Asymetrická kryptografie

Milan Radojčić

SSPŠaG – KBB

8. prosince 2025

Hlavní body

Hlavní body

Úvod

- Provedeme skok od historické kryptografie do 70. let 20. století.

Změny oproti minulému roku

- Oproti minulému roku je toto téma zkrácené.
- My vynecháme
  - **Pohligovu-Hellmanovu** exponenciální šifru a
  - šifru **ElGamal**.
- Ve skriptech jsou tato témata v sekci zajímavosti.

Hlavní body

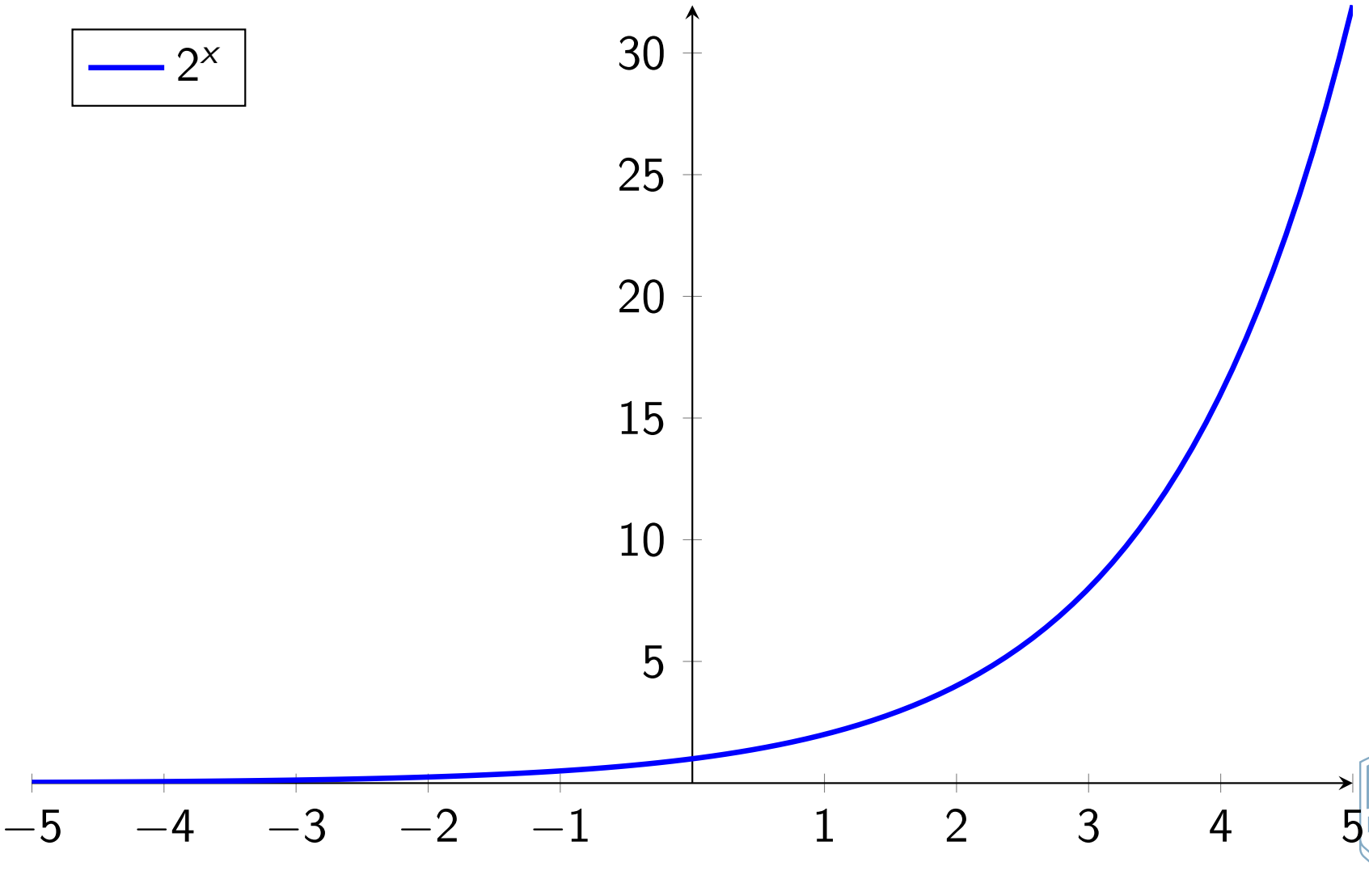
Exponenciála

- Obecná exponenciála je funkce f pro nějaké dané $a \in \mathbb{R}$:

$$f(x) = a^x.$$

- Některé vlastnosti:
  - **Rostoucí**
  - Funkční hodnota je **vždy kladná**

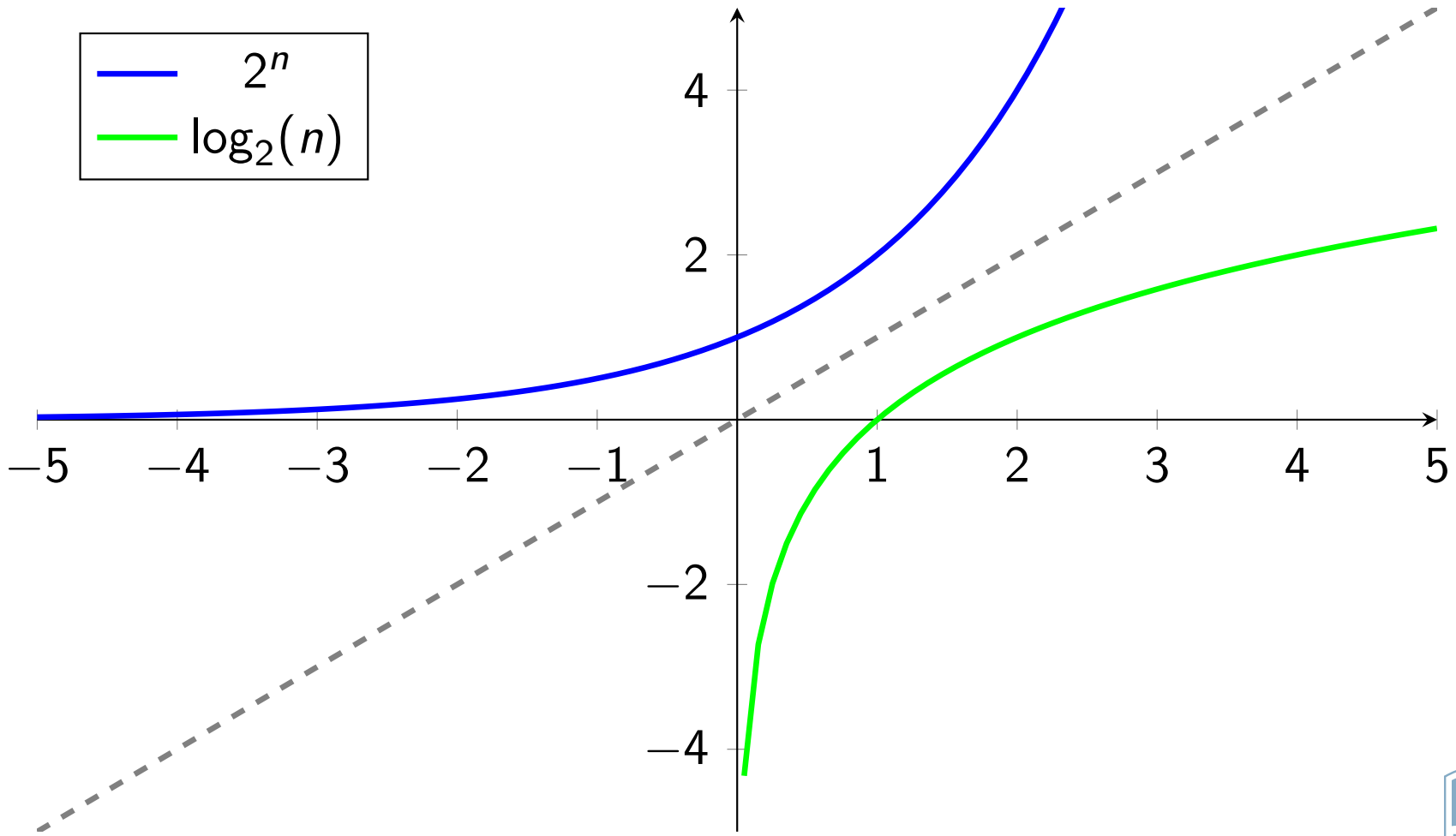
Exponenciála



Logaritmus

- Logaritmus je **inverzní funkcí** k exponenciále.
- Ptáme se „**na kolikátou?**“ musíme umocnit vstup.
  - Například $\log_2(8) = 3$, protože $2^3 = 8$.
- Existují způsoby, jak ho efektivně vypočítat.

Logaritmus



Diskrétní logaritmus

- Stejný případ, ale **modulo** n.
- Známe g, a, n a hledáme e, aby

$$g^e \equiv a \pmod{n}.$$

- Tomu se říká **problém diskrétního logaritmu (DLP)**.
- DLP je (obecně) **těžký na výpočet**!

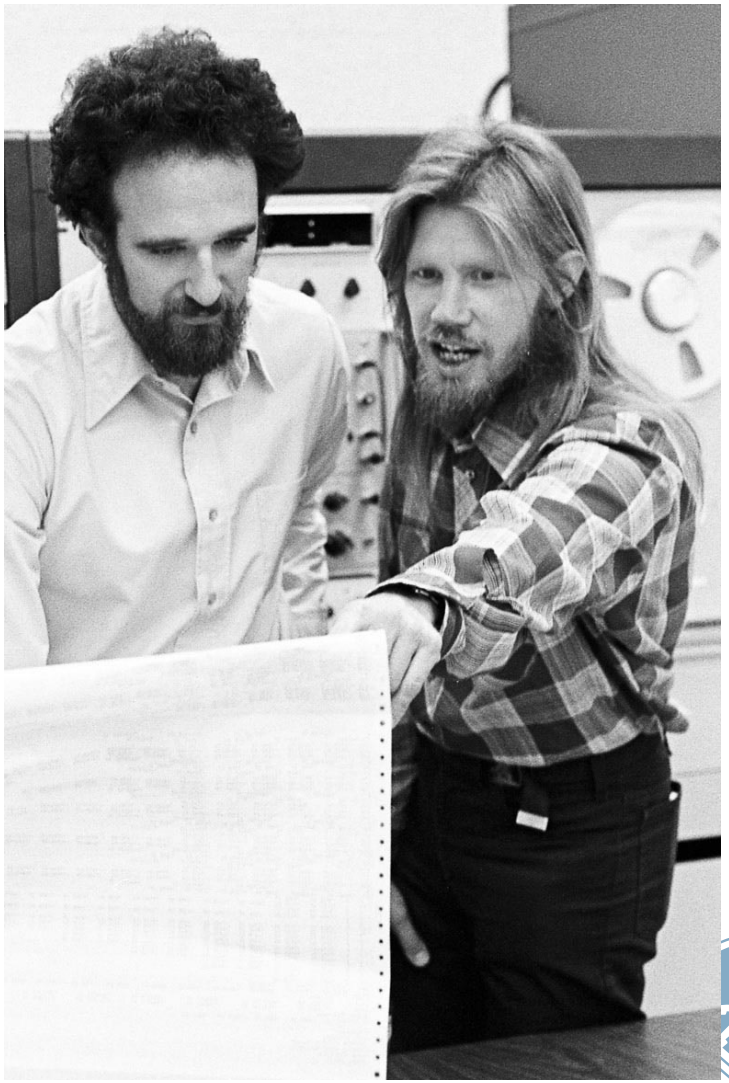
Faktorizace

- Máme složené číslo a hledáme **rozklad na součin prvočísel**.
- Například 77 lze napsat jako $7 \cdot 11$.
- Tohle je také (obecně) **těžé na výpočet**!

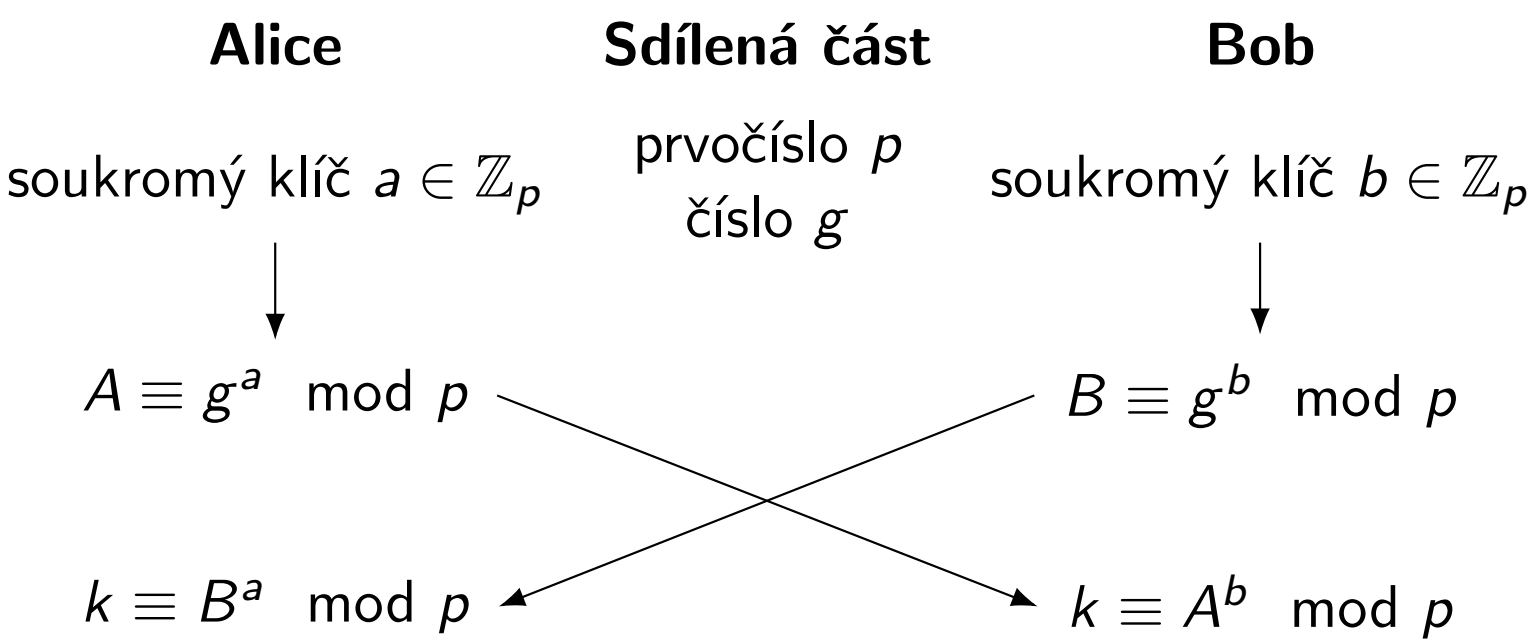
Hlavní body

Diffieho-Hellmanova výměna klíčů

- Publikována v roce 1976.
- Slouží k **zřízení společného klíče**.
- První použití pojmu **veřejného** a **soukromého** klíče.



Jak funguje DHE?



$$k \equiv A^b \equiv (g^a)^b \equiv g^{ab} \equiv (g^b)^a \equiv B^a \pmod{p}$$

Bezpečnost DHE

- Útočník vidí jen p, g, A a B.
- Pro výpočet klíče potřebuje zjistit a nebo b.
- Víme, že $A \equiv g^a \mod p$.
  - Útočník musí spočítat $\log_g A \mod p$.

  $\Rightarrow$ **problém diskrétního logaritmu!**
- Samotný algoritmus je ale **zranitelný na MitM** útoky.
  - Potřeba provést autentizaci.

Poznámky

- Číslo g musí být *generátorem*[1] grupy $\mathbb{Z}_p^*$.
- V praxi se používají **eliptické křivky**.
- Pro bezpečnost na úrovni AES-128[2]:
  - modulus (p) – 3072 bitů
  - soukromé klíče (a a b) – 256 bitů

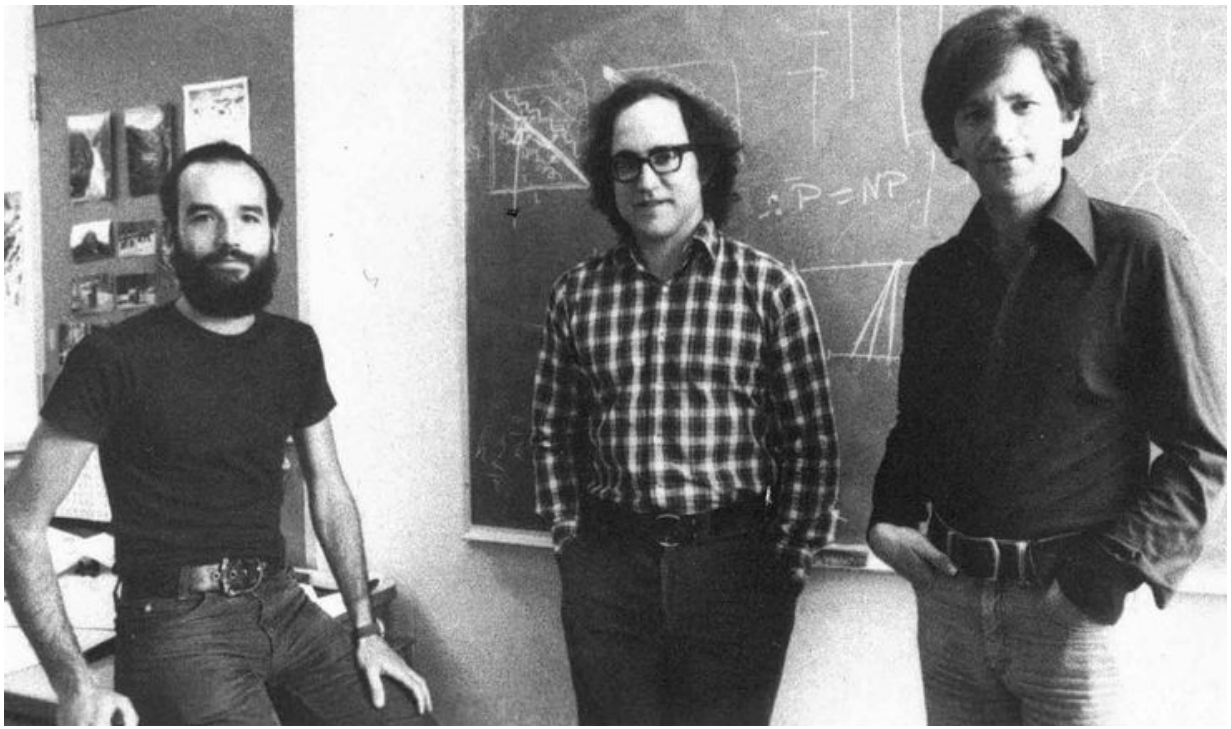
[1] Viz skripta, sekce zajímavosti.

[2] Viz Special Publication 800-57 Part 1 Revision 5, str. 54

Hlavní body

RSA

- Publikováno v roce 1977.
- Asymetrický systém



Jak RSA funguje?

Jako první věc potřebujeme **vygenerovat klíče**.

1. Vybereme dvě prvočísla p a q a spočítáme $n = pq$.
2. Spočítáme $\varphi(n) = (p-1)(q-1)$.
3. Vybereme e takové, že $2 < e < \varphi(n)$ a $\gcd(\varphi(n), e) = 1$.
4. Vypočítáme $d \equiv e^{-1} \pmod{\varphi(n)}$.

Jako veřejný klíč použijeme dvojici (e, n) a jako soukromý klíč dvojici (d, n).

Jak RSA funguje?

Pro **šifrování** pak platí

$$c \equiv p^e \pmod{n}.$$

a pro **dešifrování**

$$p \equiv c^d \pmod{n}.$$

Jak to, že RSA funguje?

- Chceme se přesvědčit, že RSA opravdu funguje.
  - Tzn. když zašifruju a dešifruju nějakou zprávu, tak dostanu zpět originální zprávu.
- Tedy chceme dokázat, že $(m^e)^d \equiv m \pmod{n}$.

Jak to, že RSA funguje?

- K důkazu budeme potřebovat následující fakta:
  - $de \equiv 1 \pmod{\varphi(n)}$, což je ekvivalentní s $de = 1 + l \cdot \varphi(n)$, pro nějaké $l \in \mathbb{Z}$.
  - Eulerova věta

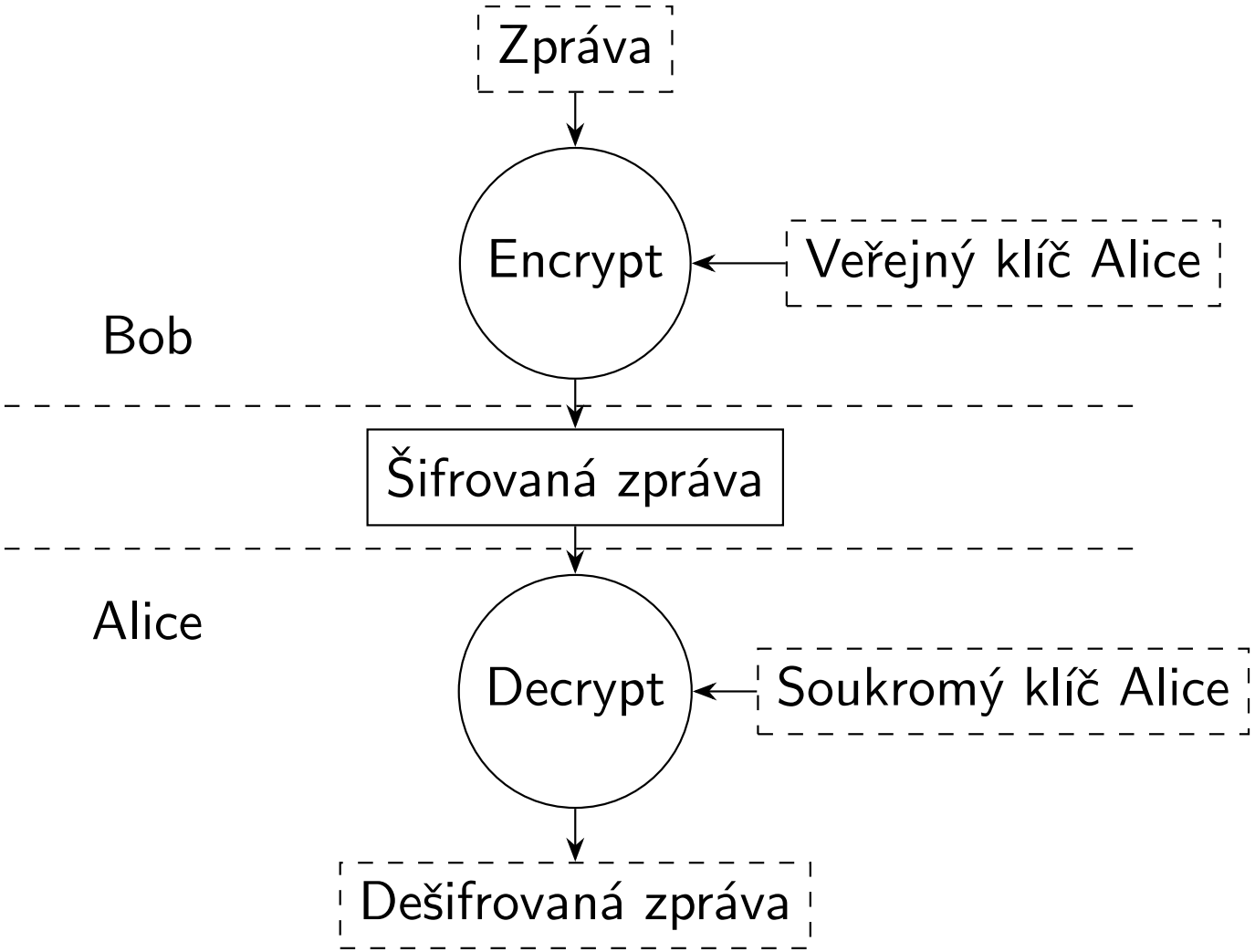
Jak to, že RSA funguje?

Ukažme, že $(m^e)^d \equiv m \pmod{n}$:

$$(m^e)^d \equiv m^{ed} \equiv m^{1+l\cdot\varphi(n)} \equiv m \cdot \left(m^{\varphi(n)}\right)^l \equiv m \cdot 1^l \equiv m \pmod{n}$$

Pozor! Tento důkaz neplatí pro $m = p$ nebo $m = q$. (Lze dokázat, že to platí i pro ně, jenom ne tímto způsobem.)

Asymetrická kryptografie - šifrování



Asymetrická kryptografie - podpis