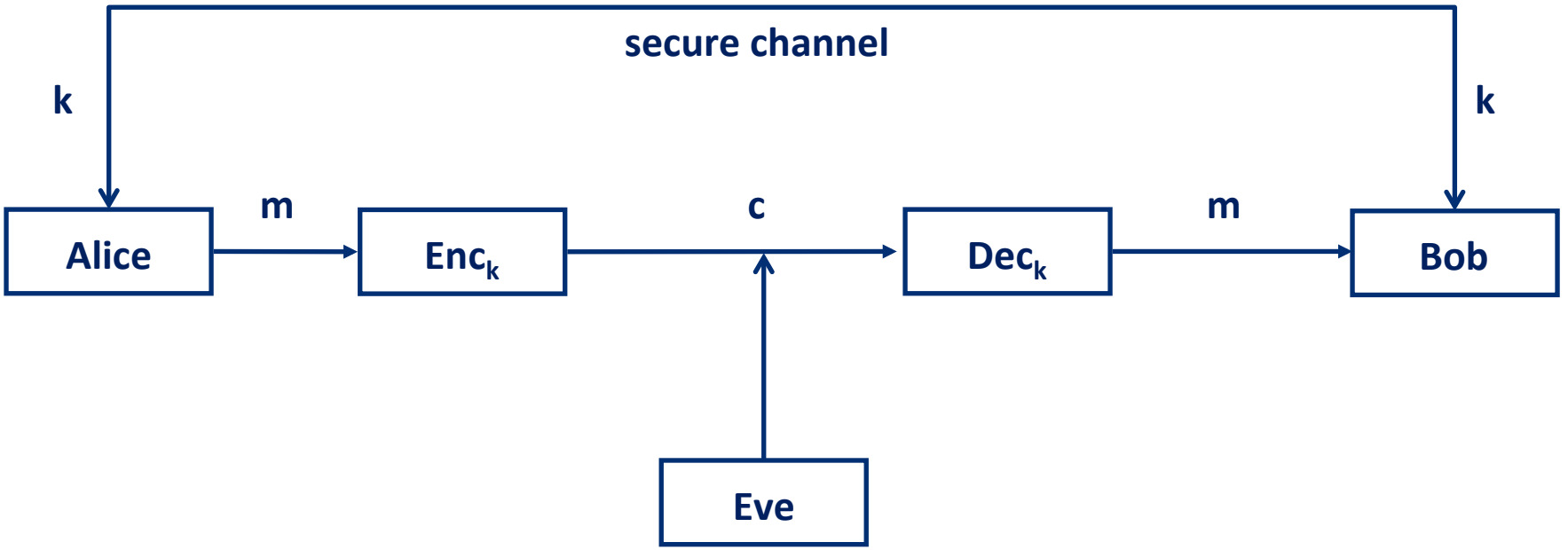
$$\forall k \in K, m \in P : Dec_k(Enc_k(m)) = m$$

Scenario and encryption schemes





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 NP\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-2016/cryptography-provable-security/

Here you find

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

Schedule

- Due to time conflicts lectures and tutorials have to be reorganized
- Lectures are Tuesdays 11am – 1pm, 2pm – 4pm
- Tutorials are Tuesdays 4pm – 6pm

- From 9am – 11am room F2.425 is reserved for the particiapants of this course
- During this time you can discuss exercises from the handouts
- Peter, Nils, and myself are avaliable for questions during this time