# Kryptografická bezpečnost

Milan Radojčić

SSPŠaG – KBB

24. února 2026

# Hlavní body



# Hlavní body



# Bezpečnost asymetrických kryptosystémů

- Asymetrické kryptosystémy mají **v jádru nějaký těžký problém**.
  - DHE: Problém diskrétního logaritmu
  - RSA: Problém faktorizace
- Nemáme žádnou „garanci“, že jsou těžké!
  - Věříme, že jsou těžké, protože se zkoumají delší dobu.
- U symetrických šifer je analýza bezpečnosti složitější.

# Hlavní body



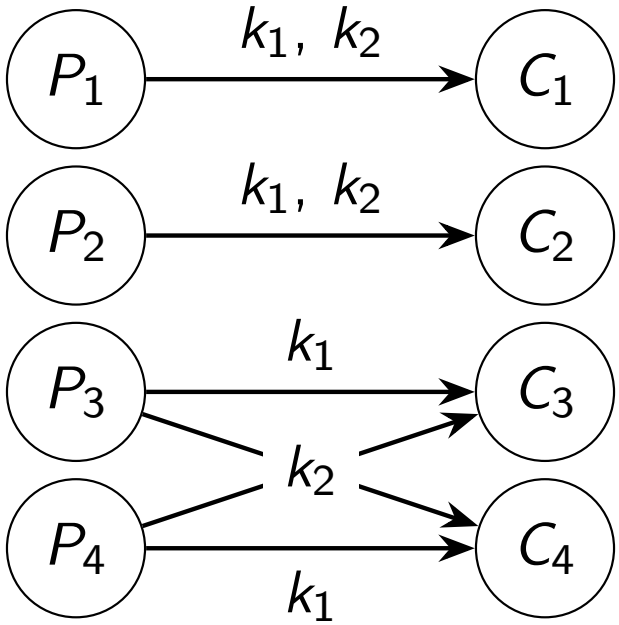
# Absolutní bezpečnost

Naše cíle v této sekci budou:

1. Definovat co je to absolutně bezpečná šifra.
2. Existují nějaké absolutně bezpečné šifry?
3. Zformulovat podmínky na absolutní bezpečnost.

# Absolutní bezpečnost

Budeme se zamýšlet nad následujícími diagramy.

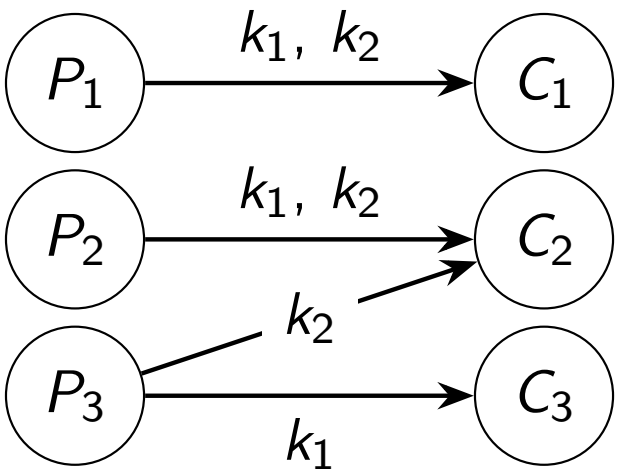


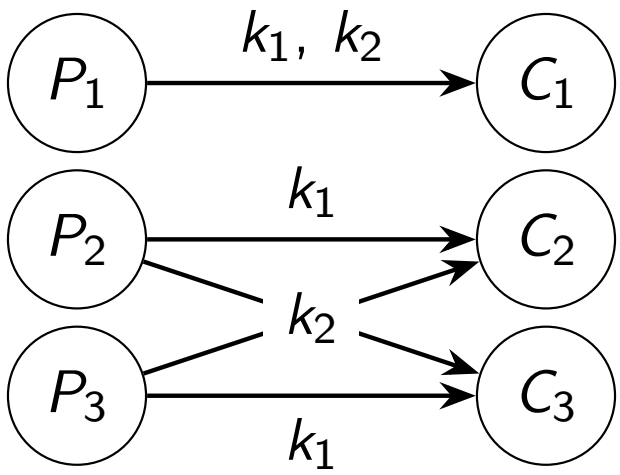

- $C_1, \ldots, C_4$ jsou šifrové texty, $P_1, \ldots, P_4$ jsou otevřené texty, $k_1$, $k_2$ jsou klíče.
- $C_1$ se tedy pomocí klíčů $k_1$ i $k_2$ zašifruje na $P_1$.
- $C_3$ se klíčem $k_1$ zašifruje na $P_3$ a klíčem $k_2$ na $P_4$.

# Absolutní bezpečnost

## Cvičení

Který z těchto diagramů není validní?



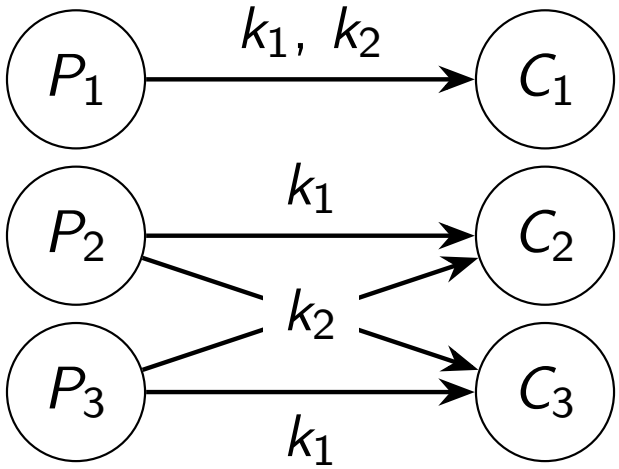




# Absolutní bezpečnost

Definujeme **valenci** šifrového textu val($C_i$) jako *počet otevřených textů, na které se $C_i$ může dešifrovat*.

## Cvičení

Kolik je val($C_1$)? Kolik val($C_2$)?

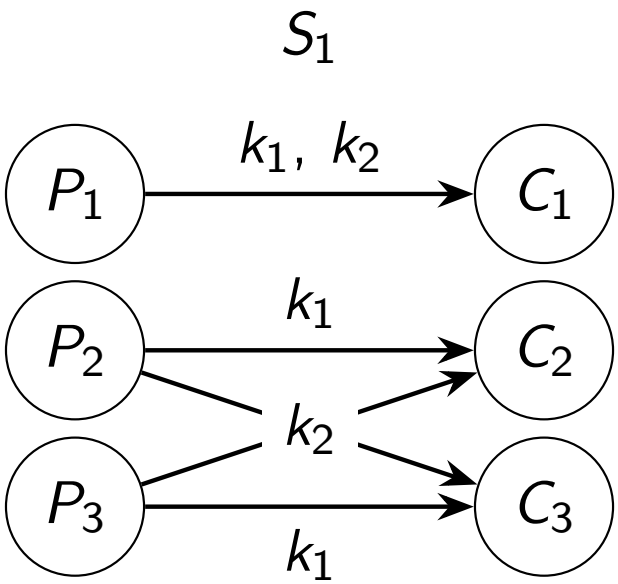


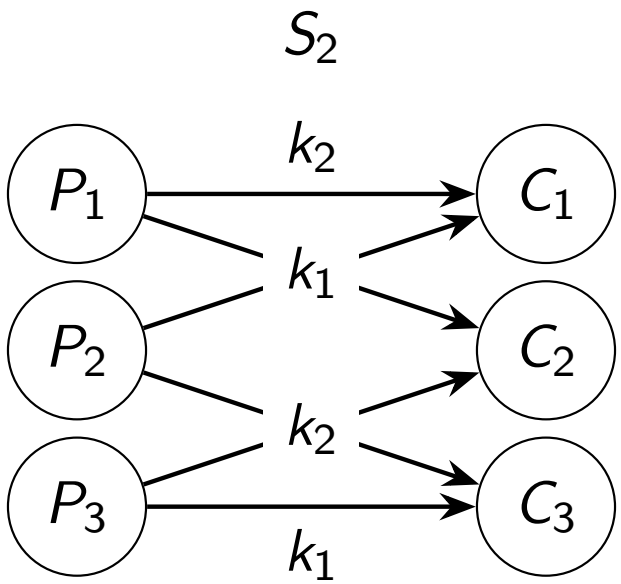

# Absolutní bezpečnost

**Valenci kryptosystému** val($S$) definujeme jako *minimální valenci přes všechny šifrové texty*.

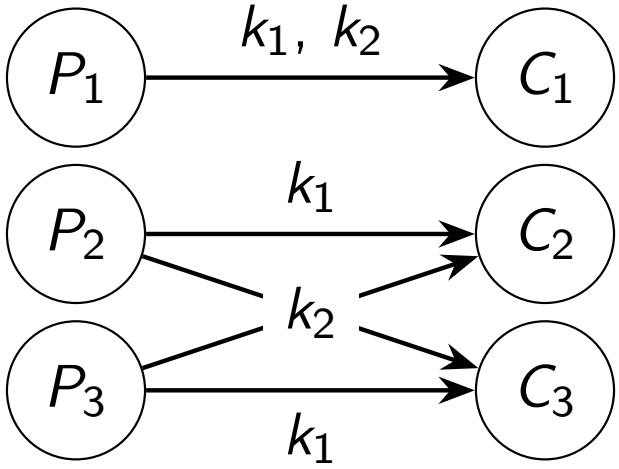
## Cvičení

Kolik je val($S_1$)? Kolik val($S_2$)?




# Absolutní bezpečnost




Označíme počet klíčů $K$ a počet otevřených textů $N$.

## Cvičení

Co můžeme říct o valenci kryptosystému v poměru k počtu klíčů $K$ a počtu otevřených textů $N$?

Platí $1 \leq \mathrm{val}(S) \leq K \leq N$.

# Úrovně důvěrnosti

Podle valence můžeme kryptosystémy rozdělit do několika kategorií:

1. **Maximální důvěrnost/Absolutní bezpečnost**: $\mathrm{val} = N$
2. **Redukovaná důvěrnost**: $1 < \mathrm{val} < N$
3. **Minimální důvěrnost**: $\mathrm{val} = 1$

## Cvičení

Jaký je výsledek útoku hrubou silou na absolutně bezpečný systém? Zjistíme něco?

# Nutné podmínky absolutní bezpečnosti

## Cvičení

Může být systém absolutně bezpečný když $K < N$?

## Nutné podmínky absolutní bezpečnosti

- $K = N$ (počet klíčů = počet zpráv)
- Vybíráme náhodně ze všech klíčů.
- Nesmíme žádný klíč použít dvakrát.

# Absolutně bezpečné šifry

## One-time pad jako absolutně bezpečná šifra

1. Zafixujme $c = 0110$, pomocí jakého klíče se dešifruje na $p = 0101$?
2. Jaký je postup pro nalezení klíče pro daný plaintext?
3. Lze najít takový klíč vždy?

# Absolutně bezpečné šifry

## Vigenèrova šifra jako absolutně bezpečná šifra

1. Zafixujme $c = \text{ABC}$, pomocí jakého klíče se dešifruje na $p = \text{PES}$?
2. Jaký je postup pro nalezení klíče pro daný plaintext?
3. Lze najít takový klíč vždy?

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

# Šifrování v praxi

## Cvičení

Jsou šifry jako ChaCha20 nebo AES, které používají 128-256 bitové klíče absolutně bezpečné? Proč?

## Výpočetně bezpečné šifry

V praxi používáme **výpočetně bezpečné šifry** — na útok hrubou silou je potřeba nezvladatelně mnoho prostředků.

# Hlavní body



# Co znamená bezpečnost?

## Cvičení

Zamyslete se, jak bychom mohli definovat bezpečnost.

- Co znamená prolomení šifry?
- K jakým informacím může mít přístup útočník?

# Modely útoku

- **COA**: ciphertext only attack
  - Útočník vidí jen šifrové texty.
- **KPA**: known plaintext attack
  - Útočník vidí šifrové texty *a příslušné otevřené texty*.[1]
- **CPA**: chosen plaintext attack
  - Útočník se může *dotazovat* na příslušné šifrové texty k daným otevřeným textům.
- **CCA**: chosen ciphertext attack
  - Oproti minulému smíme i dešifrovat.

[1] Nemá ale kontrolu nad tím, jaké plaintexty jsou zašifrovány.

# Bezpečnostní cíle

- **IND**: nerozpoznatelnost (*indistinguishability*)
  - *Šifrové texty by měly být nerozpoznatelné od náhody.*
- **NM**: *„netvárnost“ (nonmalleability)*
  - *Při změně šifrového textu by nemělo jít předpovědět co se stane s otevřeným textem.*

Modely útoku a bezpečnostní cíle kombinujeme dohromady.

- **IND-CPA**: sémantická bezpečnost
  - Šifrové texty by neměly „leakovat“ informaci, když je klíč tajný.
- **NM-CCA**
- atd.

# Bezpečnostní cíle

## Cvičení

Je one-time pad NM-CCA?

# Sémantická bezpečnost (IND-CPA)

| | **Vyzyvatel** | **Protivník**[2] |
|---|---|---|
| 1. | Může provádět libovolné šifrovací dotazy. | |
| 2. | Vybere dva plaintexty $p_1$ a $p_2$ a pošle je protivníkovi. | |
| 3. | | Vybere si z $p_1$ a $p_2$ jeden pt, ten zašifruje. Zašifrovaný ct $c_i = E(p_i)$ pošle vyzyvateli. |
| 4. | Snaží se uhodnout $i$.[3] | |

[2] Challenger a adversary

[3] Tedy který plaintext byl zašifrován.

# Sémantická bezpečnost (IND-CPA)

## Cvičení

Je AES-ECB IND-CPA?

## Důsledek

Pro IND-CPA potřebujeme *nedeterministické šifrování* — ten samý plaintext se zašifruje vždy jinak na základě nonce/náhody.

## Fakt

AES-CTR je IND-CPA.

# Výpočetní bezpečnost

- V předchozím jsme si řekli, že prakticky používané šifry nejsou absolutně bezpečné.
- Jak jejich bezpečnost tedy popisujeme?
  - V praxi existují limity na to, jaké výpočetní prostředky máme.

## Výpočetní bezpečnost

Řekneme, že šifra je $(t, \varepsilon)$-bezpečná, kde

- $t$ je limit počtu „operací“, které útočník může provádět,
- $\varepsilon$ je pravděpodobnost úspěchu,

právě tehdy, když pro každý pár otevřeného textu a šifrového textu nelze najít správný klíč s použitím maximálně $t$ operací s pravděpodobností vyšší než $\varepsilon$.

# Výpočetní bezpečnost

## Limity výpočetní bezpečnosti

Šifra, používající $n$ bitový klíč, je nanejvýš $(t, t/2^n)$-bezpečná. Proč?

## Důsledek

- Ideálně chceme, aby šifry byly $(t, t/2^n)$-bezpečné.
- Jakýkoliv jiný útok musí využívat nedokonalosti konstrukce.

# Vyjádření bezpečnosti v bitech

- Předpokládejme $\varepsilon$ blízko 1.
- Pokud k tomu potřebujeme $t = 2^n$ kroků, tak mluvíme o $n$-bitové bezpečnosti.

# Hlavní body



# Typy bezpečnosti

- **Absolutní bezpečnost** – One-time pad, Vigenère s náhodným klíčem
  - Víme o nich, že nemůžou být prolomeny.
  - Většina šifer toto ale nesplňuje, uchylujeme se k *výpočetní bezpečnosti*.
- **Vztah k (matematickému) problému** – DHE, RSA
  - Systém postavíme nějakým způsobem na těžkém problému.
  - Nemusíme mít garanci, že nejde prolomit jiným způsobem!
- **Pravděpodobná/heuristická bezpečnost** – AES, ChaCha20
  - Šifry jsou delší dobu veřejně známé a nikomu se je nepodařilo prolomit.
  - Zase nemáme žádnou garanci.

# Poznámky

Je nějaký typ bezpečnosti „lepší“? Nejde říct...

- **Absolutní bezpečnost** – Šifry jsou garantovaně bezpečné.
  - Na druhou stranu jsou velké problémy s distribucí klíče.
  - Proponenti kvantové distribuce klíče říkají, že právě tohle může vyřešit.
  - Na druhou stranu: jak rychle lze klíč přenášet?
- **Vztah k matematickému problému** – Máme alespoň nějakou intuici, proč by mohly být bezpečné.
  - Většinou neřeší praktickou implementaci — ta bývá obtížná.
- **Pravděpodobná bezpečnost** – Vycházíme z nějaké intuice a praxe.
  - Oproti více „matematičtějším“ šifrám bývají jednodušší na implementaci.