Modulární systém dalšího vzdělávání pedagogických pracovníků JmK v přírodních vědách a informatice
CZ.1.07/1.3.10/02.0024

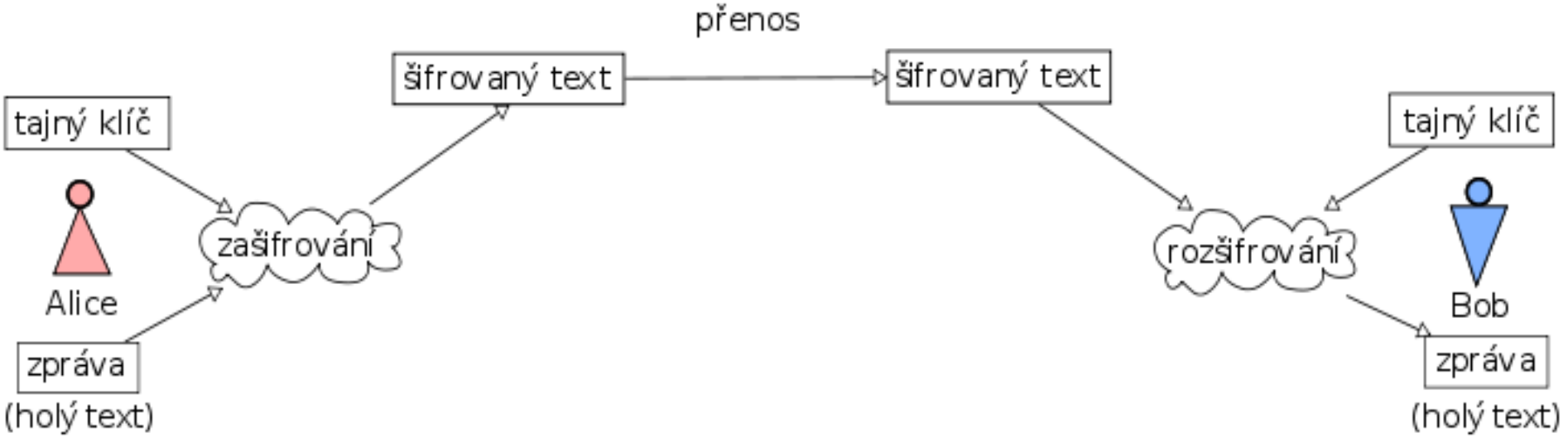
Kryptologie - základní pojmy

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

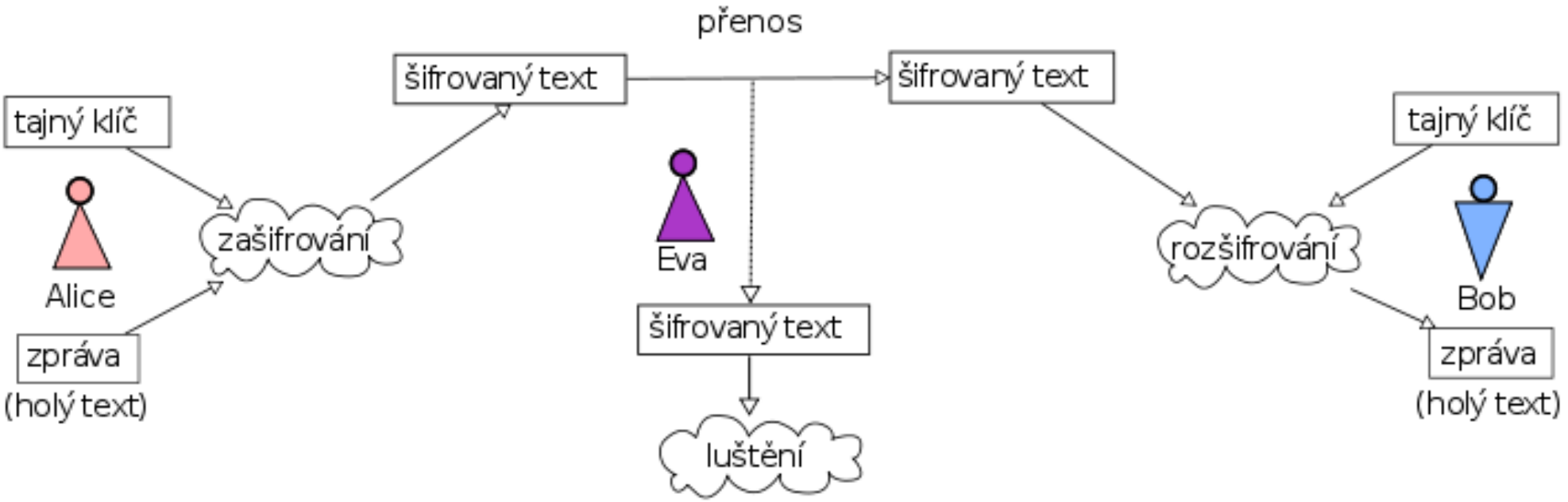
Proč šifrování?

- přenos tajné informace
- příklady použití v moderní době:
  - bankovní karty
  - elektronické bankovnictví
  - počítačová hesla
  - elektronické podpisy
  - ochrana dat
- klasické vs. moderní šifry

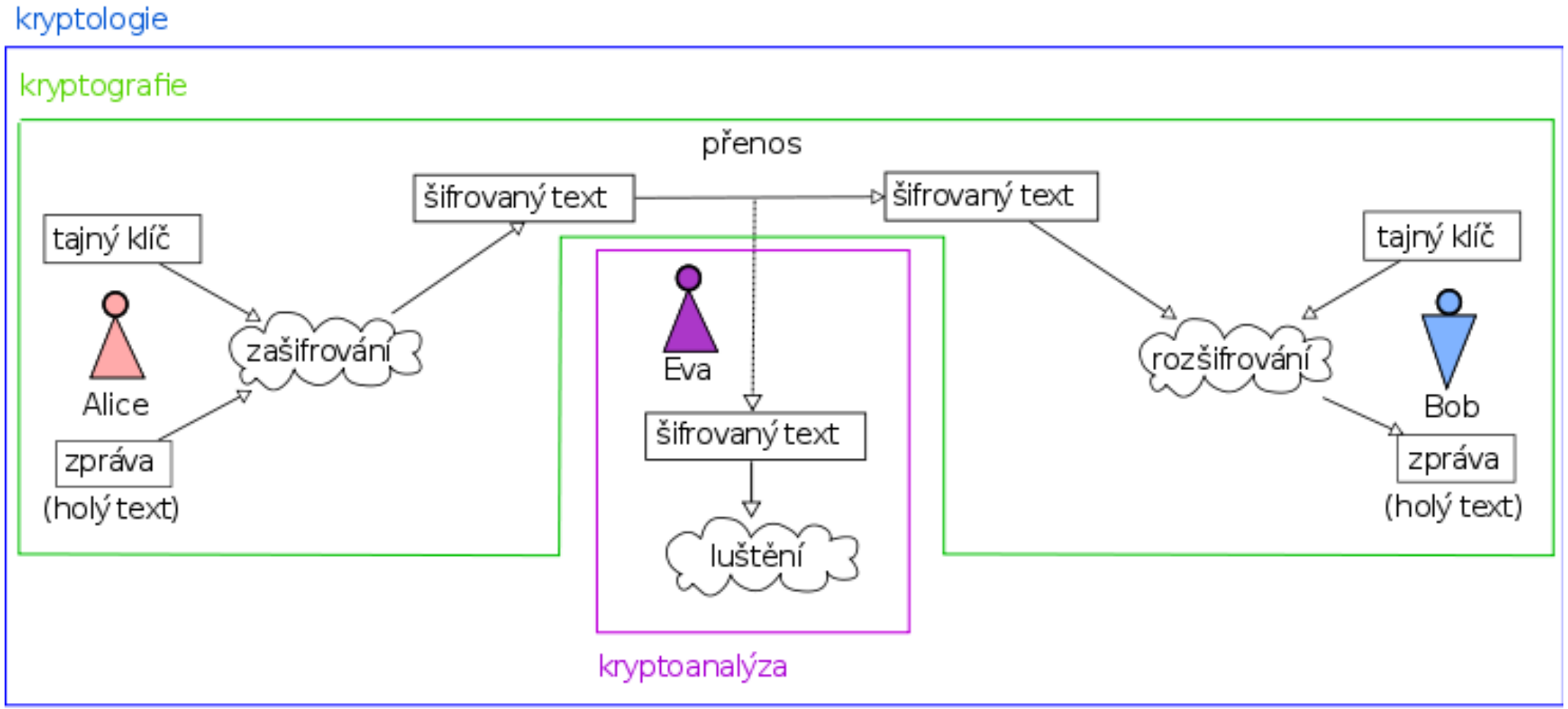
Základní model klasického šifrování



Základní model klasického šifrování



Základní model klasického šifrování



Kód versus šifra

- Kódování: změna reprezentace zprávy, pravidla známá
  - Neslouží k utajení
  - Nemá systém, jen překládá podle slovníku
  - Morseova abeceda, Braillovo písmo, binární kódování...
  - Může předcházet šifrování
- Šifrování: změna zprávy podle určitého principu, algoritmu
  - Cíl je utajení zprávy
- Steganografie
  - Cíl zakrytí existence zprávy