

Vypracované otázky k MSZ pro rok 2022

Specializace NNET

27. dubna 2022

Vladimír Dušek, xdusek27

Specializace Počítačové sítě – NNET

1. Architektura superskalárních procesorů a algoritmy zpracování instrukcí mimo pořadí, predikce skoků.
2. Paměťová konzistence a předbíhání operací čtení a zápisu, podpora virtuálního adresového prostoru.
3. Datový paralelismus SIMD, HW implementace a SW podpora.
4. Architektury se sdílenou pamětí UMA a NUMA, zajištění lokality dat.
5. Problém koherence pamětí cache na systémech se sdílenou pamětí, protokol MSI.
6. Paralelní zpracování v OpenMP: Smyčky, sekce a tasky a synchronizační prostředky.
7. Pravděpodobnost, podmíněná pravděpodobnost, nezávislost.
8. Náhodná proměnná, typy náhodné proměnná, funkční a číselné charakteristiky, významná rozdělení pravděpodobnosti.
9. Bodové a intervalové odhady parametrů, testování hypotéz o parametrech.
10. Vícevýběrové testy, testy o rozdělení, testy dobré shody.
11. Regresní analýza.
12. Markovské řetězce a základní techniky pro jejich analýzu.
13. Randomizované algoritmy (Monte Carlo a Las Vegas algoritmy).
14. Problém generalizace strojového učení a přístup k jeho řešení (trénovací, validační a testovací sada, regularizace, předtrénování, multi-task learning, augmentace dat, dropout, ...)
15. Generativní modely a diskriminativní přístup ke klasifikaci (gaussovský klasifikátor, logistická regrese, ...)
16. Neuronové sítě a jejich trénování (metoda gradientního sestupu, účelová (loss) funkce, výpočetní graf, aktivační funkce, zápis pomocí maticového násobení, ...)
17. Neuronové sítě pro strukturovaná data (konvoluční a rekurentní sítě, motivace, základní vlastnosti, použití)
18. Prohledávání stavového prostoru (informované a neinformované metody, lokální prohledávání, prohledávání v nejistém prostředí, hraní her, CSP úlohy)
19. Klasifikace formálních jazyků (Chomského hierarchie), vlastnosti formálních jazyků a jejich rozhodnutelnost.
20. Konečné automaty (jazyky přijímané KA, varianty KA, minimalizace KA, Mihill-Nerodova věta).
21. Regulární množiny, regulární výrazy a rovnice nad regulárními výrazy.
22. Zásobníkové automaty (jazyky přijímané ZA, varianty ZA).
23. Turingovy stroje (jazyky přijímané TS, varianty TS, lineárně omezené automaty, vyčíslitelné funkce).
24. Nerozhodnutelnost (problém zastavení TS, princip diagonalizace a redukce, Postův korespondenční problém).
25. Časová a paměťová složitost (třídy složitosti, úplnost, SAT problém).
26. Postrelační a rozšířené relační databáze (objektový a objektově relační databázový model – struktura a operace; podpora práce s XML a JSON dokumenty v databázích).
27. NoSQL databáze (porovnání relačních a NoSQL; CAP věta a ACID/BASE principy; typy NoSQL databází; dotazování v NoSQL databázích; agregace dat pomocí Map-Reduce a agregační pipeline).
28. Získávání znalostí z dat (pojem znalost; typické zdroje dat; základní úlohy získávání znalostí; analytické projekty a proces získávání znalostí z dat).

29. Porozumění datům (důvod a cíl; popisné charakteristiky dat a vizualizační techniky; korelační analýza).
30. Prostorové DB (problematika mapování prostoru, ukládání, indexace; využití).
31. Indexace (nejen) v prostorových DB (kD-Tree a Grid File (a jejich varianty), R-Tree).
32. Lambda kalkul (definice všech pojmu, operací...).
33. Práce v lambda kalkulu (demonstrace reprezentace čísel a pravdivostních hodnot a operací nad nimi).
34. Haskell – lazy evaluation (typy v jazyce včetně akcí, uživatelské typy, význam typových tříd, demonstrace lazy evaluation).
35. Prolog – způsob vyhodnocení (základní princip, unifikace, chování vestavěných predikátů, operátor řezu – vhodné a nevhodné užití).
36. Prolog – změna DB/programu za běhu (demonstrace na prohledávání stavového prostoru, práce se seznamy).
37. Model PRAM, suma prefixů a její aplikace.
38. Distribuované a paralelní algoritmy – algoritmy nad seznamy, stromy a grafy.
39. Interakce mezi procesy a typické problémy paralelismu (synchronizační a komunikační mechanismy).
40. Distribuované a paralelní algoritmy – předávání zpráv a knihovny pro paralelní zpracování (MPI).
41. Distribuovaný broadcast, synchronizace v distribuovaných systémech.
42. Klasifikace a vlastnosti paralelních a distribuovaných architektur, základní typy jejich topologií.
43. Distribuované a paralelní algoritmy – algoritmy řazení, select, algoritmy vyhledávání.
44. Bezdrátové lokální sítě (Wifi, Bluetooth).
45. Hledání minimální kostry obyčejného grafu (pojmy, stromy a kostry, Kruskalův algoritmus, Primův algoritmus).
46. Hledání nejkratších cest ze zdrojového uzlu do všech ostatních uzel grafu (Bellman-Fordův algoritmus, Dijkstrův algoritmus).
47. Klasifikace algoritmů volby koordinátora, algoritmus Bully a jeho složitost.
48. Podmínky konsistentního globálního stavu distribuovaného systému.
49. Principy distribuovaného zpracování MapReduce, průběh a jednotlivé operace distribuovaného výpočtu pomocí MapReduce, jeho implementace v Apache Hadoop a Apache Spark.
50. Symetrická kryptografie. Vlastnosti, vlastnosti bezpečného algoritmu, délka klíče, útok silou, příklady symetrických algoritmů, Feistelovy šifry, DES, režimy činnosti, proudové šifry.
51. Asymetrická kryptografie, vlastnosti, způsoby použití, poskytované bezpečnostní funkce, elektronický podpis a jeho vlastnosti, hybridní kryptografie, algoritmus RSA, generování klíčů, šifrování, dešifrování.
52. Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti.
53. Správa klíčů v asymetrické kryptografii (certifikáty X.509).
54. Základní architektury přepínačů, algoritmy pro plánování, řešení blokování, vícestupňové přepínací sítě.
55. Základní funkce směrovače, zpracování paketů ve směrovači, typy přepínání a architektur.
56. Metody pro výpočet směrování v sítích (Bellman-Ford, Dijkstra, Path vector, DUAL).
57. Řízení toku dat (flow-control) a prevence zahlcení (congestion-control) na transportní vrstvě (MP-TCP, QUIC, SCTP, DCCP).
58. Metody detekce síťových incidentů (signatury, statistické metody) a nástroje (IDS/IPS).
59. Sítě Peer-to-Peer: vlastnosti, chování, způsoby směrování. Strukturované a nestrukturované sítě.

60. Události v JavaScriptu (smyčka událostí, asynchronní programování, klientské události, obsluha událostí)

61. Přenos a distribuce webových dat (URI, protokol HTTP, proxy HTTP, CDN, XHR)

62. Bezpečnost webových aplikací (SOP, XSS, CSRF, bezpečnostní hlavičky HTTP)

Obsah

1	Bezdrátové lokální sítě (Wifi, Bluetooth).	6
1.1	Metadata	6
1.2	Úvod a kontext	6
2	Hledání minimální kostry obyčejného grafu (pojmy, stromy a kostry, Kruskalův algoritmus, Primův algoritmus).	7
2.1	Metadata	7
2.2	Úvod a kontext	7
2.3	Generický algoritmus	9
2.4	Kruskalův algoritmus	11
2.5	Primův-Jarníkův algoritmus	14
3	Hledání nejkratších cest ze zdrojového uzlu do všech ostatních uzel grafu (Bellman-Fordův algoritmus, Dijkstrův algoritmus).	18
3.1	Metadata	18
3.2	Úvod a kontext	18
3.3	Pomocné funkce	19
3.4	Bellman-Fordův algoritmus	20
3.5	Dijkstrův algoritmus	23
4	Klasifikace algoritmů volby koordinátora, algoritmus Bully a jeho složitost.	27
4.1	Metadata	27
4.2	Úvod a kontext	27
4.3	Problém volby koordinátora	27
4.4	Bully algoritmus	28
4.5	Ring Algoritmus	29
4.6	Algoritmus pro obecnou topologii	30
5	Podmínky konsistentního globálního stavu distribuovaného systému.	33
5.1	Úvod a kontext	33
5.2	Model komunikace	34
5.3	Konzistentní globální stav	34
6	Principy distribuovaného zpracování MapReduce, průběh a jednotlivé operace distribuovaného výpočtu pomocí MapReduce, jeho implementace v Apache Hadoop a Apache Spark.	36
6.1	Metadata	36
6.2	Úvod a kontext	36
6.3	MapReduce	37
6.4	Apache Hadoop	40

6.5	Apache Spark	41
7	Symetrická kryptografie. Vlastnosti, vlastnosti bezpečného algoritmu, délka klíče, útok silou, příklady symetrických algoritmů, Feistelovy šifry, DES, režimy činnosti, proudové šifry.	43
7.1	Metadata	43
7.2	Úvod a kontext	43
7.3	Blokové šifry	45
7.4	Provozní režimy činnosti blokových šifer	50
7.5	Proudové šifry	53
8	Asymetrická kryptografie, vlastnosti, způsoby použití, poskytované bezpečnostní funkce, elektronický podpis a jeho vlastnosti, hybridní kryptografie, algoritmus RSA, generování klíčů, šifrování, dešifrování.	57
8.1	Metadata	57
8.2	Úvod a kontext	57
8.3	Hybridní kryptografie	59
8.4	RSA	61
9	Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti.	63
9.1	Metadata	63
9.2	Historie položení otázky	63
9.3	Úvod a kontext	65
9.4	Kryptografická odolnost hashovacích funkcí	65
9.5	Hashovací funkce neklíčované	67
9.6	MAC (<i>message authentication code</i>)	68
9.6.1	HMAC (<i>hash function MAC</i>)	70
10	Správa klíčů v asymetrické kryptografii (certifikáty X.509).	72
10.1	Metadata	72
10.2	Historie položení otázky	72
10.3	Úvod a kontext	73
10.4	Správa klíčů v asymetrické kryptografii	73
10.5	Standard X.509	76

Kapitola 1

Bezdrátové lokální sítě (Wifi, Bluetooth).

1.1 Metadata

- Předmět: Bezdrátové a mobilní sítě (BMS)
- Přednáška:
 - [[todo]]
- Záznam:
 - [[todo]]

1.2 Úvod a kontext

[[todo]]

Kapitola 2

Hledání minimální kostry obyčejného grafu (pojmy, stromy a kostry, Kruskalův algoritmus, Primův algoritmus).

2.1 Metadata

- Předmět: Grafové algoritmy (GAL)
- Přednáška:
 - 5) Stromy, minimální kostry, Jarníkův a Borůvkův algoritmus.
 - 6) Růst minimální kostry, algoritmy Kruskala a Prima.
- Záznam:
 - 2020-10-22
 - 2020-10-29

2.2 Úvod a kontext

Orientovaný graf Orientovaný graf je dvojice $G = (V, E)$, kde V je konečná množina uzlů a $E \subseteq V \times V$ je množina hran.

Neorientovaný graf Neorientovaný graf je dvojice $G = (V, E)$, kde V je konečná množina uzlů a $E \subseteq \binom{V}{2}$ je množina hran. (Hrana je tedy dvouprvková množina, avšak běžně se držíme stejného značení jako u orientovaných grafů a používáme dvojici.)

Ohodnocený graf Ohodnocený graf je takový graf, jehož každá hrana má přiřazenou nějakou hodnotu, typicky definovanou pomocí váhové funkce $w : E \mapsto \mathbb{R}$.

Podgraf Graf $G' = (V', E')$ je podgraf grafu $G = (V, E)$ jestliže $V' \subseteq V$ a $E' \subseteq E$.

Sled Posloupnost uzlů $\langle v_0, v_1, \dots, v_k \rangle$, kde $(v_{i-1}, v_i) \in E$ pro $i = 1, \dots, k$ se nazývá sled délky k z v_0 do v_k .

Uzavřený sled Sled $\langle v_0, v_1, \dots, v_k \rangle$ se nazývá uzavřený, pokud existuje hrana (v_0, v_k) .

Dosažitelnost Pokud existuje sled s z uzlu u do uzlu v , říkáme, že v je dosažitelný z u sledem s , značeno $u \xrightarrow{s} v$.

Tah Tah je sled ve kterém se neopakují hrany.

Cesta Cesta je sled ve kterém se neopakují uzly.

Souvislý graf Neorientovaný graf se nazývá souvislý, pokud mezi libovolnými dvěma uzly existuje cesta.

Kružnice Uzavřená cesta se nazývá kružnice.

Cyklus Orientovaná kružnice se nazývá cyklus (první a poslední uzel je shodný).

Prostý graf Orientovaný graf bez cyklů se nazývá prostý.

Acyklický graf Graf je bez cyklů, resp. kružnic, se nazývá acyklický.

Strom Graf, který je souvislý a acyklický, se nazývá strom.

Kostra Strom, který tvoří podgraf souvislého grafu na množině všech jeho vrcholů, se nazývá kostra (*spanning tree*).

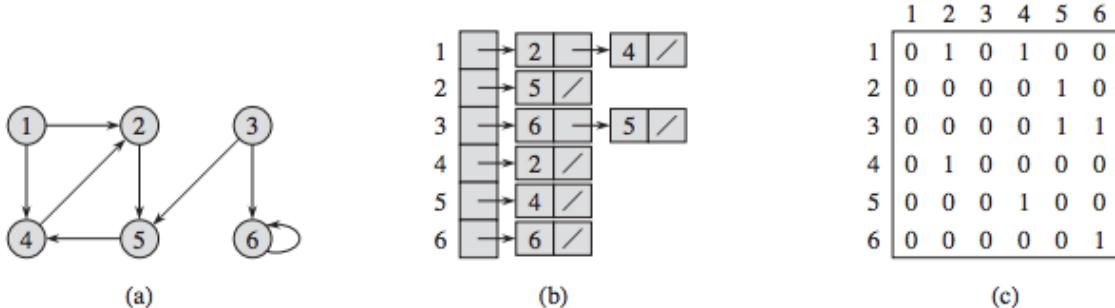
Minimální kostra Necht' $G = (V, E)$ je souvislý neorientovaný graf s váhou funkcí $w : E \mapsto \mathbb{R}$. Minimální kostra (*MST, minimum spanning tree*) je strom $G' = (V, E')$, kde $E' \subseteq E$ a

$$w(E') = \sum_{(u,v) \in T} w(u, v)$$

je minimální ze všech možných alternativních kostér.

Seznam sousedů Seznam sousedů (*Adj, adjacency list*) je reprezentace grafu v paměti. Jde o preferovanou variantu pro řídké grafy – kde $m \ll n^2$. Pro každý uzel máme definovaný seznam jeho sousedů.

Matice sousednosti Matice sousednosti (*adjacency matrix*) je reprezentace grafu v paměti. Jde o preferovanou variantu pro husté grafy – kde m je skoro n^2 .



Obrázek 2.1: Příklad reprezentace grafu pomocí seznamu sousedů a matice sousednosti.

2.3 Generický algoritmus

Hledání minimální kostry je problém, který lze řešit algoritmy, které spadají do kategorie tzv. hladových (*greedy*) deterministických algoritmů. Spočívají v tom, že průběžně odhadují kostru přidáváním dalších hran a nikdy se nemusejí vracet (neprovádí se *backtracking*). Generický algoritmus tvoří jakousi základní kostru pro další, už konkrétní, algoritmy.

Řez Necht' $G = (V, E)$ je graf. Řez grafu G je dvojice $(S, V - S)$, kde $\emptyset \subseteq S \subseteq V$.

Křížení Hrana $(u, v) \in E$ kříží řez $(S, V - S)$, pokud jeden její konec je v S a druhý v $V - S$.

Respektování Necht' $A \subseteq E$ je množina hran. Řez $(S, V - S)$ respektuje množinu hran A , pokud žádná hrana v A nekříží řez $(S, V - S)$.

Lehkost Necht' $(S, V - S)$ je řez a B je množina hran, která ho kříží. Hrana z množiny B s nejmenší hodnotou se nazývá lehká.

Bezpečnost Necht' $G = (V, E)$ je souvislý neorientovaný graf s reálnou váhovou funkcí w . Necht' $A \subseteq E$ je součástí nějaké minimální kostry G . Necht' $(S, V - S)$ je řez, který respektuje A . Necht' (u, v) je lehká hrana křížící $(S, V - S)$. Pak hrana (u, v) je bezpečná pro A .

```

1 def generic_mst(G):
2     # G je graf
3     A~= {}# A~je mnozina hran rozpracovane minimalni kostry
4     while netvorí_kostru(A, G):
5         for hrana in G.E:
6             if je_bezpecna(A, hrana):
7                 A~+= {hrana}
8     return
9 A~

```

Výpis 2.1: Generický algoritmus. Před každou iterací algoritmu je množina A podmnožinou nějaké minimální kostry. Hrana $(u, v) \in E$ je bezpečná pro A , pokud $A \cup \{(u, v)\}$ je podmnožinou nějaké minimální kostry.

Př. $G = (V, E)$ $\psi: E \rightarrow \mathbb{R}$ (definované obrazem)

1.)



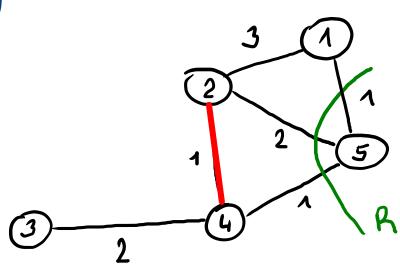
$$A = \{\emptyset\}$$

$$R = (\{\{1, 2, 5\}, \{3, 4\}\})$$

$$LH = \{(2, 4), (4, 5)\}$$

$$A \leftarrow A \cup \{(2, 4)\}$$

2.)



$$A = \{(2, 4)\}$$

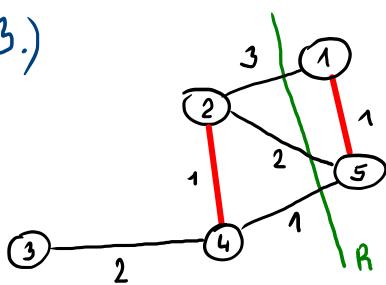
$$R = (\{\{1, 2, 3, 4\}, \{5\}\})$$

$$LH = \{(1, 5), (4, 5)\}$$

$$A \leftarrow A \cup \{(1, 5)\}$$

Obrázek 2.2: Příklad, část 1.

3.)



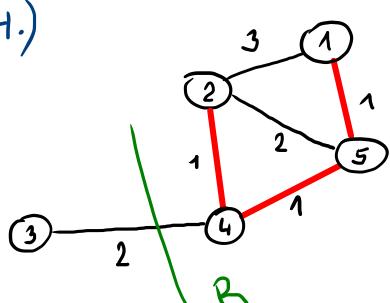
$$A = \{(1, 5), (2, 4)\}$$

$$R = (\{\{1, 5\}, \{2, 3, 4\}\})$$

$$LH = \{(4, 5)\}$$

$$A \leftarrow A \cup \{(4, 5)\}$$

4.)



$$A = \{(1, 5), (2, 4), (4, 5)\}$$

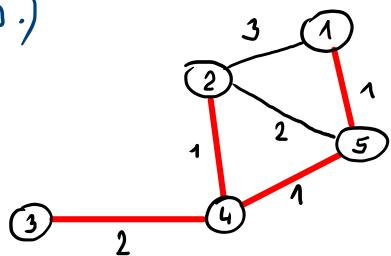
$$R = (\{\{1, 2, 4, 5\}, \{3\}\})$$

$$LH = \{(3, 4)\}$$

$$A \leftarrow A \cup \{(3, 4)\}$$

Obrázek 2.3: Příklad, část 2.

5.)



$$A = \{(3,4), (2,4), (5,4), (1,5)\}$$

A je minimální koštva

(minu jiné už nemůže učítat
věz, když by vypočítal A)

Obrázek 2.4: Příklad, část 3.

2.4 Kruskalův algoritmus

Kruskalův a Primův algoritmus se liší v tom, jakým způsobem vybírají bezpečnou hranu. Kruskalův algoritmus nahlíží na A jako na les a hledá hranu s nejmenším ohodnocením, která spojuje stromy v lese. Na konci je A jeden strom.

```

1 def kruskal_mst(G):
2     # G je graf
3
4     # inicializace, kazdy uzel je ve sve mnozine
5     A~= {}# A~je mnozina hran rozpracovane minimalni kostry
6     for v~in G.V:
7         make_set(v)
8
9     # seradit vzestupne podle w
10    E = sort(G.E, G.w)
11
12    for (u, v) in E:
13        if find_set(u) != find_set(v):
14            A~+= {(u, v)}
15            union(u, v)
16
17    return
18 A~

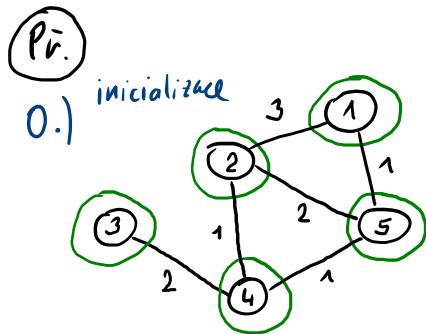
```

Výpis 2.2: Kruskalův algoritmus. Funkce `make_set(v)` vytvoří množinu obsahující v , `find_set(v)` vrátí reprezentanta množiny ve které se nachází v , `union(u, v)` sjednotí dvě množiny obsahující u a v .

Složitost

- Řádek 5 – $O(1)$
- Řádek 6-7 – n -krát složitost `make_set` (n je počet uzlů).
- Řádek 10 – $O(m \cdot \log(m))$ (m je počet hran).
- Řádky 12-15 – Závisí na implementaci `find_set` a `union`.
 - Při implementaci seznamem s heuristickou celkem: $O(m + n \cdot \log(n))$.
 - Při stromové implementaci s váhami a zkratkami celkem: $O((m + n) \cdot \alpha(n))$.
Kde α je velmi pomalu rostoucí funkce ($\alpha \leq 4$).
- Pro souvislý graf platí $m > n$. Proto množinové operace stojí $O(m \cdot \alpha(n))$. Jelikož $\alpha(n) = O(\log(n)) = O(\log(m))$, tak celková složitost je $O(m \cdot \log(m))$.
- Dále platí $m < n^2$, pak $\log(m) = O(\log(n))$, proto celkem: $O(m \cdot \log(n))$.

Příklad



$$A = \{\}$$

make-sets

$$E = [(1,5), (4,5), (2,4), (2,5), (3,4), (1,2)]$$

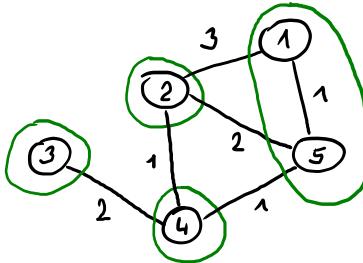
1.) $E = [(4,5), (2,4), (2,5), (3,4), (1,2)]$

$(1,5)$

sets jsou různé

$$A \leftarrow A \cup \{(1,5)\}$$

union $(1,5)$



Obrázek 2.5: Příklad, část 1.

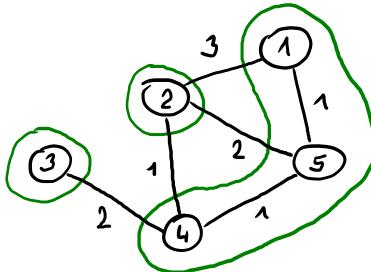
2.) $E = [(2,4), (2,5), (3,4), (1,2)]$

$(4,5)$

sets jsou různé

$$A \leftarrow A \cup \{(4,5)\}$$

union $(4,5)$



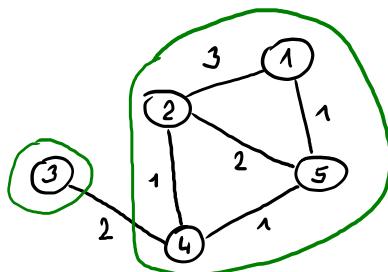
3.) $E = [(2,5), (3,4), (1,2)]$

$(2,4)$

sets jsou různé

$$A \leftarrow A \cup \{(2,4)\}$$

union $(2,4)$

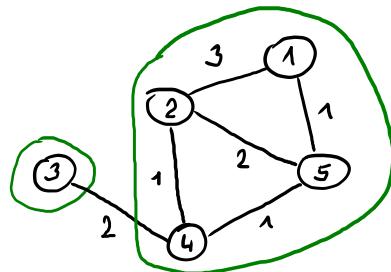


Obrázek 2.6: Příklad, část 2.

$$4.) E = [(3,4), (1,2)]$$

(2,5)

sets nejsou různé



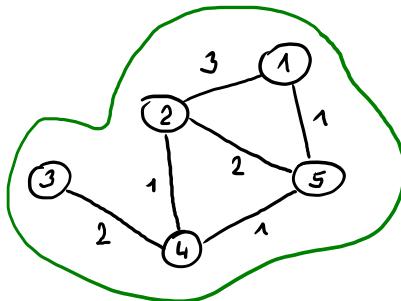
$$4.) E = [(1,2)]$$

(3,4)

sets jsou různé

$$A \leftarrow A \cup \{(3,4)\}$$

union(3,4)



$$5.) E = [] , (1,2) , \text{ sets nejsou různé}$$

Obrázek 2.7: Příklad, část 3.

2.5 Primův-Jarníkův algoritmus

Primův algoritmus buduje tzv. A strom. Má zadaný určitý uzel, ze kterého hledá nejbližší další uzel, který by připojil. A pak další a další.

```

1 def prim_mst(G, r):
2     # G je graf
3     # r je výchozí uzel
4
5     for u in G.V:
6         key[u] = INF # pole cen prechodu, kolik stojí prechod do vrcholu na indexu
7         pi[u] = NULL # pole predchudcu, kdo je predchudce vrcholu na indexu
8
9     key[r] = 0
10    Q = Queue(G.V) # prioritní fronta uzlu
11
12    while not Q.empty():
13        u = Q.extract_min(key) # vrati prvek z~Q s~nejmensi hodnotou v~key
14
15        # pro vsechny sousedy uzlu u~(Adj je seznam sousedu)
16        for v in Adj[u]:
17            # pokud je levnejsi cesta a jeste to není prozkoumaný uzel
18            if v in Q and w(u, v) < key(v):
19                pi[v] =
20        u.key[v] = w(u, v)
21        Q.decrease_key(key) # aktualizace prioritni fronty
22
23    return pi

```

Výpis 2.3: Primův algoritmus.

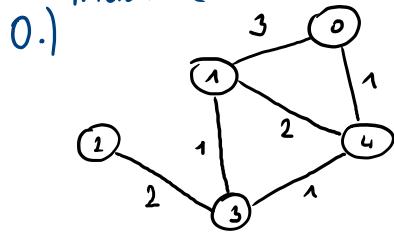
Složitost

- Řádky 5-10 – $O(n)$ za použití binární haldy (n je počet uzlů).
- Řádky 12-13 – While cyklus se provede n -krát a protože $extract_min$ stojí $O(\log(n))$, tak je celková složitost $O(n \cdot \log(n))$.
- Řádek 16 – For cyklus se provede $O(m)$ krát, protože délka všech seznamů sousedů je dohromady $2m$ (m je počet hran).
- Řádek 18-20 – $O(1)$.
- Řádek 21 – $O(\log(n))$.
- Jelikož $m > n$, tak celkem $O(n \cdot \log(n) + m \cdot \log(n)) = O(m \cdot \log(n))$.

Příklad

Pr.

0.) initialize



$$n = 1$$

$$\text{key} = [\infty, 0, \infty, \infty, \infty]$$

$$\pi = [\text{NULL}, \text{NULL}, \text{NULL}, \text{NULL}, \text{NULL}]$$

$$Q = [0, 1, 2, 3, 4]$$

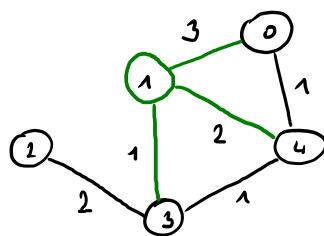
1.) $u = 1$

$$Q = [0, 1, 3, 4]$$

$$v \in \{0, 3, 4\}$$

$$\text{key} = [3, 0, \infty, 1, 2]$$

$$\pi = [1, \text{NULL}, \text{NULL}, 1, 1]$$



Obrázek 2.8: Příklad, část 1.

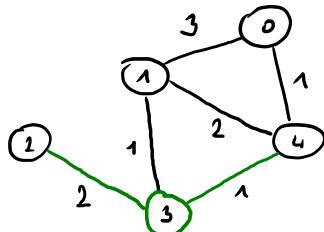
2.) $u = 3$

$$Q = [0, 1, 4]$$

$$v \in \{1, 2, 4\}$$

$$\text{key} = [3, 0, 2, 1, 1]$$

$$\pi = [1, \text{NULL}, 3, 1, 3]$$



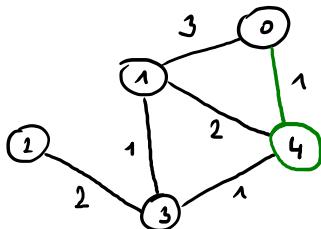
3.) $u = 4$

$$Q = [0, 1]$$

$$v \in \{0, 1, 3\}$$

$$\text{key} = [1, 0, 2, 1, 1]$$

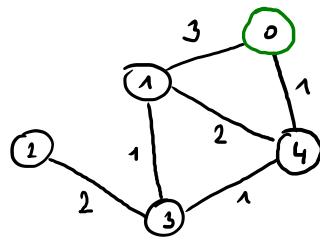
$$\pi = [4, \text{NULL}, 3, 1, 3]$$



Obrázek 2.9: Příklad, část 2.

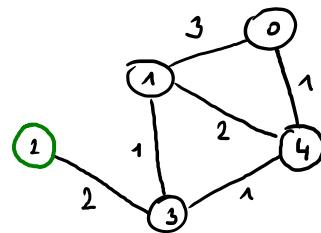
4.) $u = 0$
 $Q = [1]$
 $v \in \{1, 4\}$

$key = [1, 0, 2, 1, 1]$
 $\pi = [4, \text{NULL}, 3, 1, 3]$



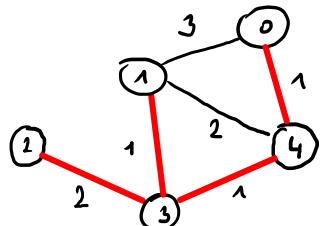
5.) $u = 2$
 $Q = []$
 $v \in \{3\}$

$key = [1, 0, 2, 1, 1]$
 $\pi = [4, \text{NULL}, 3, 1, 3]$



Obrázek 2.10: Příklad, část 3.

6.) $key = [1, 0, 2, 1, 1]$
 $\pi = [4, \text{NULL}, 3, 1, 3]$



Obrázek 2.11: Příklad, část 4.

Kapitola 3

Hledání nejkratších cest ze zdrojového uzlu do všech ostatních uzelů grafu (Bellman-Fordův algoritmus, Dijkstrův algoritmus).

3.1 Metadata

- Předmět: Grafové algoritmy (GAL)
- Přednáška:
 - 7) Nejkratší cesty z jednoho vrcholu, Bellman-Fordův algoritmus, nejkratší cesta z jednoho vrcholu v orientovaných acyklických grafech.
 - 8) Dijkstrův algoritmus. Nejkratší cesty ze všech vrcholů.
- Záznam:
 - 2020-11-05

3.2 Úvod a kontext

Viz. „Úvod a kontext“ v předchozích otázkách z tohoto předmětu.

Cena cesty Necht' $G = (V, E)$ je ohodnocený graf s váhovou funkcí $w : E \mapsto \mathbb{R}$. Cena cesty $p = \langle v_0, v_1, \dots, v_k \rangle$ je suma

$$w(p) = \sum_{i=0}^k w(v_i, v_{i+1})$$

Cena nejkratší cesty Cena nejkratší cesty z u do v je

$$\delta(u, v) = \begin{cases} \min(\{w(p) : u \xrightarrow{p} v\}) \\ \infty \text{ pokud cesta neexistuje} \end{cases}$$

Nejkratší cesta Nejkratší cesta z u do v je pak libovolná cesta p taková, že $w(p) = \delta(u, v)$.

Cena cesty se záporným cyklem Pokud na cestě z u do v existuje záporný cyklus (cyklus jehož celková cena je záporná), pak $\delta(u, v) = -\infty$.

Záporné ohodnocení hran Pokud na cestě z u do v neexistuje záporný cyklus, tak algoritmy pracují dobře i se záporným ohodnocením hran.

Reprezentace cesty Cestu reprezentujeme pomocí pole předchůdců π .

Hledání nejkratších cest ze všech uzlů do jednoho Tento problém lze řešit stejnými algoritmy. Graf se transponuje (převrácení orientace hran), provede se algoritmus pro problém „hledání nejkratších cest ze jednoho uzlu do všech ostatních uzlů“ a poté se transponuje zpět.

Reprezentace nejkratší cesty Nejkratší cestu grafu $G = (V, E)$ reprezentujeme pomocí pole předchůdců π , kde $\pi[v]$ označuje předchůdce uzlu $v \in V$ na nejkratší cestě. Podgraf předchůdců pak je $G_\pi = (V_\pi, E_\pi)$, $V_\pi = \{v \in V : \pi[v] \neq \text{NULL}\} \cup \{s\}$, $E_\pi = \{(\pi[v], v) \in E : v \in V_\pi - \{s\}\}$. V okamžiku dokončení algoritmu výpočtu nejkratších cest je G_π strom nejkratších cest. Tj. kořenový strom obsahující nejkratší cesty ze zdroje s do všech ostatních uzlů.

3.3 Pomocné funkce

Představené algoritmy pracují z důvodu efektivity se sledy a nikoliv s cestami (bylo by nutné stále kontrolovat, zda nebyla porušena podmínka cesty), ačkoliv je problém nazývá hledání nejkratší cesty.

```

1 def initialize_single_source(G, s):
2     # G je graf
3     # s~je vychozi uzel
4     for v~in G.V:
5         d[v] = INF # d je pole vzdalenosti
6         pi[v] = NULL # pi je pole predchudcu
7         d[s] = 0

```

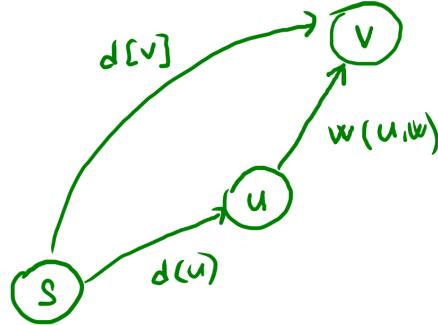
Výpis 3.1: Pomocná inicializační funkce. Složitost je $\Theta(n)$, kde n je počet uzlů.

```

1 def relax(u, v, w):
2     # u~a v~jsou uzly grafu
3     # w je vahova funkce
4     if d[v] > d[u] + w(u, v):
5         d[v] = d[u] + w(u, v)
6         pi[v] =
7 u~

```

Výpis 3.2: Pomocná funkce *relax*. Složitost je $O(1)$.



Obrázek 3.1: Ukázka činnosti funkce *relax*.

3.4 Bellman-Fordův algoritmus

Slouží pro řešení v obecných grafech, mohou obsahovat cykly a záporné hrany. Záporné cykly je však nutné detektovat a vrátit specifickou hodnotu. V podstatě se jedná o *brute force* algoritmus, provede se relaxace $n - 1$ -krát pro každou hranu.

```

1 def bellman_ford(G, s, w):
2     # G je graf
3     # s~je vychozi uzel
4     # w je vahova funkce
5
6     # faze inicializace
7     initialize_single_source(G, s)
8     n = len(G.V) # pocet uzlu
9
10    # faze relaxace: provedeni (n-1) * m relaxaci (m je pocet hran)
11    for _ in range(0, n-1):
12        for u, v~in G.E:
13            relax(u, v, w)
14
15    # faze detekce zaporneho cyklu
16    for u, v~in G.E:
17        if d[u] > d[v] + w(u, v):
18            return NULL
19
20    return pi

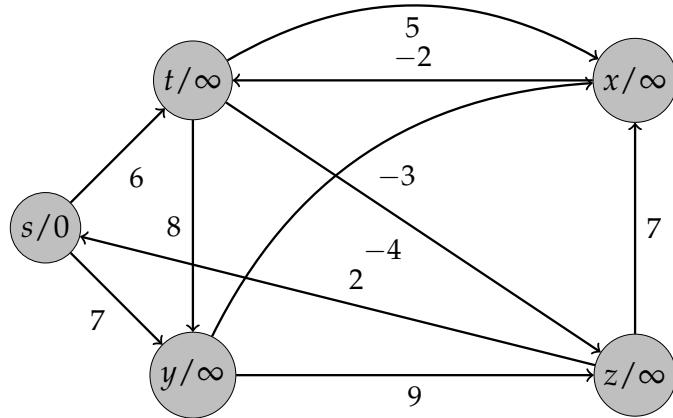
```

Výpis 3.3: Algoritmus Bellman-Ford. Proč $n - 1$ iterací? Protože mezi libovolnými dvěma uzly v grafu, existuje cesta o maximálním počtu hran $n - 1$.

Složitost

- Řádek 7, 8 – $\Theta(1)$.
- Řádky 11, 12, 13 – $(n - 1) \cdot \Theta(m) = \Theta(n \cdot m)$, kde n je počet uzelů a m je počet hran grafu.
- Řádek 16, 17, 18 – $\Theta(m)$.
- Celkem $\Theta(n \cdot m)$.

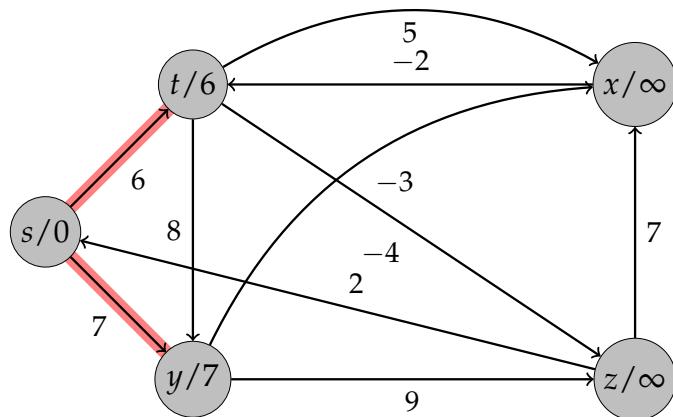
Příklad



Obrázek: Práce algoritmu Bellman-Ford.

- ▶ Pokud $(u, v) \in E$ je označená, pak $\pi[v] = u$
- ▶ Hrany se relaxují v tomto pořadí:
 $(t, x), (t, y), (t, z), (x, t), (y, x), (y, z), (z, x), (z, s), (s, t), (s, y)$.

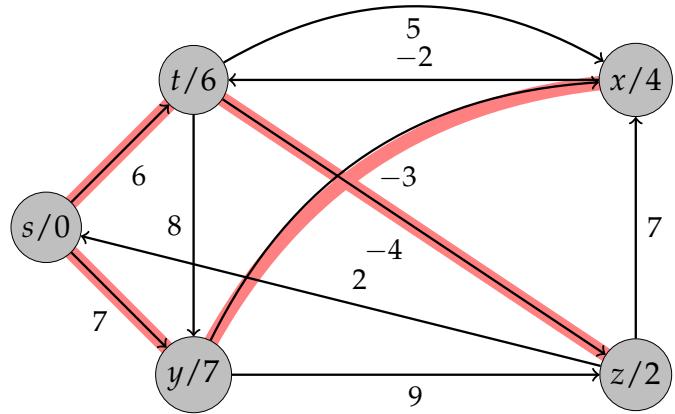
Obrázek 3.2: Příklad, část 1.



Obrázek: Práce algoritmu Bellman-Ford.

- ▶ Pokud $(u, v) \in E$ je označená, pak $\pi[v] = u$
- ▶ Hrany se relaxují v tomto pořadí:
 $(t, x), (t, y), (t, z), (x, t), (y, x), (y, z), (z, x), (z, s), (s, t), (s, y)$.

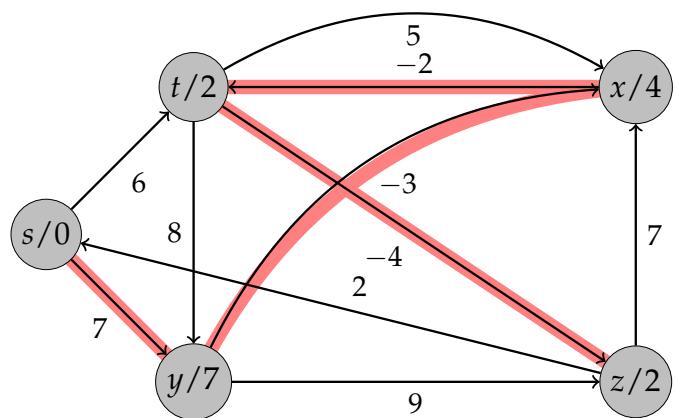
Obrázek 3.3: Příklad, část 2.



Obrázek: Práce algoritmu Bellman-Ford.

- ▶ Pokud $(u, v) \in E$ je označená, pak $\pi[v] = u$
- ▶ Hrany se relaxují v tomto pořadí:
 $(t, x), (t, y), (t, z), (x, t), (y, x), (y, z), (z, x), (z, s), (s, t), (s, y)$.

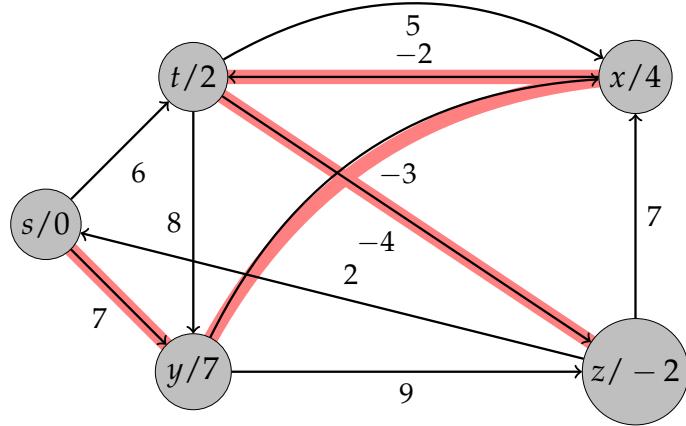
Obrázek 3.4: Příklad, část 3.



Obrázek: Práce algoritmu Bellman-Ford.

- ▶ Pokud $(u, v) \in E$ je označená, pak $\pi[v] = u$
- ▶ Hrany se relaxují v tomto pořadí:
 $(t, x), (t, y), (t, z), (x, t), (y, x), (y, z), (z, x), (z, s), (s, t), (s, y)$.

Obrázek 3.5: Příklad, část 4.



Obrázek: Práce algoritmu Bellman-Ford.

- ▶ Pokud $(u, v) \in E$ je označená, pak $\pi[v] = u$
- ▶ Hrany se relaxují v tomto pořadí:
 $(t, x), (t, y), (t, z), (x, t), (y, x), (y, z), (z, x), (z, s), (s, t), (s, y)$

Obrázek 3.6: Příklad, část 5.

3.5 Dijkstrův algoritmus

Slouží pro řešení v acyklických grafech bez záporných hran. Pro takto omezený problém existují rychlejší algoritmy než pro problém v obecných grafech.

```

1 def dijkstra(G, s, w):
2     # G je graf
3     # s~je výchozí uzel
4     # w je vahová funkce
5
6     # fáze inicializace
7     initialize_single_source(G, s)
8     Q = Queue(G.V) # prioritní fronta uzlu
9     S~= {}# množina uzlu, která už byla prozkoumána
10
11    # fáze relaxace
12    while not Q.empty():
13        u~= Q.extract_min(d) # vrátí prvek z~Q s~nejmenší hodnotou v~d
14        S~+= {u}
15        # pro všechny sousedy uzlu u~(Adj je seznam sousedů)
16        for v~in Adj[u]:
17            relax(u, v, w)
18
19        Q.decrease_key(d) # aktualizace prioritní fronty
20
21    return d, pi

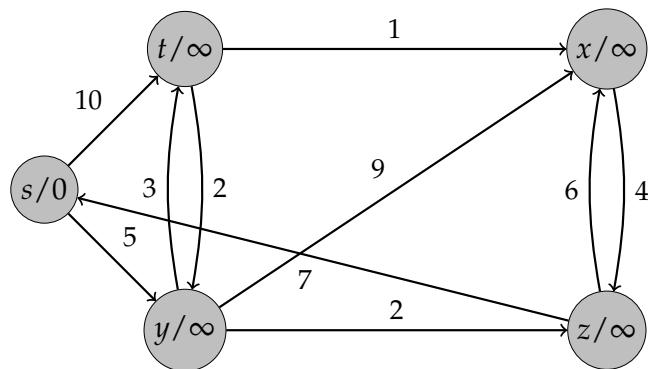
```

Výpis 3.4: Algoritmus Dijkstra.

Složitost

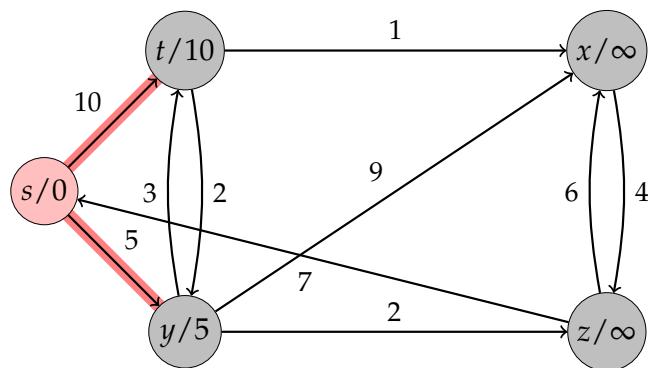
- Předpokládejme implementaci prioritní fronty pomocí pole.
- Řádek 8, 18 – $O(1)$.
- Řádek 11 – While cyklus se provede n -krát, kde n je počet uzlů.
- Řádek 12 – $O(n)$, najítí minima v poli uzlů. Celkově (s cyklem) $O(n^2)$.
- Řádek 16 – $O(m)$, pro všechny hrany. Celkově (s cyklem) $O(m \cdot n)$.
- Celkem $O(n^2 + m) = O(n^2)$.
- Pro řídké grafy lze využít implementaci fronty pomocí binární haldy a získat tak $O(m \cdot \log(n))$.
- Při implementaci fronty pomocí Fibonacciho haldy dostaneme časovou složitost $O(n \cdot \log(n) + m)$.

Příklad



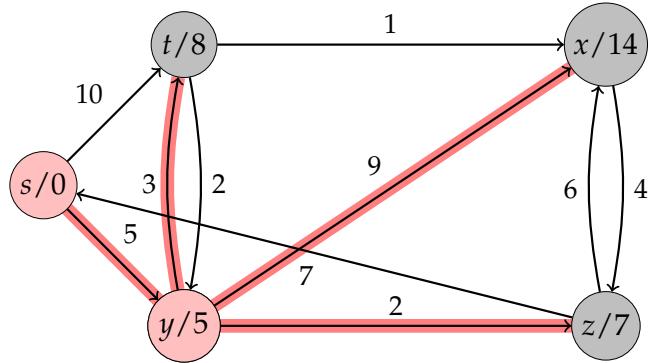
Obrázek: Práce Dijkstrova algoritmu. Označené uzly značí uzly z množiny S .

Obrázek 3.7: Příklad, část 1.



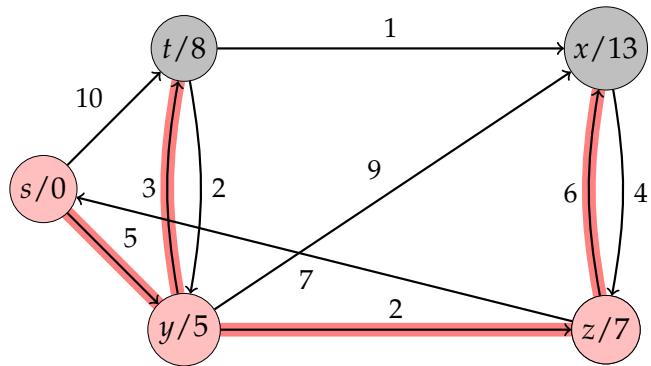
Obrázek: Práce Dijkstrova algoritmu. Označené uzly značí uzly z množiny S .

Obrázek 3.8: Příklad, část 2.



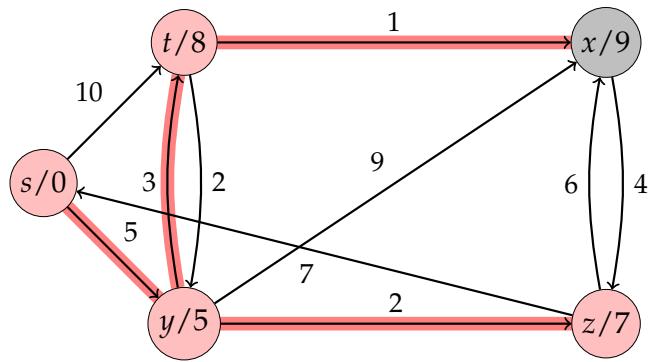
Obrázek: Práce Dijkstrova algoritmu. Označené uzly značí uzly z množiny S .

Obrázek 3.9: Příklad, část 3.



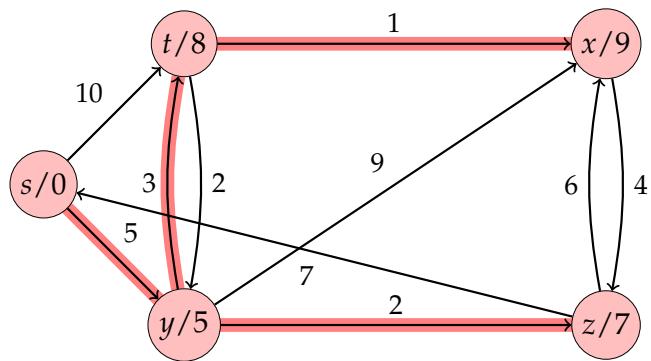
Obrázek: Práce Dijkstrova algoritmu. Označené uzly značí uzly z množiny S .

Obrázek 3.10: Příklad, část 4.



Obrázek: Práce Dijkstrova algoritmu. Označené uzly značí uzly z množiny S .

Obrázek 3.11: Příklad, část 5.



Obrázek: Práce Dijkstrova algoritmu. Označené uzly značí uzly z množiny S .

Obrázek 3.12: Příklad, část 6.

Kapitola 4

Klasifikace algoritmů volby koordinátora, algoritmus Bully a jeho složitost.

4.1 Metadata

- Předmět: Prostředí distribuovaných aplikací (PDI)
- Přednáška:
 - 7) Synchronizace
- Záznam:
 - 2020-11-02

4.2 Úvod a kontext

- Mějme množinu procesů v rámci distribuovaného systému. Řešíme problém nalezení shody na nějaké věci (synchronizační problém). Problém můžeme rozdělit na dvě situace:
 - **Problém volby koordinátora** – Výběr jednoho z procesů, který bude vedoucím procesem (koordinátor). Tento proces pak může vykonat určitou činnost nebo může sloužit ostatním procesům k realizaci význačné role v systému.
 - **Problém vzájemného vyloučení** – Předpokládejme, že konkrétní zdroj může v daném okamžiku používat pouze jeden proces. Tento problém se běžně vyskytuje ve víceprocesorových systémech, ale také v distribuovaných systémech.
- Synchronizační problémy lze v rámci operačních systémů nebo multiprocesorových systémů řešit pomocí provádění atomických operací, sdílené paměti apod. (je pro ně podpora v rámci operačního systému nebo hardwaru). V distribuovaných systémech nic takového není z principu možné a proto se synchronizační problémy řeší pomocí zasílání zprav, resp. algoritmicky.

4.3 Problém volby koordinátora

- Předpokládáme:

- Každý proces má unikátní ID.
 - Procesy neznají stav (běžící, neběžící) dalších procesů.
 - Každý proces zná ID dalších procesů (záleží na topologii).
- Cíl:
 - Dosáhnutí shody mezi všemi procesy na procesu, který je koordinátor.
 - Kritérium výběru koordinátora může být různé. Např. na základě proces ID (proces s největším ID se stane koordinátorem).

4.4 Bully algoritmus

Pro topologii každý s každým – každý proces může komunikovat s každým dalším procesem. Používá tři druhy zpráv: ELECTION, OK, COORDINATOR.

Postup

- Proces P, který má podezření, že chybí koordinátor, může zahájit volby.
 1. Proces P odešle zprávu ELECTION všem procesům s větším ID.
 2. Pokud nikdo neodpoví, P vyhrává volby a stává se koordinátorem.
 3. Pokud některý z procesů s větším ID odpoví (zpráva OK), tak přebírá řízení a práce P je ukončena.
 4. Pokud P obdrží zprávu ELECTION od procesů s menším ID, pošle jim odpověď OK na zablokování procesů.
- Nakonec zůstane pouze P (nový koordinátor), který o tom informuje ostatní zasláním zprávy COORDINATOR.
- Pokud se proces probudí nebo je restartován, první akcí je vyvolání voleb.

Složitost

Složitost z hlediska počtu zpráv.

Nejhorší případ (iniciátor s nejmenším ID):

- $(n - 1)$ iterací
- $2(n - 1)$ zpráv ELECTION a OK pro každou iteraci
- $(n - 1)$ zpráv COORDINATOR
- Celkem: $(n - 1) \times 2(n - 1) + (n - 1) \approx n^2$

Nejlepší případ (iniciátor s největším ID):

- $(n - 1)$ zpráv COORDINATOR
- Celkem: $(n - 1)$

Příklad

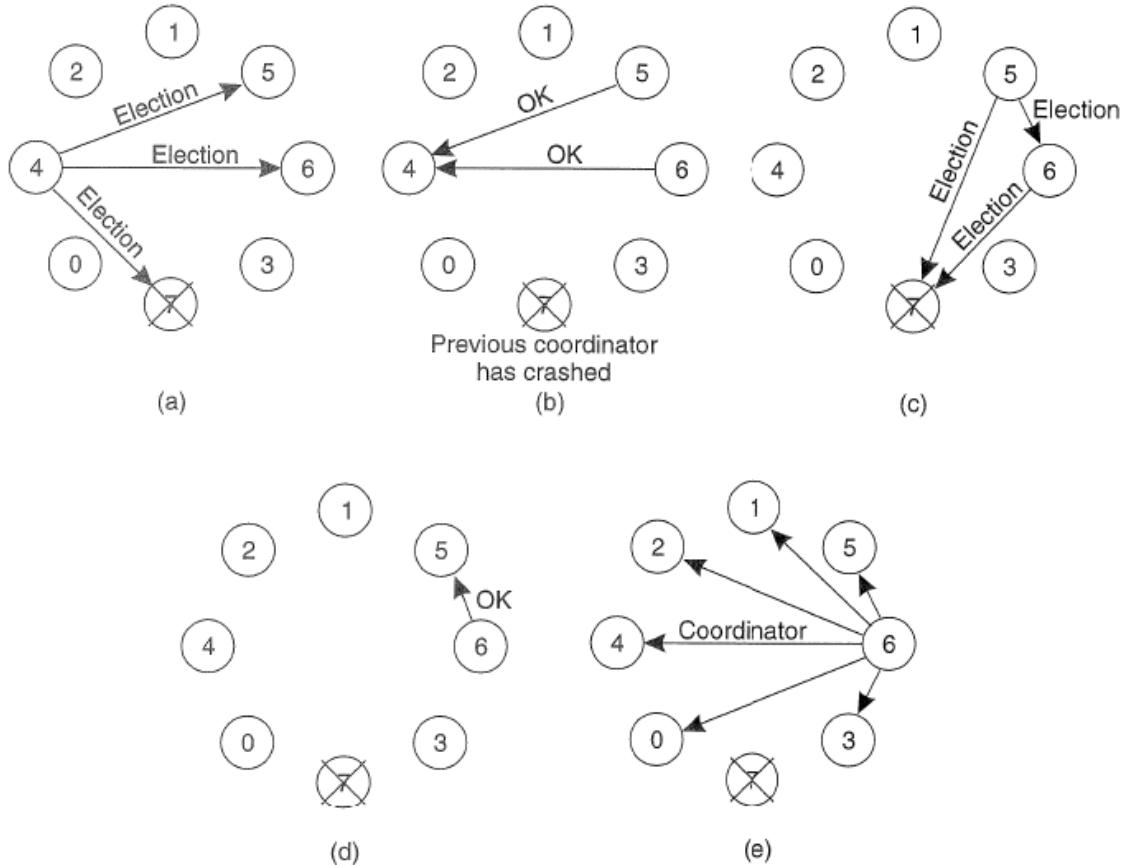


Figure 5-11. The bully election algorithm. (a) Process 4 holds an election. (b) Processes 5 and 6 respond, telling 4 to stop. (c) Now 5 and 6 each hold an election. (d) Process 6 tells 5 to stop. (e) Process 6 wins and tells everyone.

Obrázek 4.1: Příklad činnosti Bully algoritmu.

4.5 Ring Algoritmus

Pro kruhovou topologii – procesy jsou uspořádané do kruhu podle svého proces ID. Každý proces musí vědět nejenom o svém následovníkovi, ale také o jeho následníkovi, který funguje jako „záloha“, v případě že by se přímý následník stal nedostupný. Používá dva druhy zpráv: ELECTION, COORDINATOR.

Postup

- Proces P, který má podezření, že chybí koordinátor, může zahájit volby.
 1. Zašle zprávu ELECTION obsahující jeho ID dalšímu procesu (pokud další proces nereaguje, proces P zašle stejnou zprávu dalšímu v kruhu).
 2. Každý člen topologie přijme zprávu ELECTION, přidá do ní své ID a přepošle zprávu dalšímu procesu.

- Když se zpráva vrátí k procesu P, je zpráva převedena na zprávu COORDINATOR a poslána následujícímu procesu v topologii, aby bylo možné nahlásit:
 1. Novým koordinátorem se stává proces s nejvyšším ID.
 2. Členové sítě jsou stále aktivní.
- Po síti může obíhat více zpráv zároveň.

Složitost

Složitost z hlediska počtu zpráv.

Vždy $2n \approx n$ zpráv. Jedno kolečko „oběhne“ zpráva ELECTION a druhé zpráva COORDINATOR.

Příklad

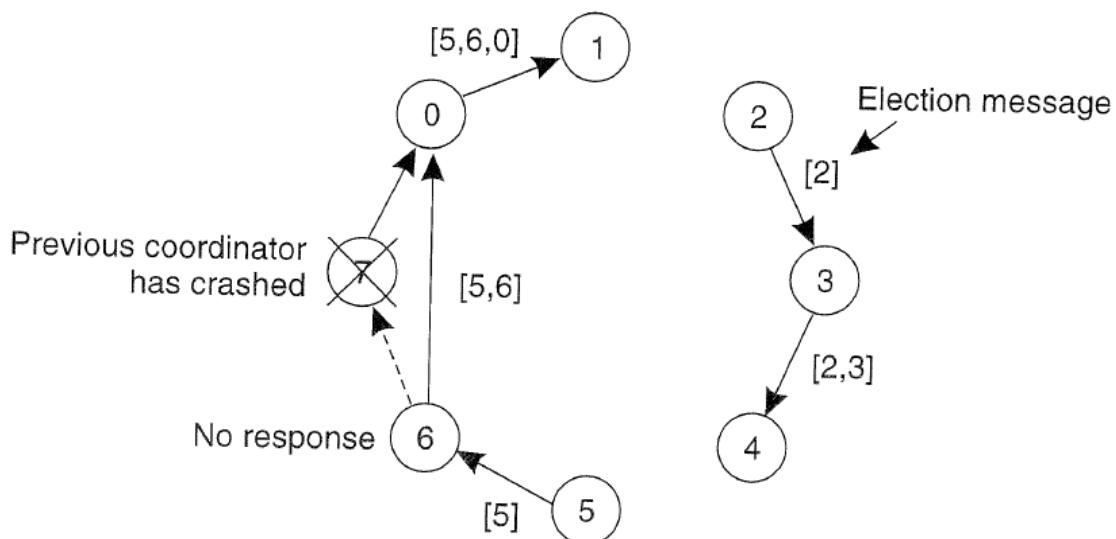


Figure 5-12. Election algorithm using a ring.

Obrázek 4.2: Příklad činnosti Ring algoritmu.

4.6 Algoritmus pro obecnou topologii

Předpokládáme, že nemáme ani kruhovou topologii ani spojení každý s každým. Např.: peer-to-peer sítě, sensorové sítě, ...

Postup

- V první iteraci se broadcastem posílá zpráva ELECTION.
- Každý uzel si uloží od kterého souseda dostal zprávu ELECTION jako první. Tím vzníká kostra grafu (*spanning tree*).

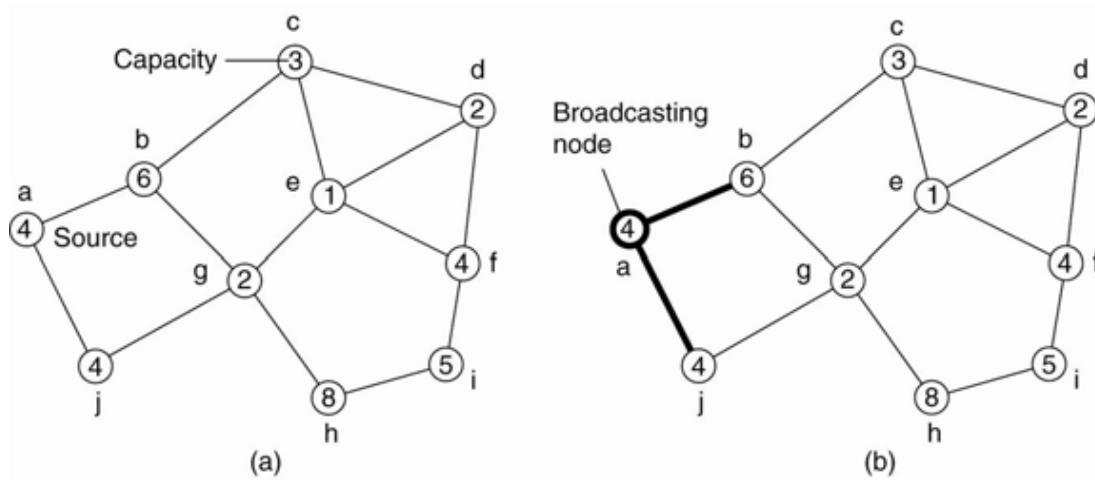
- Uložený soused je poté využijí pro zpětnou komunikaci. To znamená, že další komunikace už probíhá přes strom, nikoliv přes broadcast. Tím je ušetřena některé komunikace.

Složitost

Složitost z hlediska počtu zpráv.

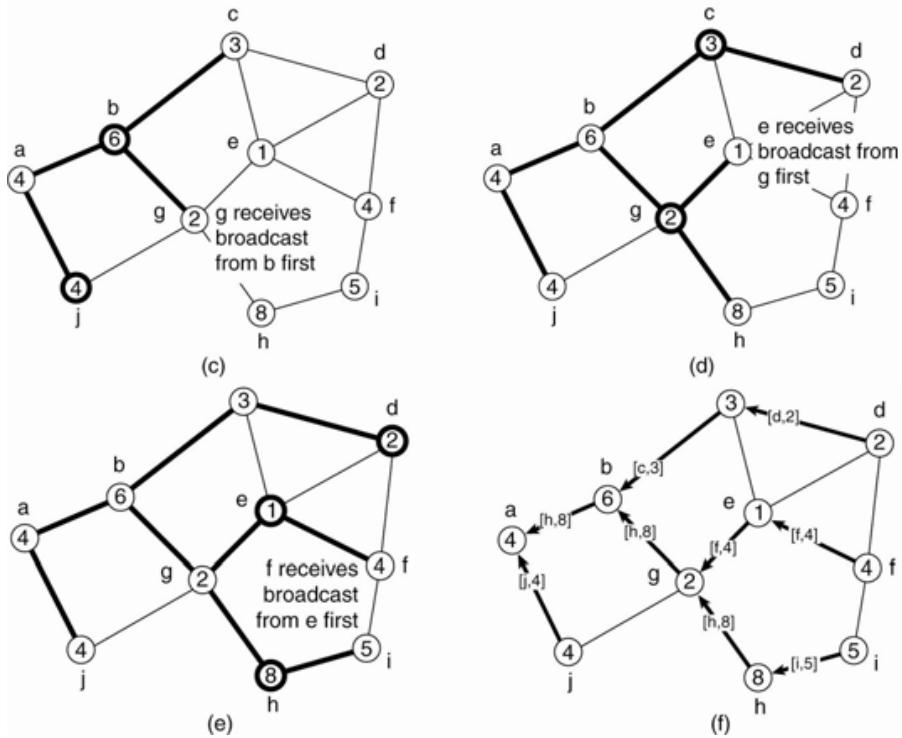
- Inicializační broadcast: počet hran grafu.
- Odpověď: počet hran kostry grafu.
- Result broadcast: počet hran kostry grafu.

Příklad



Node *a* initiates an election.

Obrázek 4.3: Příklad činnosti algoritmu pro obecnou topologii, část 1.



In the end, source *a* notes that *h* is the best leader and broadcasts this info to all nodes.

Obrázek 4.4: Příklad činnosti algoritmu pro obecnou topologii, část 2.

Kapitola 5

Podmínky konsistentního globálního stavu distribuovaného systému.

Metadata

- Předmět: Prostředí distribuovaných aplikací (PDI)
- Přednáška:
 - 4) Globální stav a snapshots
- Záznam:
 - 2020-10-12

5.1 Úvod a kontext

Distribuovaný systém Distribuovaný systém je množina procesů p_1, p_2, \dots, p_n , které jsou propojeny komunikačními kanály. V systému neexistuje žádná globální paměť ani globální hodiny. Procesy spolu komunikují pouze zasíláním zpráv skrze komunikačními kanály.

Komunikační kanál Komunikační kanál mezi procesy p_i a p_j značíme C_{ij} .

Událost Rozlišujeme tři typy událostí: interní událost procesu, zaslání zprávy a přijetí zprávy.

Zpráva Zpráva m_{ij} značí zprávu zaslanou procesem p_i procesu p_j . $send(m_{ij})$ značí odeslání zprávy a $recv(m_{ij})$ přijetí.

Stav procesu Lokální stav procesu p_i značíme LS_i . Lokální stav je definován jako sekvence všech událostí, o kterých proces p_i ví. Nechť e je libovolná událost, $e \in LS_i$ značí, že událost e patří do lokálního stavu procesu p_i , $e \notin LS_i$ značí, že událost e nepatří do lokálního stavu procesu p_i .

Stav komunikačního kanálu Stav komunikačního kanálu C_{ij} značíme SC_{ij} a je definován množinou zpráv, které obsahuje. Pro kanál C_{ij} můžeme definovat jeho stav na základě lokálních stavů procesů LS_i a LS_j :

$$transit(LS_i, LS_j) = \{m_{ij} \mid send(m_{ij}) \in LS_i \wedge rec(m_{ij}) \notin LS_j\}$$

5.2 Model komunikace

- FIFO – Komukační kanál funguje jako fronta zpráv *first in, first out*. Kanál tedy zachovává pořadí zpráv sám o sobě.
- non-FIFO – Komunikační kanál se chová jako datová struktura množina, do které odesílatel vkládá zprávy a příjemce je odebírá v náhodném pořadí.
- Causal ordering (kauzální uspořádání) – Systém, který podporuje kauzální doručení zpráv splňuje následující vlastnost. Pro jakékoli dvě zprávy m_{ij} a m_{kj} platí, pokud $send(m_{ij}) \rightarrow send(m_{kj})$, pak i $recv(m_{ij}) \rightarrow recv(m_{kj})$.

5.3 Konzistentní globální stav

Globální stav Globální stav distribuovaného systému je kolekce lokálních stavů procesů a komunikačních kanálů.

$$GS = \left\{ \bigcup_i LS_i, \bigcup_{i,j} SC_{ij} \right\}$$

Časoprostorový diagram Diagram pro vizualizaci komunikace procesů v distribuovaném systému. Viz obrázek 5.1 a 5.2.

Konzistentní globální stav Konzistentní globální stav (*snapshot*) je stav systému v určitém časovém okamžiku. Lze si jej představit jako řez v časoprostorovém diagramu, který rozděluje diagram na dvě části: minulost a budoucnost. Aby byl řez (globální stav) konzistentní, tak pokud je doručení nějaké zprávy v minulosti, musí být v minulosti i její odeslání. Formálně jde o globální stav, který splňuje následující podmínky:

$$send(m_{ij}) \in LS_i \Rightarrow m_{ij} \in SC_{ij} \oplus recv(m_{ij}) \in LS_j$$

,

$$send(m_{ij}) \notin LS_i \Rightarrow m_{ij} \notin SC_{ij} \wedge recv(m_{ij}) \notin LS_j$$

K čemu je *snapshot* *Snapshot* lze využít např. pro tvorbu záloh systému nebo při zotavování systému po chybách.

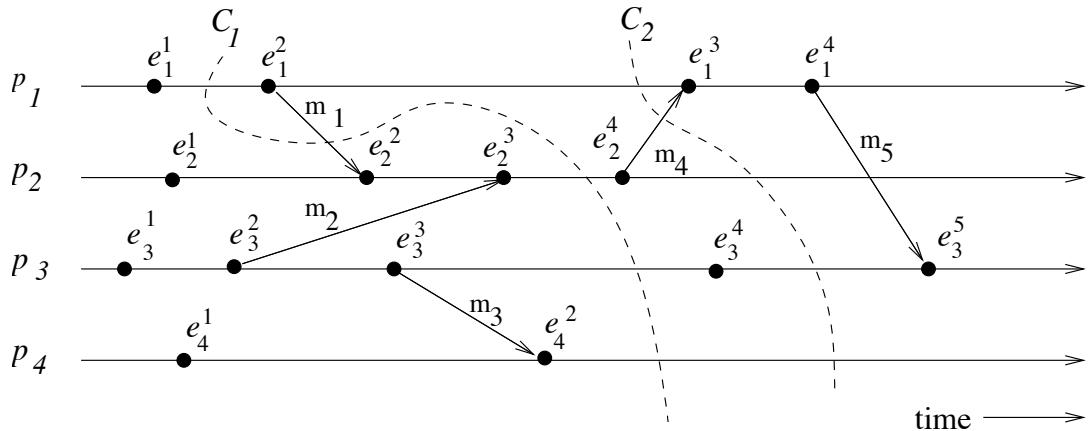
Jak lze *snapshot* vytvořit Absence globální sdílené paměti, globálních hodin a nepředvídatelná délka zpoždění v odesílání zpráv v distribuovaném systému činí problém vytváření snapshotů netriviálním. Způsob vytváření lze rozdělit do dvou kategorií: na základě algoritmů a na základě checkpointů.

Problémy při zaznamenávání *snapshotu* Jak rozlišit mezi zprávami, které mají být součástí snapshotu a které nikoliv?

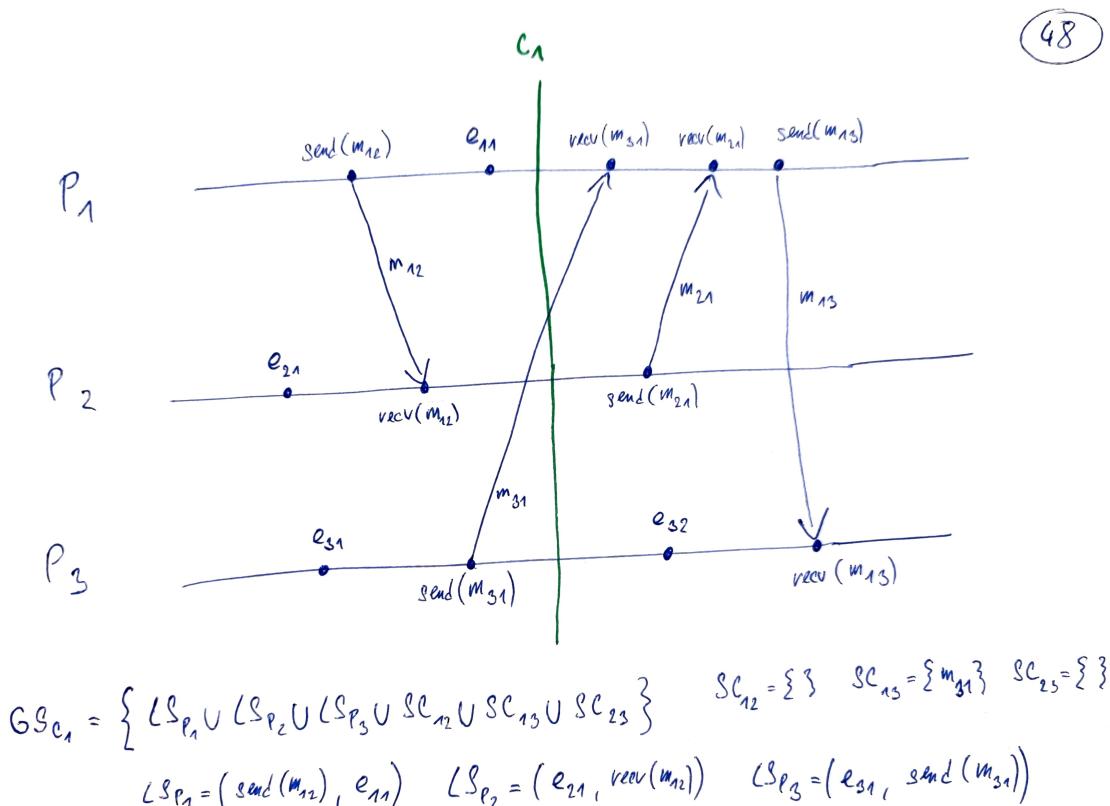
- Zprávy, které jsou odeslány procesem před zaznamenáním svého snapshotu, jsou zaznamenány do stavu.
- Zprávy, které jsou odeslány procesem po zaznamenání svého snapshotu, nejsou zaznamenány do stavu.

Jak rozpozнат okamžik, ve kterém má proces zaznamenat snapshot?

- Proces p_j musí zaznamenat svůj snapshot před zpracováním zprávy m_{ij} , která byla poslána procesem p_i po zaznamenání jeho snapshotu.



Obrázek 5.1: Příklad řezu v časoprostorovém diagramu. Řez C_1 je nekonzistentní, kvůli zprávě m_1 . Řez C_2 je konzistentní a zpráva m_4 je zachycena ve stavu kanálu Ch_{21} .



Obrázek 5.2: Příklad konzistentního globální stavu formálně.

Kapitola 6

Principy distribuovaného zpracování MapReduce, průběh a jednotlivé operace distribuovaného výpočtu pomocí MapReduce, jeho implementace v Apache Hadoop a Apache Spark.

6.1 Metadata

- Předmět: Prostředí distribuovaných aplikací (PDI)
- Přednáška:
 - 9) Programovací model MapReduce a Apache Hadoop
 - 10) Distribuované souborové systémy
 - 11) Apache Spark
- Záznam:
 - 2020-11-16
 - 2020-11-23

6.2 Úvod a kontext

OLTP OLTP (*Online Transactional Processing*, provozní databáze, systémy pro online zpracování transakcí) jsou standardní databázové systémy s pevnou strukturou dat definovou pomocí databázového schématu. Jsou navrženy a optimalizovány pro chod provozních aplikací s primárním cílem zajistit rychlý a souběžný přístup k datům. To vyžaduje transakční zpracování, řízení souběžnosti a techniky obnovy (rollback), které zaručují konzistence dat. Díky těmto vlastnostem mají OLTP databáze špatný výkon při provádění složitých dotazů, které potřebují spojit mnoho relačních tabulek dohromady nebo agregovat velké objemy dat. Kromě toho obsahují typicky podrobná data a neobsahují historická data, která jsou při datové analýze potřeba.

OLAP OLAP (*Online Analytical Processing*, online analytické zpracování) je databázové paradigma specificky zaměřené na dotazy, zejména na analytické dotazy. Používají se zde jiné techniky indexování a optimalizace dotazů. Normalizace není pro toto paradigma žádoucí, protože rozděluje databázi na mnoho tabulek. Složité dotazy v takovém případě vyžadují rekonstrukci dat a s tím spojený vysoký počet spojování tabulek. Pracuje se s tzv. multidimenzionálními kostkami, avšak v pozadí jsou stále relační databáze.

NoSQL Potřeba ukládat proudy dat (zpracovávané v reálném čase bez možnosti poza-stavení), obrázky, multimédia, velké JSON soubory, ..., vedla ke vzniku NoSQL databází. NoSQL databáze používají jiné prostředky než tabulková schémata tradiční relační data-báze. Často jde o „hloupé“, nestrukturované uložiště klíč-hodnota.

BigData Velká, nestrukturovaná (různorodá), rychle rostoucí data, která není možné uložit ani zpracovávat běžnými přístupy (na jednom uzlu, jedním uzlem). Produkují je např.: IoT senzory, sociální sítě, chatovací aplikace, webové vyhledávače, ... Pro jejich zpracování je nutné využít distribuované systémy (pro uložení i zpracování).

Distribuované zpracování dat Distribuované zpracování dat je zpracování velkých dat (*big data*) pomocí distribuovaných systémů. To s sebou přináší problémy. Jak zaručit vhodnou distribuci dat a výpočtu mezi uzly? Jak řešit nespolehlivost a výpadky uzlů? Jak a kam zajistit doručení výsledků výpočtu? ...

6.3 MapReduce

Algoritmy pro indexování webových stránek (Page Rank) přestávaly být udržitelné, bylo potřeba zvýšit jejich škálovatelnost. Google vydal příspěvek „MapReduce: Simplified Data Processing on Large Clusters“, kde bylo představeno paradigma MapReduce. Jde o para-digma distribuovaného výpočtu založené na funkcích *map* a *reduce* z funkcionálního pro-gramování.

Map Funkce *map* má ve funkcionálním programování 2 vstupní parametry a vrací seznam hodnot. První parametr je unární operátor (nebo funkce fungující jako unární operátor) a druhý je seznam hodnot. Výstupní seznam je spočítán jako aplikace unárního operátoru na vstupní seznam. Příklad:

$$\text{map}(\text{square}, [1, 2, 3, 4]) = [1, 4, 9, 16]$$

. V paradigmata MapReduce *map* vrací data jako seznam dvojic klíč-hodnota, přesněji:

$$\text{map}((\text{key}, \text{value})) \rightarrow [(\text{key}, \text{value})]$$

Reduce Funkce *reduce* má ve funkcionálním programování 2 vstupní parametry a vrací jednu hodnotu. První parametr je binární operátor (nebo funkce fungující jako binární operátor) a druhý je seznam hodnot. Výstupní hodnota je spočítána jako postupná aplikace binárního operátoru na všechny hodnoty ve vstupním seznamu. Příklad:

$$\text{reduce}(+, [1, 4, 9, 16]) = 30$$

. V paradigmata MapReduce *reduce* bere na vstupu klíč a seznam hodnot a vrací opět seznam dvojic klíč-hodnota, přesněji:

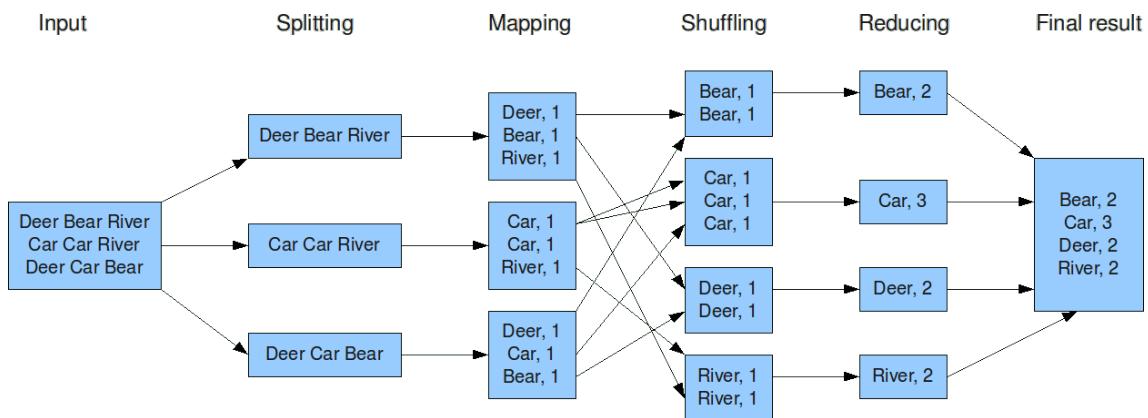
$$\text{reduce}(\text{key}, [\text{value}]) \rightarrow [(\text{key}, \text{value})]$$

```

1 def map(input_key: str, input_value: str) -> list[tuple[str, int]]:
2     # input_key - document name
3     # input_value - document content (etc. line)
4     result = []
5     for word in input_value.split(' '):
6         result.append((word, 1))
7     return result
8
9 def reduce(input_key: str, input_value: list[int]) -> tuple[str, int]:
10    result = 0
11    for val in input_value:
12        result += value
13    return (input_key, result)

```

Výpis 6.1: Příklad implementace funkcí *map* a *reduce* v paradigmatu MapReduce pro počítání četnosti slov ve vstupu v Pythonu.

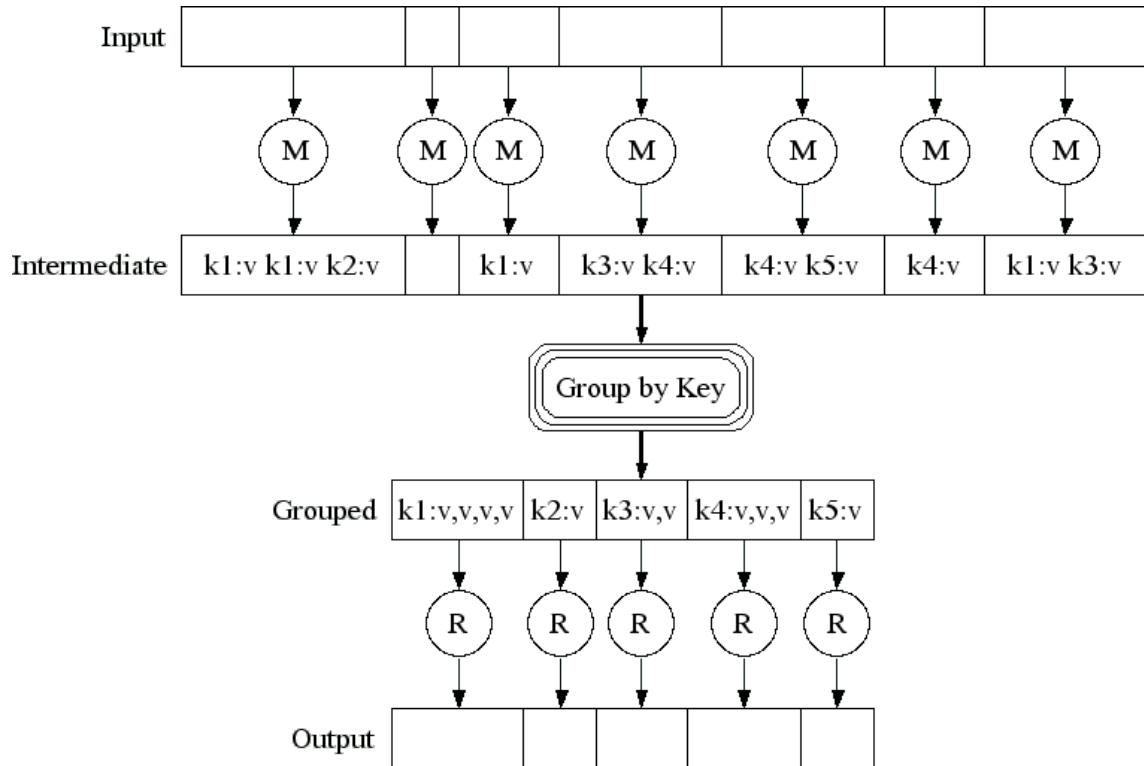


Obrázek 6.1: Úloha počítání četnosti slov v paradigmatu MapReduce v diagramu.

Průběh MapReduce Celý MapReduce probíhá v několika krocích, viz obrázek 6.1.

1. Input – Přípravený vstup pro distribuovaný výpočet (např. soubory ve virtuálním distribuovaném souborovém systému, viz dále HDFS).
2. Splitting – Rozdělení vstupu na části, které budou přiděleny jednotlivým uzelům. Může být výchozí (např. rozdělení textového souboru po řádcích) nebo definováno uživatelem.
3. Mapping – Každý uzel aplikuje funkci *map* na svoji přidělenou část. Uživatel definuje jak má funkce *map* vypadat.
4. Shuffling (také Grouping, Partitioning, Comparing) – Výpočetní uzly si mezi sebou vyměňí hodnoty, které spočítaly, na základě klíče. Tento krok zařizuje platforma pro distribuovaný výpočet sama o sobě, typicky na základě hashů klíčů. Tento krok je většinou *bottleneck*.

5. Reducing – Každý uzel zapojený do tohoto kroku (často je v tomto kroku potřeba méně uzlů, než v kroku mapping) aplikuje funkci *reduce* na svoji přidělenou část. Uživatel definuje jak má funkce *reduce* vypadat.
6. Final Result – Finální výsledek (např. zapsán do do virtuálního distribuovaného souborového systému, viz dále HDFS).



Obrázek 6.2: Výpočet MapReduce v obecném schématu.

Combiner Optimalizační krok, jde o „jakési“ provedení operace *reduce* už ve fázi *map* (každým uzlem). Tím je snížen počet mezivýsledků ve fázi Shuffling. Typicky funkce *combine* je stejná jako *reduce*.

Virtuální distribuovaný souborový systém Pro realizaci distribuovaného výpočtu je rovněž potřeba distribuovaný souborový systém (DFS). Ten je typicky realizován jako virtuální souborový systém nad jednotlivými souborovými systémy uzlů. Např.: GFS – Google File System, HDFS – Hadoop File System (viz dále). DFS obsahuje data samotná (*data nodes*) a metadata o tom, která data jsou na jakých uzlech (*name nodes*).



Obrázek 6.3: Výpočet MapReduce v obecném schématu a rozdělením práce na jednotlivé uzly (uzel je typicky víceprocesorový).

6.4 Apache Hadoop

Apache Hadoop je *open-source* implementace MapReduce paradigmatu vyvíjená Apache Software Foundation. Jde o implementaci v Java, ta je vhodná, jelikož díky JVM (Java Virtual Machine) je spouštění uživateli definovaných funkcí *map* a *reduce* snadné.

Hadoop MapReduce – Implementace MapReduce paradigmata. Data jsou čtena a ukládána na HDFS (včetně mezivýsledků). To znamená, můžeme pracovat v podstatě neomezenými daty, ale ukládání a načítání výpočet zpomalují.¹

HDFS HDFS (*Hadoop Distribute File System*) je virtuální distribuovaný souborový systém. Standardní soubor je rozdělen na datové bloky které jsou distribuovány na různé datové uzly. Architektura HDFS se skládá ze dvou typů uzlů – Name Node a Data Node. Name Node obsahuje alokační tabulkou pro souborový systém. Ví které datové bloky patří kterému souboru a kde jsou uloženy. Obsahuje další metadata jako názvy souborů, cesty, ... Data Node obsahuje datové bloky. Typicky redundancy a replikace, počítá se s možným selháním uzlů. Pro **čtení dat** se klient zeptá Name Nodu na konkrétní soubor v HDFS. Name Node vrátí metadata o souboru, na jakých Data Nodech se vyskytuje. Klient požádá příslušné Data Nody, ty mu pošlou data, která se na klientovi „poskládají“ do výsledného souboru. Pro **zápis dat** se klient zeptá Name Nodu, kam by měl zapisovat. Klient zapíše na příslušný Data Node. Data Node poté vyřeší replikace s dalšími uzly.

¹ Nebylo přednášeno podrobněji, pravděpodobně stačí princip obecného MapReduce, který byl vysvětlen v předchozí sekci.

Hadoop YARN Hadoop YARN je plánovač (*scheduler*). Plánuje výpočet tak, aby proběhl co nejlepším způsobem na konkrétní distribuované architektuře. Plánovač má obecné obecné rozhraní a Hadoop YARN lze nahradit za jiný.

Hadoop Common Hadoop Common jsou další knihovny a ovladače pro klienty.

Další nástroje Nad Apache Hadoop existuje mnoho dalších nástrojů. Apache Pig pro *high level* programování map-reduce úloh. Apache Hive pro dolování dat nad Apache Hadoop. Apache HBase jako distribuovaná databáze nad Apache Hadoop, ...

6.5 Apache Spark

Apache Spark je *open-source* nástroj pro distribuované zpracování rozsáhlých dat vyvíjený Apache Software Foundation. Hlavní cíl je zvýšení rychlosti. Spark na to jde přesunutím co nejvíce výpočtů do operační paměti jednotlivých uzlů a tím pádem zminimalizovat počet zápisů a čtení z DFS (snaha odstranit *bottleneck* v kroku shuffling u Hadoopu). Tím ale vzniká jiný problém, a sice výpadek uzlu znamená, že data jsou ztraceny.



Obrázek 6.4: Architektura Apache Spark. Hlavní je Spark Core, zbytek funguje na systému pluginů a může používat HDFS, Hadoop YARN a Hadoop Common.

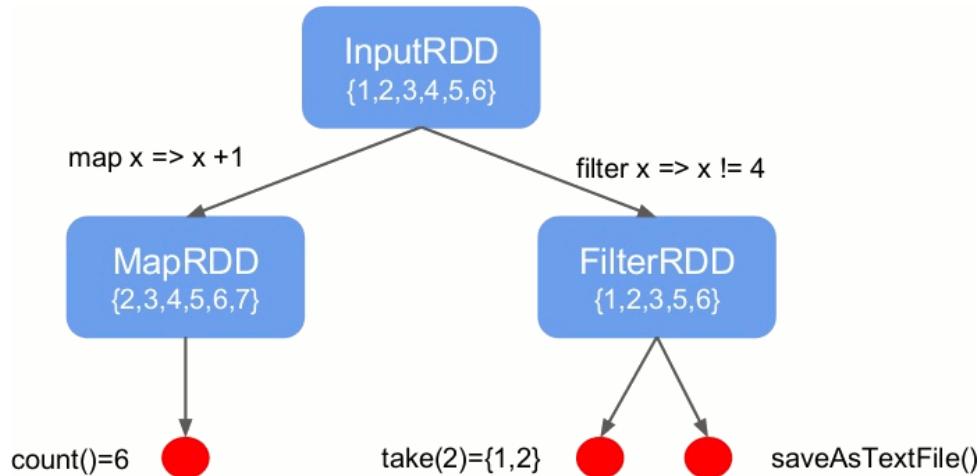
Resilient Distributed Dataset Resilient Distributed Dataset (RDD) je základní datová struktura Sparku. Jedná se o typované kolekce n-tic, které jsou neměnné (*read only*). Vstup je transformován na RDD a každá operace je pak transformace jednoho RDD na jiné.

$$RDD_1 \rightarrow map() \rightarrow RDD_2 \rightarrow reduce() \rightarrow RDD_3$$

Strategie vyhodnocování Spark uplatňuje strategii vyhodnocování *lazy evaluation*. Vyhodnocování výrazu je odkládáno až do doby, dokud není potřeba jeho hodnota. Zabraňuje opakování vyhodnocování. Je vyhodnocována pouze ta část, která je potřeba. RDD funguje jako abstraktní datová struktura, nemusí obsahovat data uvnitř, ale pouze předpis jak data získat a získá je, až když jsou potřeba.

Struktura výpočtu Struktura výpočtu odpovídá orientovanému acyklickému grafu (DAG, *Directed Acyclic Graph*). Uzly jsou RDD a hrany jsou transformace. DAG je znám i dalším uzlům, takže pokud nastane výpadek uzlu a výpočet je ztracen, může být uzel snadno zastoupen.

Klíčové vlastnosti Klíčové vlastnosti Sparku jsou *lazy evaluation*, *in-memory* a *parallel computing*.



Obrázek 6.5: Příklad výpočtu v Apache Spark.

Kapitola 7

Symetrická kryptografie. Vlastnosti, vlastnosti bezpečného algoritmu, délka klíče, útok silou, příklady symetrických algoritmů, Feistelovy šifry, DES, režimy činnosti, proudové šifry.

7.1 Metadata

- Předmět: Kryptografie (KRY)
- Přednáška:
 - 3) Symetrická kryptografie. Vlastnosti, vlastnosti bezpečného algoritmu, délka klíče, útok silou.
 - 4) Příklady symetrických algoritmů, Feistelovy šifry, DES, struktura, činnost, slabiny, režimy činnosti.
 - 5) Typické aplikace symetrické kryptografie.
- Záznam:
 - 2021-02-22
 - 2021-03-01
 - 2021-03-08

7.2 Úvod a kontext

Kryptografie Kryptografie (šifrování) je věda o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.

Kryptoanalýza Kryptoanalýza je věda zabývající se metodami získávání obsahu šifrovaných informací bez přístupu k tajným informacím, které jsou za normálních okolností potřeba, tzn. především k tajnému klíči.

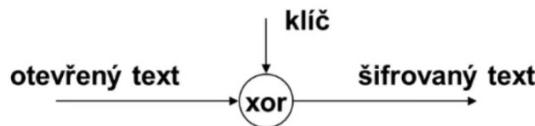
Kryptologie Jeden výraz pro kryptografii a kryptoanalýzu.

Caesarova šifra Princip Caesarovy šifry je založen na tom, že všechna písmena zprávy jsou během šifrování zaměněna za písmeno, které se abecedně nachází o pevně určený počet míst dále (tj. posun je pevně zvolen). Caesarova šifra spadá do kategorie substitučních šifer (stejný znak je při více výskytech vždy zašifrován na stejný znak).

Vigenerova šifra Rozšíření Caesarovy šifry, klíč je delší než 1 znak. Klíč je řetězec, který reprezentuje posuny. V případě že vstup je delší než klíč, je klíč perioricky opakován. Vigenerova šifra spadá do kategorie polyalfabetických substitučních šifer (stejný znak může být při více výskytech zašifrován na jiný znak).

Vernamova šifra (*One Time Pad*) Vernamova šifra spadá do kategorie polyalfabetických substitučních šifer a je i dnes nerozluštitelná pokud:

- klíč je delší než vstupní text,
- klíč se nepoužije opakováně,
- klíč je náhodný.



Obrázek 7.1: Vernamova šifra.

Autoklíč (*autokey*) Šifrování klíčem a když vstupní text je delší než klíč, tak se pokračuje šifrováním otevřeným nebo šifrovaným textem. Lze použít u Vigenerovy nebo Vernamovy šifry.

Symetrická kryptografie Algoritmy používají k šifrování i dešifrování stejný klíč. Výhodou symetrických šifer je jejich nízká výpočetní náročnost. Asymetrické šifry mohou být i stotisíckrát pomalejší. Nevýhodou je nutnost sdílení tajného klíče, takže jedna strana musí klíč vygenerovat a potom ho bezpečným způsobem předat druhé straně.

Typy útoků

- Ciphertext Only Attack (COA) – Útočník zná pouze zašifrovaný text a snaží se zjistit klíč nebo otevřený text. Nejčastější případ.
- Known Plaintext Attack (KPA) – Útočník zná zašifrovaný text a otevřený text a snaží se zjistit klíč.
- Chosen Plaintext Attack (CPA) – Útočník zná to co v KPA a navíc si text může zvolit.

Útok silou Při útoku silou (*brute force*) zkouší útočník všechny teoreticky možné klíče, dokud nenajde ten správný.



Obrázek 7.2: Princip kryptografie, podle typu klíčů dělíme na symetrickou (tajný klíč) a asymetrickou (veřejný klíč, soukromý klíč).

Bezpečný algoritmus V moderní kryptografii je nepřijatelné utajování algoritmů (*security by obscurity*) – předpokládáme, že útočník zná šifrovací algoritmus. Bezpečnost musí záviset pouze na utajení klíče (Kerckhoffuv princip, *security by design*). Symetrický algoritmus je považován za bezpečný, pokud neexistuje rychlejší útok než útok silou.

Délka klíče Dnes je považováno 80 bitů a více za dostatečné. Typicky se délka zaokrouhuje na mocninu 2 (typicky 128b). Klíče symetrických algoritmů jsou kratší než asymetrických. Konkrétně: DES – 56b, 3DES – 112, AES – variabilní.

Využití Symetrická kryptografie je vhodná pro šifrování většího objemu dat. Narozdíl od asymetrické, která je pro tento účel příliš pomalá. Proto např. HTTPS využívá asymetrickou kryptografií pro výměnu symetrických klíčů a poté symetrickou kryptografií pro šifrování provozu.

Vlastnosti moderní kryptografie Symetrická kryptografie zaručuje všechny následující, kromě nepopiratelnosti – více entit má k dispozici klíč.

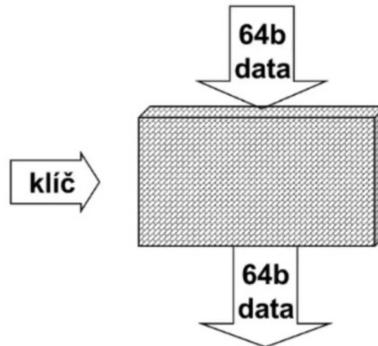
- Důvernost – Utajení informace. Bez znalosti klíče, není možné data číst.
- Autentizace – Prokázání, že zprávu skutečně poslal odesíatel a nikoliv útočník, který se za odesílatele vydává.
- Integrita – Prokázání, že nikdo nemohl data po cestě od odesílatele k příjemci změnit. Ochrana proti neoprávněné, neodhalené modifikaci zprávy.
- Nepopiratelnost – Pokud odesíatel data poslal, nemůže tuto skutečnost popřít.

7.3 Blokové šifry

Blokové šifry šifrují data po blocích pevně stanovené délky (64b, 128b, 256b, ...). Pokud je dat více, rozdělí se na více bloků, přičemž do zbylého místa v posledním je umístěno zarovnání *padding* (informace o délce zarovnání může být obsažena v posledním bytu). Příklady blokových šifer:

- Feistelova šifra (spíše princip)
- Data Encryption Standard (DES)
- Triple Data Encryption Algorithm (3DES)
- International Data Encryption Algorithm (IDEA)

- Blowfish
- Tiny Encryption Algorithm (TEA)
- Advanced Encryption Standard (AES)



Obrázek 7.3: Princip blokových šifer.

Feistelova šifra

Feistelova šifra (Feistelův princip) je koncept šifrování, který konkrétní algoritmy využívají. Jedná se o substituční-permutační síť. Vstupní blok je rozdělen na dvě poloviny L a R , výpočet výstupu pak vypadá následovně.

$$L_i = R_{i-1} \quad (7.1)$$

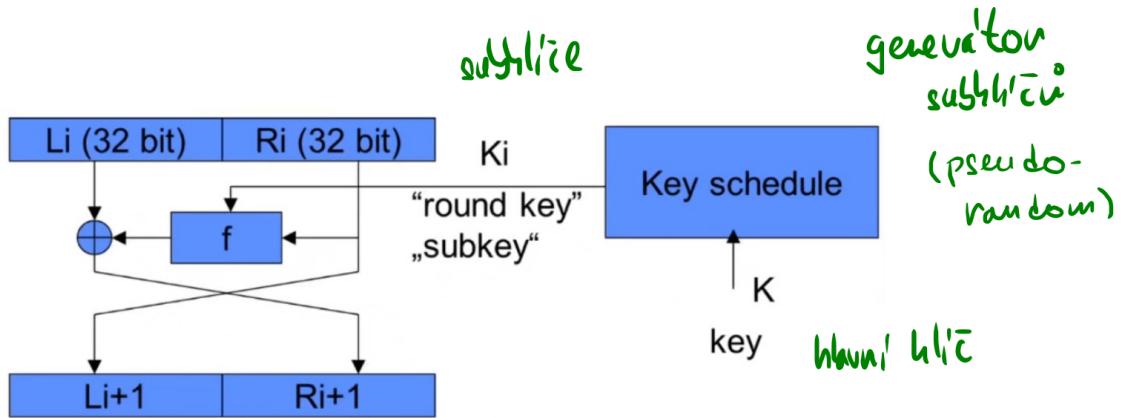
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \quad (7.2)$$

Funkce F F je funkce, na kterou Feistelova šifra neklade žádné požadavky. Jednotlivé algoritmy, využívající Festelovu šifru, funkci samy definují. Požadavky na funkci F , aby algoritmus byl bezpečný:

- skrytí vlastností zprávy;
- skrytí vlastností zprávy.

Subklíč K je tzv. subklíč, který je generován typicky nějakým pseudonáhodným generátorem na základě inicializačního klíče (hlavní).

Dešifrování Dešifrování se provádí stejným způsobem, pouze pořadí subklíčů je opačné.



Obrázek 7.4: Jeden krok opakování (Feistelův krok) vizuálně.

Příklad

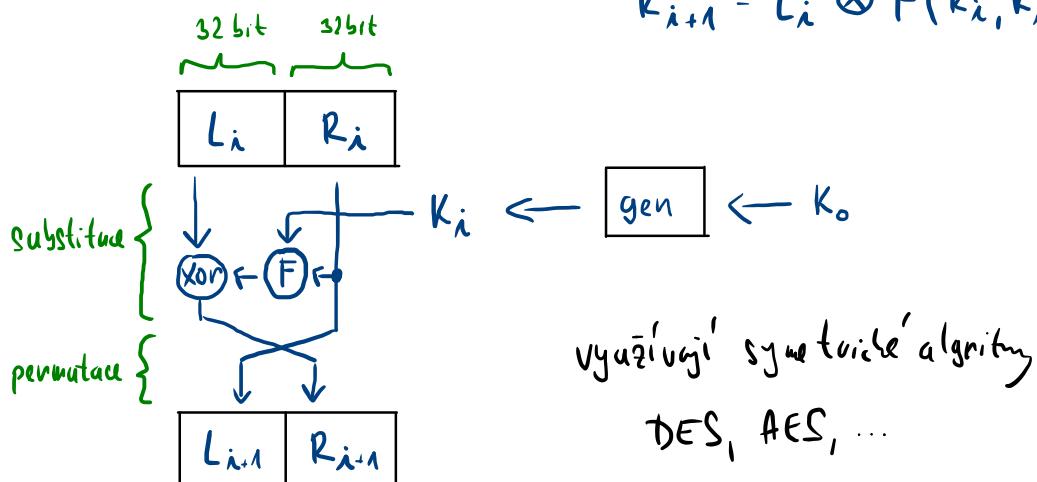
9. Nakreslit a popísať Feistelovu šifru, napísat algoritmus ktorý to používa.

- Princip klasických symetrických říz

- Vstup rozdělen na bloky o 64 bitech
↳ vstup rozšířen

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \otimes F(R_i, K_i)$$



Obrázek 7.5: Feistelova šifra – příklad a rekapitulace.

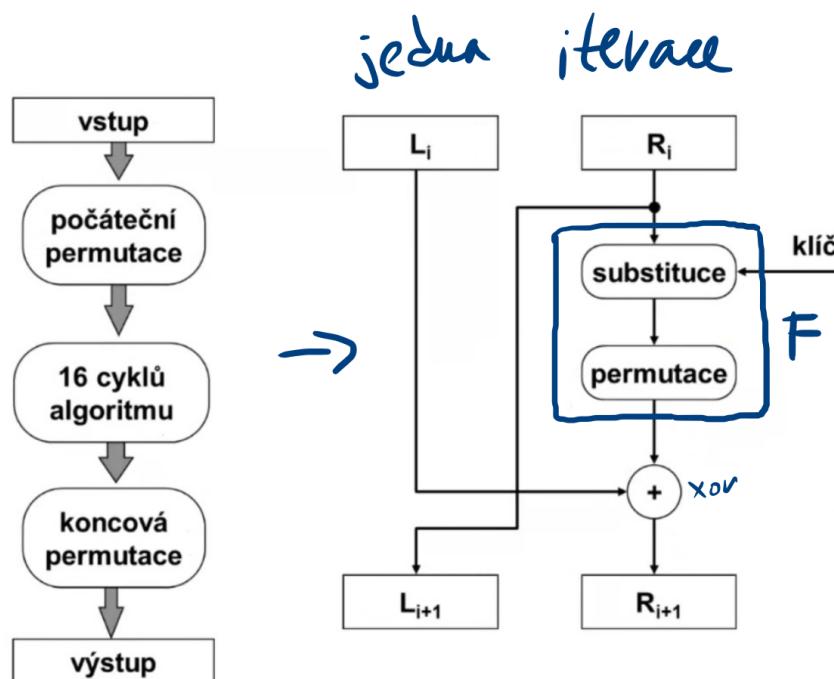
Data Encryption Standard (DES)

DES byl první algoritmus s veřejnou specifikací (*security by design*). Využívá princip Feistelovy šifry – 16 kol. Dodatečně přidává na začátek a konec permutaci navíc. Klíč je dlouhý 64b (resp. 56 významových bitů a 8 paritních).

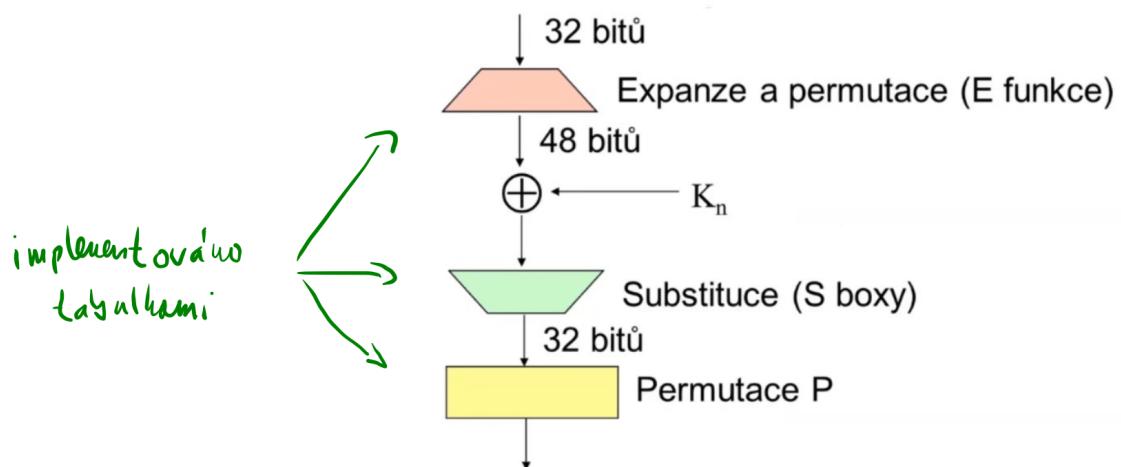
Slabiny

- 56 bitový klíč je příliš krátky a je možný útok silou.

- Rozdílná velikost bloku a klíče (zvláštnost).
- Existence slabých a poloslabých klíčů.
- Není jasné proč zrovna 16 iterací a zda je to dostatečné.



Obrázek 7.6: DES – Schéma fungování algoritmu.



Obrázek 7.7: DES – funkce F.



Obrázek 7.8: DES – generování subklíčů.

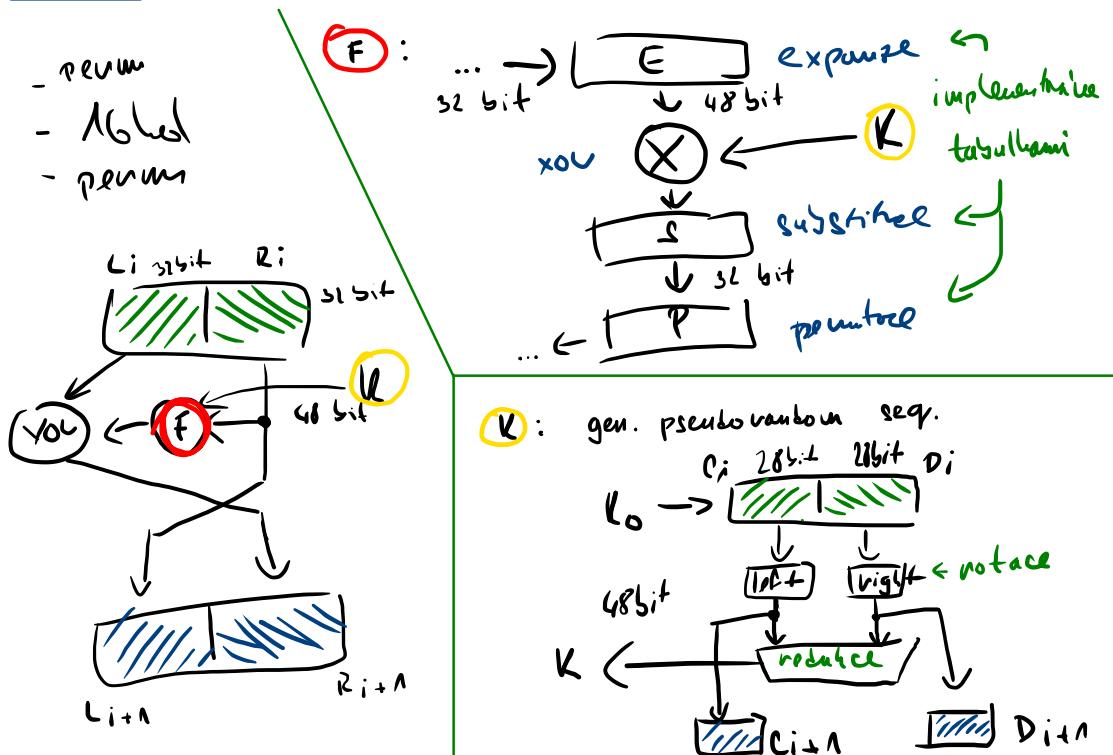


Figure 2.4 Single Round of DES Algorithm

Obrázek 7.9: DES – jedno kolo algoritmu. *Left shift* je ve skutečnosti bitová rotace.

Příklad

3. Nakreslete schema DES, včetně key scheduler, popište všechny 3 části funkce F, jaký mají účel a napишите proč je treba pochybovat o bezpečnosti DESu



Obrázek 7.10: DES – příklad a rekapitulace.

7.4 Provozní režimy činnosti blokových šifer

Jak použít blokové šifry abychom byli schopni šifrovat data delší než jeden blok?

Electronic Code Book (ECB)

ECB („kódová kniha“) je výchozí *naivní* režim. Bloková šifra se při něm přímo aplikuje nezávisle na jednotlivé bloky, tedy při daném klíči odpovídá stejnému bloku otevřeného textu stejný blok šifrového textu. To má nežádoucí důsledky z hlediska bezpečnosti, v datech zůstane původní struktura, např. šifrovaný obrázek je rozpoznatelný.



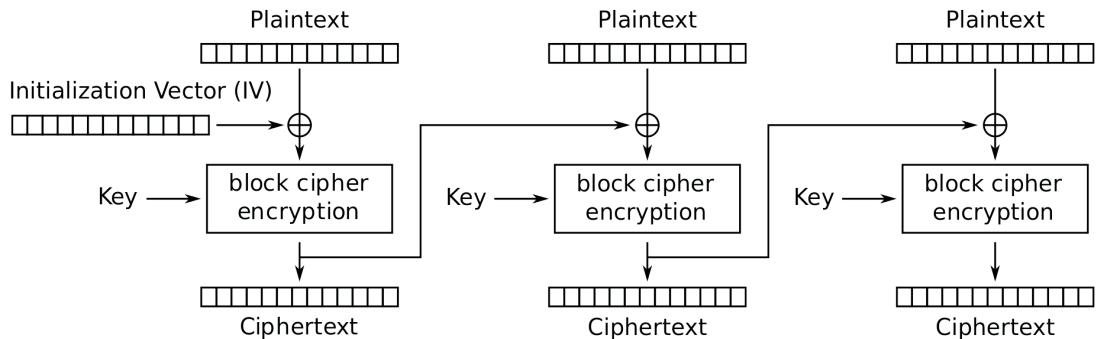
Electronic Codebook (ECB) mode encryption

Obrázek 7.11: Ukázka režimu ECB.

Cipher Block Chaining (CBC)

V režimu CBC („řetězení šifrových bloků“) je každý blok před šifrováním xorován zašifrovaným předchozím blokem a první blok je xorován inicializačním vektorem. Tento režim je široce používán. Nevýhody plynou ze zřetězené závislosti (šifrovaný blok závisí na všech předcházejících): Šifrování nelze paralelizovat a při poškození šifrového bloku nelze dešifrovat ani blok přímo následující. Dešifrování paralelizovat lze.

$$\begin{aligned} C_i &= E_K(P_i \oplus C_{i-1}) \\ P_i &= D_K(C_i) \oplus C_{i-1} \\ C_0 &= IV \end{aligned} \quad (7.3)$$



Cipher Block Chaining (CBC) mode encryption

Obrázek 7.12: Ukázka režimu CBC.

Cipher Feedback (CFB)

Režim CFB (šifrová zpětná vazba) se liší oproti CBC v prohození pořadí operací xor a šifrování – nejprve se zašifruje předchozí šifrovaný blok (resp. inicializační vektor) a výsledek se xoruje s otevřeným blokem. Toto prohození má významné implementační dopady: díky symetrii operace XOR vypadá dešifrovací funkce obdobně jako šifrovací. Šifruje pomaleji než CBC. Vstup není nutné zarovnávat. Plynou stejné nevýhody jako pro CBC.

$$\begin{aligned}
 C_i &= E_K(C_{i-1}) \oplus P_i \\
 P_i &= E_K(C_{i-1}) \oplus C_i \\
 C_0 &= IV
 \end{aligned} \tag{7.4}$$



Cipher Feedback (CFB) mode encryption

Obrázek 7.13: Ukázka režimu CFB.

Output Feedback (OFB)

Režim OFB (*výstupní zpětná vazba*) se liší od CFB pouze v tom, kde bere zpětnou vazbu. Šifrování probíhá pouhým xorováním otevřeného bloku s heslem, které je v každém kroku zašifrováno použitou blokovou šifrou. První blok hesla je získán zašifrováním inicializačního vektoru. Režim převádí blokovou šifru na synchronní proudovou šifru.

Slabina Celý blok encryption je pouze generátor pseudonáhdon posloupnosti (je nezávislá na otevřeném nebo šifrovaném textu). To umožňuje Known Plaintext Attack. Z toho plyne, že jedním klíčem není bezpečné šifrovat více než jednu zprávu.

$$\begin{aligned}
 C_i &= E_K(C_{i-1}) \\
 P_i &= P_i \oplus C_i \\
 C_0 &= IV
 \end{aligned} \tag{7.5}$$



Obrázek 7.14: Ukázka režimu OFB.

Counter (CTR)

Režim CTR („čítačový režim“) převádí stejně jako OFB blokovou šifru na synchronní proudovou. Heslo, se kterým se blok otevřeného textu xoruje, je však získáno zašifrováním čítače, který se každou iteraci zvětšuje o pevně danou hodnotu, zpravidla o 1. Obsah čítače je opět před šifrováním nastaven inicializačním vektorem. Každý blok je šifrován nezávisle na ostatních, díky tomu je možné paralelizovat.

$$\begin{aligned} CTR_i &= CTR_{i-1} + 1 \\ P_i &= P_i \oplus E_k(CTR_i) \\ CTR_0 &= IV \end{aligned} \tag{7.6}$$



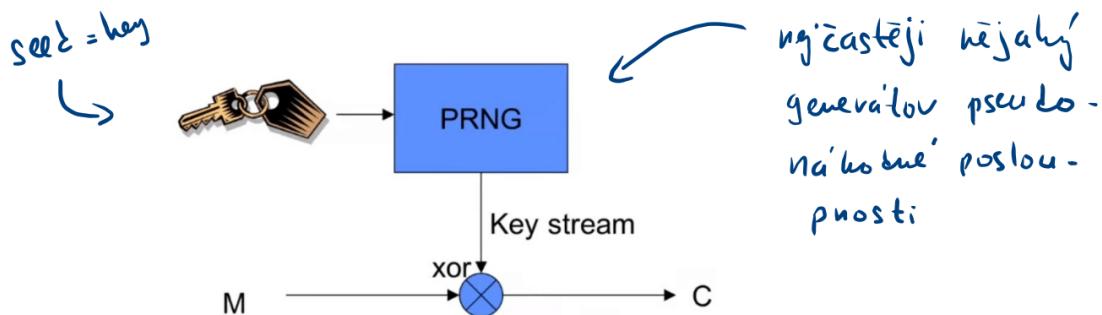
Obrázek 7.15: Ukázka režimu CTR.

7.5 Proudové šifry

Proudové šifry šifrují data jako *proud* (stream), nejčastěji po jednotlivých bytech. Dešifrování vždy probíhá stejným způsobem. Proudové šifry jsou rychlejší než blokové šifry a pro implementaci potřebují jednodušší hardware.

Problémy

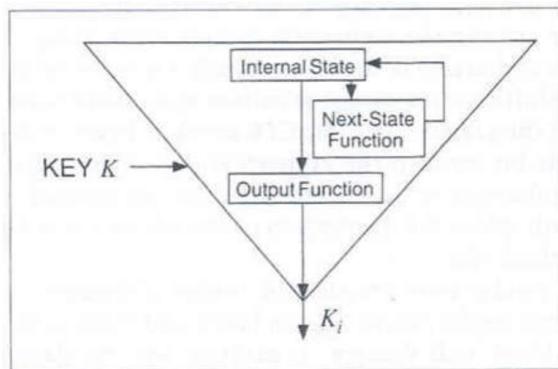
- Nezajišťují samy o sobě integritu.
- Na rozdíl od blokových šifer jsou náchylnější ke kryptoanalytickým útokům, pokud jsou nevhodně implementovány (počáteční stav nesmí být použit opakován) – „problém s inicializačním vektorem“.



Obrázek 7.16: Princip proudových šifer.

Rozdělení proudových šifer

Synchronní proudové šifry Proud pseudonáhodných čísel *key stream* je generován nezávisle na vstupním textu nebo zašifrované zprávě. Poté dochází ke kombinaci vygenerovaných čísel se vstupujícím textem (k zakódování) nebo se šifrovaným textem (k dekódování). Nejběžnější formou kombinace keystreamu a vstupního textu je použití operace XOR. Např.: Vernamova šifra, DES v režimu OFB. Pokud se průběhu dešifrování něco ztratí, je konec.



Obrázek 7.17: Princip synchronní proudové šifry.

Samosynchronizující proudové šifry Proud pseudonáhodných čísel *key stream* závisí na pevném počtu předcházejících bytů šifrovaného (nebo otevřeného) textu. To znamená, že se šifra dokáže po chybě sama *zotavit* (resynchronize)¹. Např.: Vigenere Autokey, DES v režimu CFB.

¹Dnes se nesnášíme dešifrovat poškozená data, pokud nastane chyba v přenosu, vyžádáme si data znova.



Obrázek 7.18: Princip samosynchronizující proudové šifry.

Generátory PRNG

Generátory PRNG (*pseudo-random number generator*) generují pseudo-náhodnou posloupnost (*key stream*) z malého klíče (*seed*).

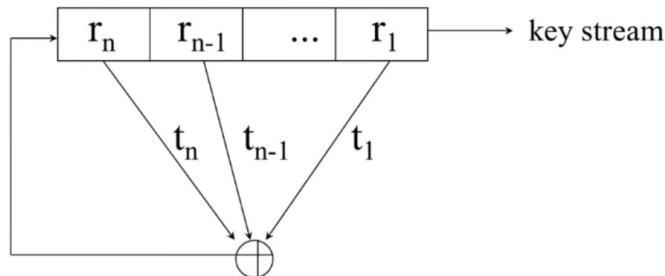
Blokové šifry v režimu OFB Blokové šifry v režimu OFB jsou pomalé.

Linear Feedback Shift Registers (LFSR) LFSR (posuvný registr s lineární zpětnou vazbou) je posuvný registr, jehož výstup je lineárně závislý na jeho předchozích výstupech a stavu. Mějme

- posuvný registr $R = (r_1, r_2, \dots, r_n)$,
- sekvenci zpětných vazeb $T = (t_1, t_2, \dots, t_n)$.

Alternativně lze zapsat polynomem:

$$T(x) = x^n + x^{n-1} + \dots + x + 1$$



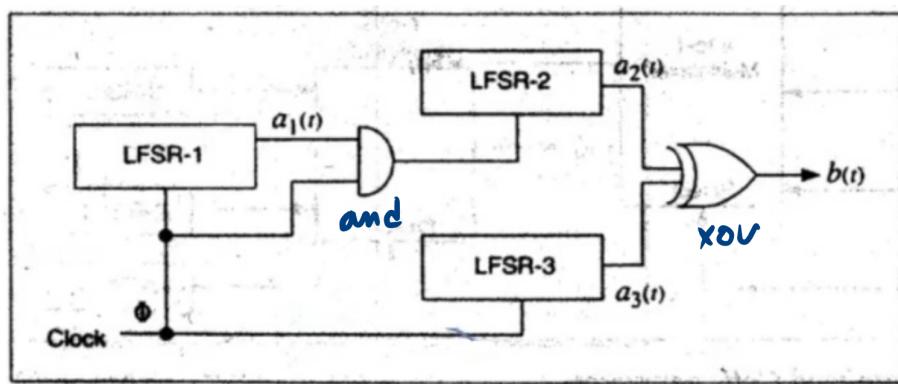
Obrázek 7.19: Příklad LFSR.

Geffe generátor Geffe generátor (kombinovaný generátor) je využití 2 a více LFSR propojených multiplexorem.



Obrázek 7.20: Příklad Geffe generátoru.

Stop and Go generátor Stop and Go generátor je několik LSFR s různým zdrojem hodin.



Obrázek 7.21: Příklad Stop and Go generátoru.

Kapitola 8

Asymetrická kryptografie, vlastnosti, způsoby použití, poskytované bezpečnostní funkce, elektronický podpis a jeho vlastnosti, hybridní kryptografie, algoritmus RSA, generování klíčů, šifrování, dešifrování.

8.1 Metadata

- Předmět: Kryptografie (KRY)
- Přednáška:
 - 6) Asymetrická kryptografie, vlastnosti, způsoby použití, poskytované bezpečnostní funkce.
 - 7) Elektronický podpis a jeho vlastnosti, hybridní kryptografie.
 - 8) Příklady asymetrických algoritmů, RSA.
- Záznam:
 - 2021-03-08
 - 2021-03-22

8.2 Úvod a kontext

Viz. „Úvod a kontext“ v předchozích otázkách z tohoto předmětu.

Asymetrická kryptografie

- V asymetrické kryptografii se používají páry klíčů (soukromý a veřejný). Soukromý je používán k dešifrování, resp. vytvoření digitálního podpisu. Veřejný je používán k šifrování, resp. ověření digitálního podpisu.
- Každý uživatel generuje svůj pár klíčů. Veřejný klíč je zveřejněn (znají ho všichni), soukromý je držen v tajnosti (zná ho pouze vlastník).

- Všechny asymetrické algoritmy jsou blokové.
- Asymetrické algoritmy jsou pomalejší než symetrické.

Způsoby použití Asymetrická kryptografie lze využít k:

- šifrování,
- digitálnímu podepisování,
- pro výměnu symetrického klíče (*key exchange*).

Vlastnosti Vlastnosti symetrické a asymetrické kryptografie¹.

	Důvěrnost	Autentizace	Integrita	Nepopiratelnost
Symetrická	ano	?	?	ne
Asymetrická - šifrování	ano	?	?	ne
Asymetrická - podepisování	ne	ano	ano	ano
Asymetrická - kombinace	ano	ano	ano	ano

```

1 # Odesilatel (A):
2 msg = encrypt(msg, SK_A) # nechť msg je zprava k~odeslani
3 msg = encrypt(msg, PK_B)
4 send(msg_2)
5
6 # Přjemce (B):
7 msg = receive()
8 msg = decrypt(msg, SK_B)
9 msg = decrypt(msg, PK_A)

```

Výpis 8.1: Kombinace klíčů obou stran u asymetrické kryptografie. Pořadí operací může být i opačné.

Digitální podpis Vytvoření digitálního podpisu konkrétních dat pomocí soukromého klíče podepisatele. Každý kdo zná veřejný klíč podepisatele, může pravost podpisu ověřit. Digitální podpis zajišťuje autentizaci, integritu a nepopiratelnost.

Algoritmy Algoritmy asymetrické kryptografie se nedají *vymyslet*, musí se objevit. Jsou založeny na těžkých matematických problémech.

- Problém batohu (*knapsack problem*) – MH (Merkle-Hellman)
- Faktorizace čísel – RSA (Rivest-Shamir-Adleman)
- Diskrétní logaritmus – DSA (Digital Signature Algorithm), DH (Diffie-Hellman)
- Eliptické křivky – ECDSA, ECDH

Problém batohu Problém batohu je NP-úplný problém kombinatorické optimalizace. Nechť x_1, x_2, \dots, x_n je množina objektů, každý objekt má svoji cenu v_i a svoji hmotnost w_i , dále mějme batoh, který má kapacitu W . Cílem je vybrat takovou množinu objektů,

¹Otazníky – částečně, za předpokladu, ...

jejichž hmotnost je menší nebo rovna W a má nejvyšší možnou cenu². Formálně chceme maximalizovat sumu

$$\sum_{i=1}^n v_i \cdot x_i$$

, při splnění

$$\sum_{i=1}^n w_i \cdot x_i \leq W$$

, kde $x_i \in x_1, x_2, \dots, x_n$.

Faktorizace čísel Faktorizace čísel označuje problém rozložení čísla na součin menších čísel, v nejčastější podobě pak rozklad celého čísla na součin prvočísel.

Diskrétní logaritmus Necht' p, g, k, Y jsou přirozená čísla, pro něž platí $Y \equiv g^k \pmod{p}$. Potom každé číslo k odpovídající uvedené rovnici nazveme diskrétní logaritmus o základu g z Y vzhledem k modulu p . Tato definice nedefinuje číslo k jednoznačně, proto se někdy upravuje tak, že ze všech možných diskrétních logaritmů ve smyslu předchozí definice se vybere ten nejmenší.

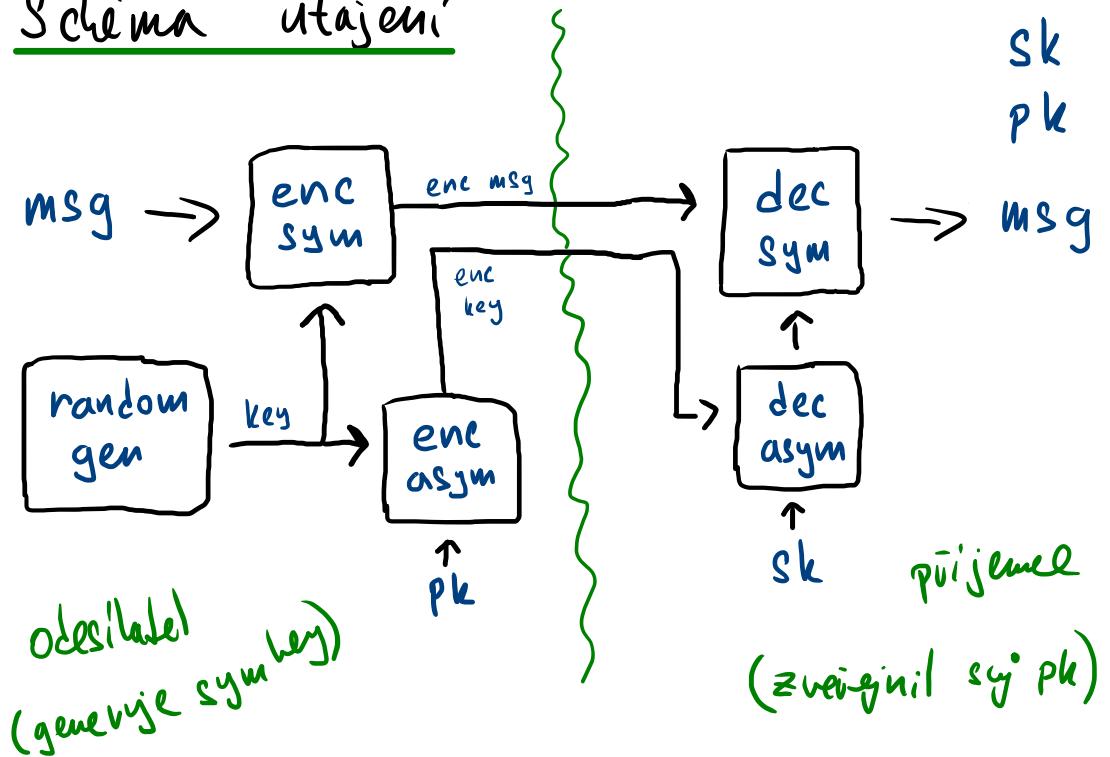
Eliptické křivky Jedná se o matematický aparát, na kterém aplikujeme různé algoritmy (DSA, DH).

8.3 Hybridní kryptografie

Hybridní kryptografie je kombinace symetrické a asymetrické kryptografie, ve které jsou využity přednosti obou (symetrická – rychlá, ale potřeba stejný klíč; asymetrická – pomalá, ale dva klíče). Asymetrická je využita pro bezpečné zaslání symetrického klíče.

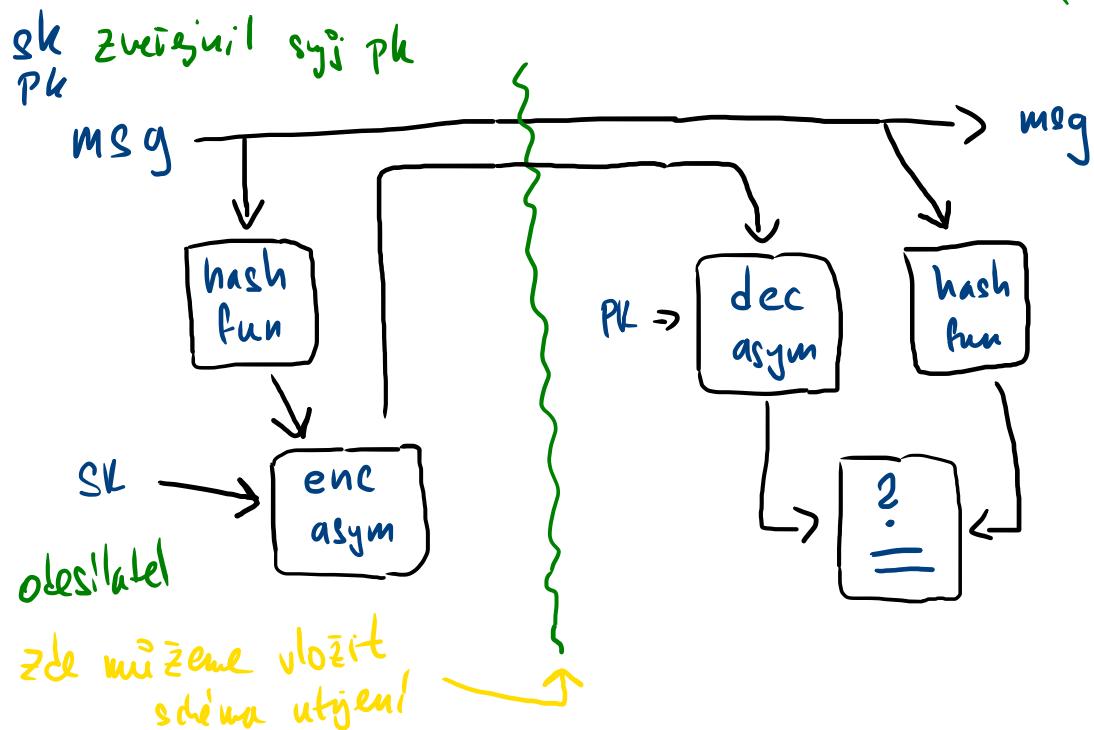
²Problém má více obdobných variant.

Schéma utajení



Obrázek 8.1: Schéma utajení hybridní kryptografie.

Schéma digitálního podpisu



Obrázek 8.2: Schéma digitálního podpisu hybride kryptografie.

8.4 RSA

Algoritmus RSA (Rivest-Shamir-Adleman) lze použít jak pro šifrování dat pro digitální podepisování. Je založen na problému faktorizace velkých čísel.

Klíče Klíče se skládají z:

- p, q – dvě náhodná soukromá prvočísla,
- n – veřejný modul ($n = p \cdot q$),
- e – veřejný exponent ($e < \Phi(n)$ \wedge $GCD(\Phi(n), e) = 1$), typicky 3 nebo $2^{16} + 1^3$,
- d – soukromý exponent,
- musí platit vztah: $e \cdot d \bmod \Phi(n) = 1$.

Veřejný klíč $PK = (n, e)$, soukromý klíč $SK = (n, d)$.

Postup generování Postup generování klíčů:

1. vygenerovat prvočísla p a q ,
2. spočítat modul $n = p \cdot q$,
3. spočítat $\Phi(n) = (p - 1) \cdot (q - 1)$,

³ GCD – největší společný dělitel

4. zvolit veřejný exponent $e < \Phi(n) \wedge GCD(\Phi(n), e) = 1$,
5. spočítat soukromý exponent d tak, že platí $e \cdot d \bmod \Phi(n) = 1$.

Šifrování a dešifrování Mějme zprávu m reprezentovanou jako celé číslo a zašifrovanou zprávu c reprezentovanou také jako celé číslo. Digitální podpis se vytváří stejným způsobem, pouze se prohodí exponenty.

$$c = m^e \bmod n \quad (8.1)$$

$$m = c^d \bmod n \quad (8.2)$$

Útoky a slabiny Pokud útočník rozloží číslo n na činitele p a q , tak může dopočítat soukromý klíč. Pokud útočník uhádne hodnotu $(p-1) \cdot (q-1)$, tak může dopočítat soukromý klíč. Šifrování malých čísel je zranitelné, proto se používá „předzpracování“ – zarovnání na X bitů (2048).

Příklad

1. RSA $n = 143$, $p = 11$, $q = 13$, $e = 7$. Vypočítat d , napsat VK, PK a zašifrovat číslo 9.

$$p = 11$$

$$q = 13$$

$$n = p q = 143$$

$$e = 7$$

$$\Phi(n) = (p-1)(q-1)$$

$$\Phi(143) = 10 \cdot 12 = 120$$

$$e \cdot d \bmod \Phi(n) = 1$$

$$7d \bmod 120 = 1$$

$$d = 103$$

$$VK = (n, e) = (143, 7)$$

$$SK = (n, d) = (143, 103)$$

$$m = 9$$

$$120x + 7y = 1$$

$$gcd(120, 7)$$

$$\begin{aligned} 120 &= 17(7) + 1 \\ 1 &= 120 - 17(7) \end{aligned}$$

$$\begin{aligned} 1 &= 120 - 17(7) \\ -17(7) &= 1 \\ -17 + 120 &= 103 \end{aligned}$$

$$C = m^e \bmod n = 9^7 \bmod 143 = 4782969 \bmod 143 = \underline{\underline{48}}$$

$$m = C^d \bmod n = 48^{103} \bmod 143 = \underline{\underline{9}}$$

Obrázek 8.3: Příklad RSA.

Kapitola 9

Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti.

9.1 Metadata

- Předmět: Kryptografie (KRY)
- Přednáška:

– KRY04_Asym_MNG.pdf

- Záznam:

– 2021-03-22

9.2 Historie položení otázky

- Rok: 2013
 - Jméno otázky: Haš, klíčovaný haš, HMAC
 - Zkoušel: Hanáček Petr, doc. Dr. Ing.
 - Známka: E
 - Zacal jsem definici hasovaci funkce, ten slajd, pak padla otázka klíčovaný has, tak zas definice co to je a tak. Potom chtěl vědět útoky a složitost útoku a jeho pravděpodobnost. K tomu jsme se s jeho značnou pomocí úspěšně dobrali. Dost pomáhal.
- Rok: 2014
 - Jméno otázky: Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti
 - Zkoušel: Hanáček Petr, doc. Dr. Ing.
 - Známka: E
 - Co jsem k tomu rekl(a)/na co se ptali/co mne vytkli: Ptal se na MAC, říkal jsem že slouží pro podpis a začal jmenovat ty 3 potřebné podmínky pro hash.funkce. Tím sem si sám naběhl, protože jsem zapomněl 2nd preimage. Na to, co jsem místo toho „vyvářil“, řekl, že to je ale 1st preimage, a chtěl to vědět správně, nakonec to musel říct za mě. Dál se ptal na sílu hashe, takové to, co bylo i letos na zkoušce, že pro útok vůči collision resistance je složitost 2^{80} i když hash má délku 2^{160} . Patlal jsem se v tom, tak nakonec chtěl přesně vědět jak se na každou věc útočí a jakou složitost to bude mít.

- Rok: 2015
- Jméno otázky: Hašovací funkce, klíčovaný haš, MAC
- Zkoušel: Hanáček Petr, doc. Dr. Ing.
- Známka: E
- Začal jsem tím, co je to hašovací funkce, jaké jsou na ní kladené podmínky (preimage resistance, ...). Tam mě Hanáček přerušil a začal se ptát, kolik pokusů musí útočník vyzkoušet při útoku hrubou silou, aby pokořil každou z těch podmínek. Úplně jsem se do toho zamotal, rozklepal jsem se a nebyl schopen kloudného slova. Hanáčkův poker face v tom taky nijak nepomáhal, ale asi se snažil nějak pomoci (To n značí prostor vstupních dat? Jak chcete, jen se ptám.), a ačkoli jsem to věděl, nebyl jsem v tu chvíli schopen formulovat odpověď. Nechal mě v tom ještě hodnou chvíli koupat a pak to ukončil.
- Rok: 2018
- Jméno otázky: Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti
- Zkoušel: Hanáček Petr, doc. Dr. Ing.
- Známka: B
- Prvně jsem uvedl co je hašovací funkce (základní definice, first preimage resistance, second preimage resistance, collision resistance). P. Hanáček se následně začal doptávat na vztah mezi second preimage resistance a collision resistance včetně potřebné síly útoku. Kolem tohoto tématu jsme se točili asi další 2 minuty. Následně se P. Hanáček dotázel na klíčovaný haš a MAC, což jsem obecně popsal. Zmínil jsem také jakým způsobem se klíč přidává ke zprávě a částečně jsem popsal HMAC. Následně se P. Hanáček zeptal, k čemu je klíčovaný haš dobrý - uvedl jsem, že zajišťuje integritu dat a autentizaci, což se při neklíčovaných hašovacích funkcích musí zajistit například podpisem pomocí asymetrické šifry. Tím také zkoušení skončilo. Trvalo 5-6 minut. Přestože, jsem byl na tuto otázku připraven, nebylo zkoušení moc příjemné a P. Hanáček mě občas dokázal docela znejistit.
- Rok: 2018
- Jméno otázky: Hašovací funkce, klíčovaný haš a MAC a jejich použití a vlastnosti
- Zkoušel: Hanáček Petr, doc. Dr. Ing.
- Známka: A
- Začal jsem takové obecné kely a rychle se přesunul na požadavky/vlastnosti, které chceme aby hashovací funkce měla. Popsal jsem First Preimage, Second Preimage a Collision Resistance. Pak jsme docela dlouho zůstali viset na rozdílu mezi second preimage a collision resistance. Celkově se mi pan docent snažil naznačit, jak mám mezi nimi tedy určit ten rozdíl. Ptal se mne pak jak je to s útoky, tak jsem zmínil, že je zde Birthday paradox, a uvedl jsem, že na 160 bitech stačí typicky projít 2^{80} možností než dojdu ke kolizi. Na to myslím, námitky nebyly a přesunuli jsme se ke klíčovanému haši. Někde na začátku zazvonil budík, ale jeli jsme dál. Řekl jsem, že tam je ten klíč, a řekl jsem, že jsme si uvedli některé typy použití, ale nejvýznamnější je HMAC. Zeptal jsem se, zda jej chce popsat, což nechtěl. Načež byl dotaz – K čemu ten klíčovaný hash slouží, tak jsem řekl že autentizaci. S tím pan docent souhlasil. Zeptal se mne, že co to znamená pro útočníka z hlediska bezpečnosti, tak jsem řekl, že je to pro něj horší, protože nezná klíč, což sice částečně potvrdil, ale chtěl pak ještě něco, ale to už si napamatují a nevěděl jsem to.

9.3 Úvod a kontext

Viz. „Úvod a kontext“ v předchozích otázkách z tohoto předmětu.

Hashovací funkce Hashovací funkce je funkce (resp. algoritmus) pro převod vstupních dat do (relativně) malého čísla. Výstup hashovací funkce se označuje otisk, *fingerprint*, *digest* či *hash*. Jsou jednosměrné a odolné proti kolizím (viz vlastnosti).

Obecné vlastnosti Hashovací funkce by měla:

- Být aplikovatelná na argument o libovolné velikosti.
- Mít výstup konstantní délky.
- Dokázat spočítat výstup rychle.

Neklíčované hashovací funkce Hashovací funkce má pouze jeden argument – data. Např. MD2, MD4, MD5, SHS, SHA1, SHA2, SHA3.

$$f(data) \rightarrow hash$$

Klíčované hashovací funkce Hashovací funkce má dva argumenty – data a klíč. Také se jim někdy říká MAC (*message authentication code*).

$$f(data, key) \rightarrow hash$$

9.4 Kryptografická odolnost hashovacích funkcí

Vlastnosti z hlediska odolnosti Hashovací funkce by z hlediska kryptografické odolnosti měly splňovat:

- *First preimage resistance* – Pro konkrétní y je výpočetně nezvládnutelné najít takové x , aby platilo $h(x) = y$. Útočník má k dispozici konkrétní hash, a snaží se pro něho nalézt zprávu.
- *Second preimage resistance* – Pro konkrétní x je výpočetně nezvládnutelné najít takové x' , aby platilo $h(x) = h(x')$. Útočník má k dispozici konkrétní zprávu (nemůže si ji zvolit), ke které se snaží nalézt jinou zprávu, která bude mít stejný hash.
- *Collision resistance* – Je výpočetně nezvládnutelné najít libovolnou dvojici x, x' takovou, aby platilo $x \neq x'$ a $h(x) = h(x')$. Útočník si může zvolit libovolnou zprávu, ke které se snaží nalézt jinou zprávu, která bude mít stejný hash. Pokud platí *collision resistance*, tak platí i *second preimage resistance*.

Narozeninový problém V teorii pravděpodobnosti je narozeninový problém úloha vypočítat minimální početnost skupiny lidí, ve které je alespoň 50% pravděpodobnost nalezení dvojice se stejným datem narození. Narozeninovým paradoxem je pak označována skutečnost, že tento počet (23) je mnohem menší než intuitivní odhad. Výsledek je intuitivnější, když uvážíme, že porovnání narozenin bude provedeno mezi všemi možnými dvojicemi jedinců. Při počtu 23 jedinců je třeba uvažovat $(23 \cdot 22)/2 = 253$ dvojic, což je více než polovina počtu dnů v roce (182, 5).

Jednodušší je nejprve spočítat jev opačný $\bar{p}(n)$, tedy pravděpodobnost, že všech n narozenin je rozdílných. Pro $n > 365$ je 1, jinak:

$$\begin{aligned}\bar{p}(n) &= 1 \cdot \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdots \left(1 - \frac{n-1}{365}\right) = \\ &= \frac{365 \cdot 364 \cdots (365-n+1)}{365^n} = \\ &= \frac{365!}{365^n (365-n)!}\end{aligned}\tag{9.1}$$

$$p(n) = 1 - \bar{p}(n)\tag{9.2}$$

Narozeninový útok Mějme hashovací funkci, která má n bitový výstup (celkový počet možných hashů je 2^n). Útočník vytvoří dokument „přátelská dohoda“ a přibližně $2^{n/2}$ sémanticky ekvivalentní verzí (úprava bílých znaků, úprava pořadí celků, jiné formulace, ...). Podobně vytvoří dokument „nepřátelská dohoda“ a přibližně $2^{n/2}$ sémanticky ekvivalentní verzí. S pravděpodobností 0,5 existuje verze „přátelské dohody“ a „nepřátelské dohody“, které mají stejný hash. Pokud takové verze existují, útočník dá oběti podepsat „přátelskou dohodu“ \Rightarrow existuje validní podpis „nepřátelské dohody“.

Bezpečnostní cíle OWHF Bezpečnostní cíle OWHF (*one way hash function*). Některé protokoly nevyžadují bezkoliznost, proto má smysl řešit i tento případ.

- Vyžadované vlastnosti: *first preimage resistance* a *second preimage resistance*
- Cíl útočníka: vytvořit *first preimage* nebo *second preimage* (oba úkoly jsou stejně těžké)
- Složitost: $O(2^n)$ (n je počet bitů hashe)
- Požadovaná délka: $n \geq 80$

Bezpečnostní cíle CRHF Bezpečnostní cíle CRHF (*collision resistance hash function*).

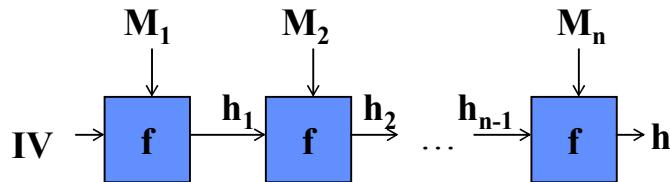
- Vyžadované vlastnosti: *collision resistance*
- Cíl útočníka: vytvořit kolizi
- Složitost: $O(2^{n/2})$ (n je počet bitů hashe) (kvůli narozeninovému útoku)
- Požadovaná délka: $n \geq 160$

Bezpečnostní cíle MAC Bezpečnostní cíle MAC (*message authentication code*).

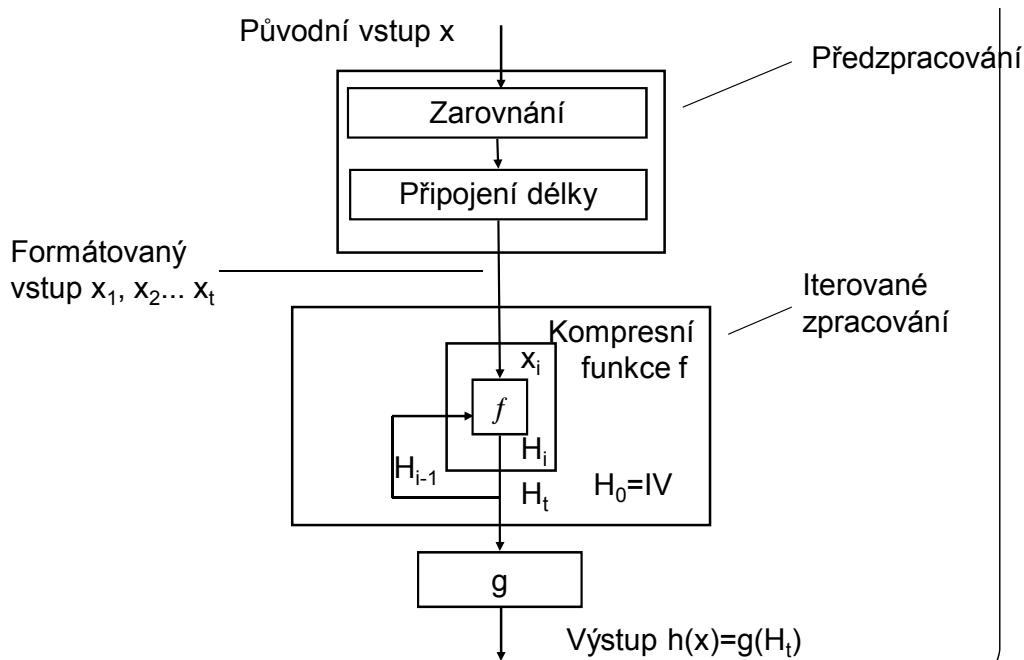
- Vyžadované vlastnosti: *computation resistance*, *key non-recovery*
- Cíl útočníka (útočník si může vybrat):
 - Vytvořit nový hash, který bude odpovídat nové zprávě
 - Nalézt klíč
- Složitost (n je počet bitů hashe, t je počet bitů klíče):
 - Vytvořit nový hash: $O(\max(2^{-n}, 2^{-t}))$
 - Nalézt klíč: $O(2^n)$
- Požadovaná délka: $n \geq 64 \wedge t \geq 64$

9.5 Hashovací funkce neklíčované

Nejčastější způsoby sestrojení hashovací funkce neklíčované jsou založené na principu iterace.



Obrázek 9.1: Schéma iterativní neklíčované hashovací funkce. Zpráva je rozdělena na n částí. f je tzv. kompresní funkce. IV je inicializační vektor, resp. konstanta. h_1 až h_{n-1} jsou mezivýsledky („mezihashe“) a h je výsledný hash.



Obrázek 9.2: Podrobnější schéma iterativní neklíčované hashovací funkce.

Jednotlivé kroky hashovací funkce:

- Předzpracování – Vstupní data jsou rozdělena na bloky o stejně délce. Je provedeno zarovnání posledního bloku. Je připojena informace o délce zprávy.
- Iterativní zpracování – V iteracích se postupně „přihashovávají“ vstupní bloky. Zpětná vazba pomocí stavové proměnné. Uvnitř kompresní funkce, která z delšího vstupu udělá kratší výstup.
- Postzpracování – Volitelný krok.

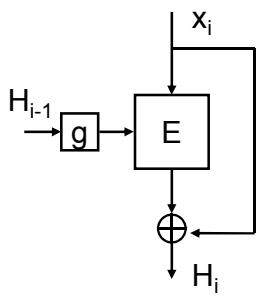
Merkelova meta-metoda Necht' f je kompresní funkce odolná proti kolizím. Hashovací funkce h na principu iterace využívající kompresní funkci f je rovněž odolná proti kolizím.

Merkel-Damgardovo zesílení Pokud je do vstupu hashovací funkce vložena délka zprávy, tak je zajištěno, že žádná zpráva není prefixem jiné zprávy.

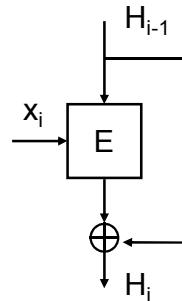
Zarovnání Nejednoznačné zarovnání (*ambiguous padding*) – připoj ke zprávě kolik bitů, aby délka zprávy byla násobkem délky bloku. Jednoznačné zarovnání (*unambiguous padding*) – připoj ke zprávě jeden bit a poté proved’ nejednoznačné zarovnání.

Hashovací funkce s využitím blokových šifer

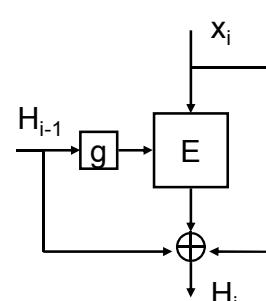
Alternativně lze využít pro konstrukci hashovacích funkcí blokové šifry. Avšak blokové šifry byly navrhovány pro jiný režim činnosti, kterém útočník nezná klíč (a není schopen ho ovlivnit), zná pouze šifrovaný text (ten je schopen ovlivnit). V tomto případě útočník může přímo ovlivňovat hodnoty klíče.



Matyas-Meyer-Oseas



Davies-Meyer

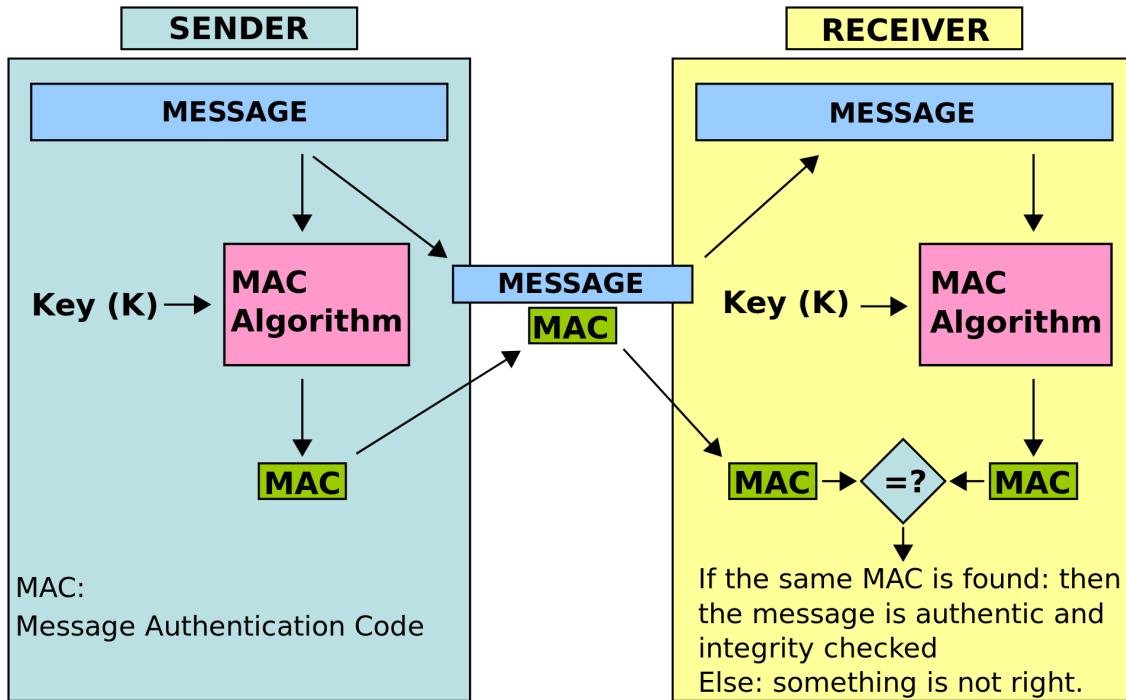


Miyaguchi-Preneel

Obrázek 9.3: Ukázka několika možných způsobů využití blokových šifer pro konstrukci kompresní funkce. S využitím iteračního způsobu lze zobecnit pro celou hashovací funkci.

9.6 MAC (*message authentication code*)

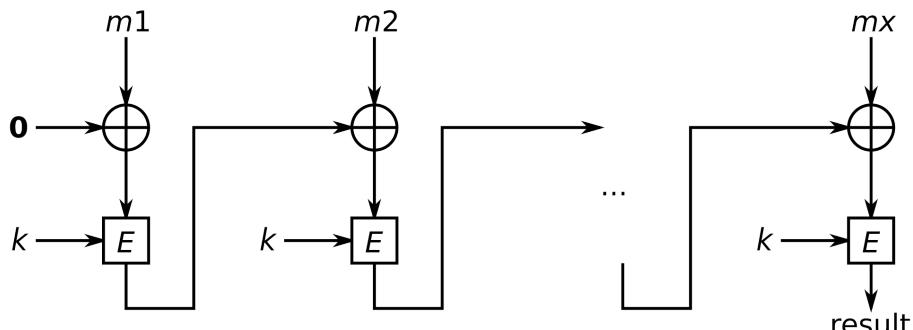
- Rodina hashovacích funkcí h_k , které jsou parametřitelné klíčem k .
- Vlastnosti (stejné jako u obecných hashovacích funkcí, pouze rozšířené o klíč):
 - Výstup $h_k(x)$ lze spočítat rychle, pokud je znám klíč k .
 - Jsou výpočetně bezpečné – při znalosti dvojice $(x, h_k(x))$ je výpočetně nemožné spočítat novou dvojici $(x', h_k(x'))$, pro $x \neq x'$, pokud není znám klíč.
- Využití: zajištění autentizace a integrity (nepopiratelnost zajistit nedokáže).



Obrázek 9.4: Schéma použití MAC. Pokud je stejný MAC výpočítán na straně příjemce, tak má jistotu, že zpráva nebyla po cestě změněna a že zprávu poslal skutečně odesílatel.

Sestrojení MAC pomocí blokové šifry v CBC

Pro sestrojení MAC hashovací funkce je využita symetrická bloková šifra v režimu CBC (*cipher block chaining*, šifrová zpětná vazba). Rozdíl oproti CBC šifrování spočívá v tom, že mezivýsledky se zahazují a pracuje se až s posledním blokem. Z něho se vezme určitý počet posledních bitů (podle požadované délky hashe – 32, 48, 64) a ten tvoří výsledný hash (MAC).



Obrázek 9.5: Ukázka sestrojení MAC funkce pomocí symetrické blokové šifry v režimu CBC.

Proč stačí výrazně menší délka? Protože klíč. Útočník sice může vyzkoušet všechny možné hashe, ale bez znalosti klíče, nezjistí, který je ten správný.

Sestrojení MAC pomocí neklíčované hashovací funkce

Pro sestrojení MAC hashovací funkce je využita neklíčovaná hashovací funkce. Klíč je připojen ke zprávě a je použita standardní hashovací funkce.

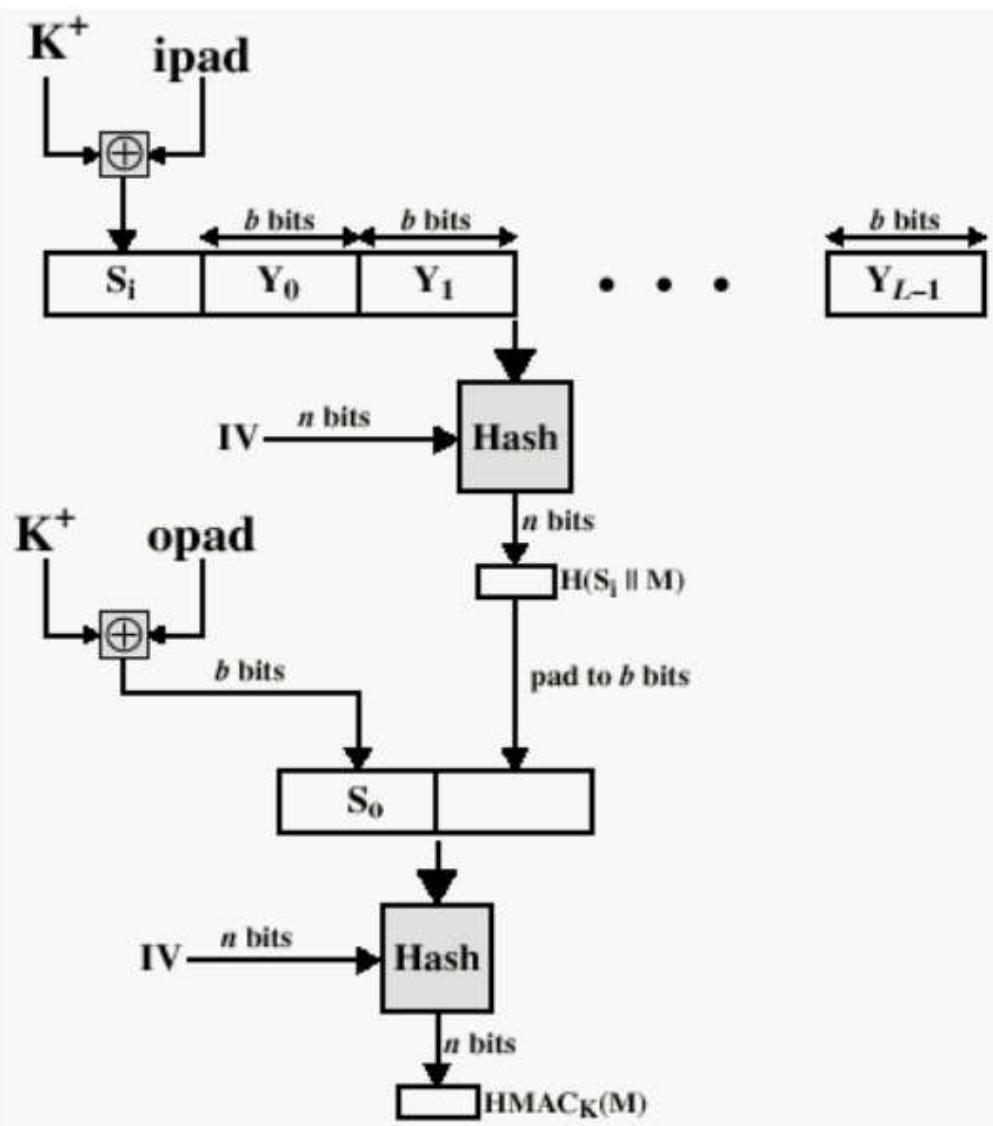
Secret prefix Klíč je přidán na začátek zprávy. Formálně: $H = h(k||x)$, kde H je výsledný hash (MAC), h je hashovací funkce, k je klíč a x je zpráva. Útočník může libovolně „při-hashovávat“ další bloky bez znalosti klíče a tím vytvářet nové validní hashe – $h(k||x||y)$, kde y je útočníkova zpráva \Rightarrow nepřijatelný způsob.

Secret suffix Klíč je přidán na konec zprávy. Formálně: $H = h(x||k)$. Útočník, který může zvolit x , může také vytvořit x' , pro které $h(x) = h(x')$ se složitostí $O(2^{n/2})$, kde n je délka hashe, bez ohledu na délku klíče k (narozeninový útok) \Rightarrow nepřijatelný způsob (útok který je neovlivnitelný délkou klíče).

Enveloping Klíč je přidán na začátek i na konec zprávy. Formálně: $H = h(k||p||x||k)$, kde p je zarovnání. Přijatelný způsob. Základ pro algoritmus HMAC.

9.6.1 HMAC (*hash function MAC*)

HMAC (*hash function MAC*) je do dnes používaný algoritmus. Specifikuje použití metody *enveloping*, ale ne, která hashovací funkce se použije.



Obrázek 9.6: Schéma HMAC; $ipad$ a $opad$ jsou vstupní/výstupní konstanty, které slouží k zarovnání; Y_i jsou bloky vstupní zprávy; IV je inicializační vektor.

Kapitola 10

Správa klíčů v asymetrické kryptografii (certifikáty X.509).

10.1 Metadata

- Předmět: Kryptografie (KRY)
- Přednáška:
 - KRY04_Asym_MNG.pdf
- Záznam:
 - 2021-03-29

10.2 Historie položení otázky

- Rok: 2016
 - Jméno otázky: Správa klíčů v asymetrické kryptografii
 - Zkoušel: Staudek Jan, Doc. Ing. CSc.
 - Známka: E
 - Předpokládal jsem že se mě ptá Hanáček, začal jsem mluvit směrem k němu, začal jsem o principech asymetrické kryptografie, asi po půl minutě mě přerušil Staudek (který do té doby spal), že tohle vědět nechce, tak jsem začal o certifikátech, zase mě přerušil, že to taky nechce, takhle se to opakovalo ještě jednou, tak jsem se ho přímo zeptal, že co jako chce slyšet, vytřeštil oči a koukal na mě tak se do toho vložil Hanáček, asi se mi snažil nějak pomoci, ale v jeho případě to nepadal moc na úrodnou půdu, moc jsme si nerozuměli co se týkalo záměn slov certifikát a klíč, motali jsme se v tom, základní myšlenku jsem sice řekl, ale Staudek do toho pořád rýpal, že to slyšet nechce, ale prostě nebylo vůbec jasné, co chce. Byl dost nepřijemný, strašně mumlal, nebylo mu rozumět a když jsem mu nerozuměl a chtěl at' zopakuje otázku, tak odpovídal dost nasraně, jako by to bral jako útok na sebe. Čas jsem překročil asi dvojnásobně, a byť jsem většinu času mluvil, a myslím si že k věci a korektně, tak při odchodu jsem si nebyl úplně jistý, že mi to dá, ale prošlo to.
- Rok: 2018
 - Jméno otázky: Správa klíčů v asymetrické kryptografii
 - Zkoušel: doc. Ing. Václav Zeman Ph.D.

- Známka: C
- Nechal mě chvíli mluvit, řekl jsem že v asym. Jsou 2 klíče - SK, VK, které generuje uživatel, je tam CA, které spravuje a podepisuje VK uživatelů, jaké tam jsou položky. A pak se začal ptát, protože viděl, že vzpomínám tak nějak marně :D. Ptal se na něco ve stylu, jak bych ověřil platnost certifikátu nějakého uživatele, tak jsem začal plácat o tom, že normálně dotaz a pak nad CA je strom CA a ty potvrzují CA... ale chtěl slyšet něco jiného... a poslední otázka byla jak bych to implementoval, že je tam nějaké políčko, na kterém to CA podepisuje tak chtěl vědět jak se jmeneje, to jsem si nevzpomněl, tak řekl, že mu to stačí. Venku mi kamarád řekl, že by se na to dalo použít LDAP... kdo ví.

10.3 Úvod a kontext

Viz. „Úvod a kontext“ v předchozích otázkách z tohoto předmětu.

Problém se zveřejňováním veřejných klíčů Jak můžu vědět, že publikovaný veřejný klíč patří opravdu entitě, které patří? Je potřeba zajistit autenticitu (pravost) veřejných klíčů – Vytvořit spolehlivou vazbu mezi veřejným klíčem a jménem jeho vlastníka.

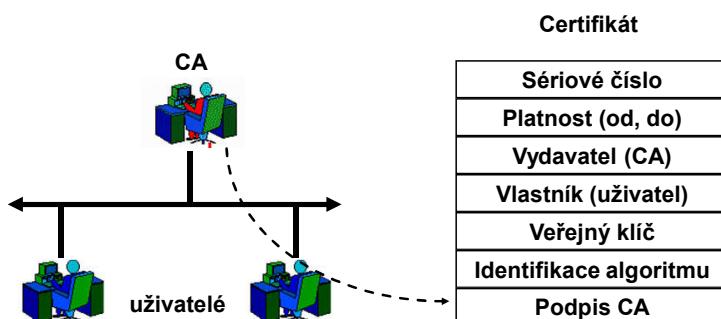
Systémy založené na veřejném klíči Systémy založené na veřejném klíči (PKI, *Public Key Infrastructure*) je označení infrastruktury správy a distribuce veřejných klíčů. PKI umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy bez nutnosti jejich individuální kontroly.

10.4 Správa klíčů v asymetrické kryptografii

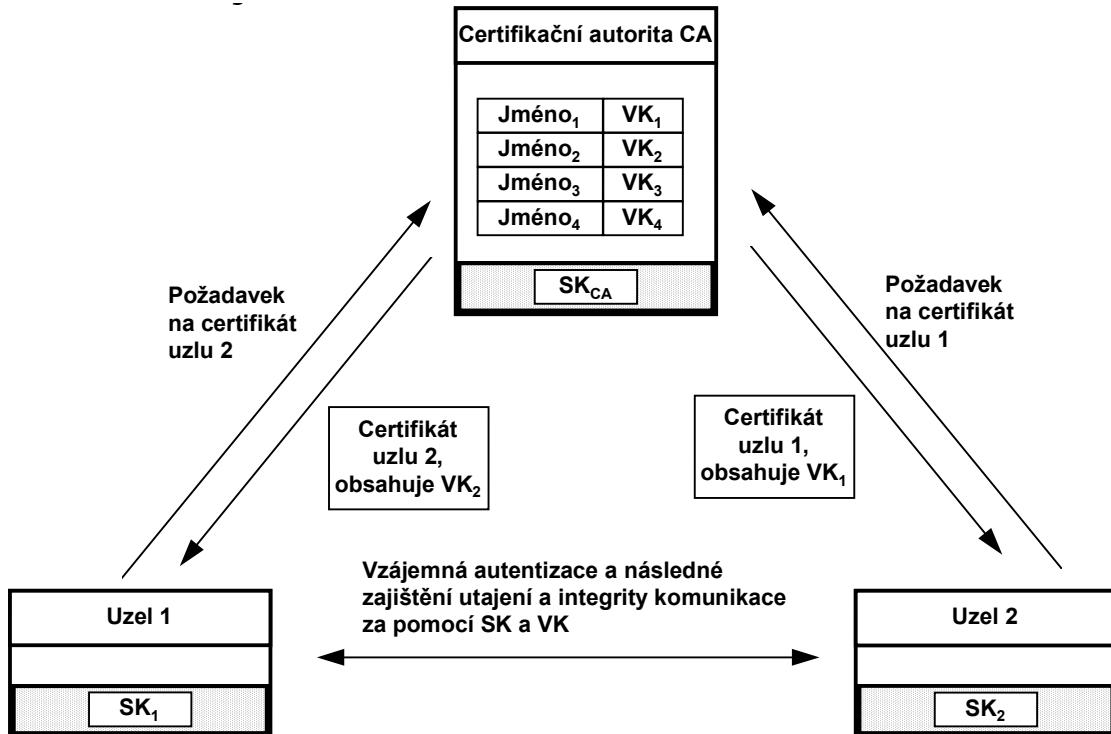
Certifikát Certifikace veřejného klíče. Nějaký prostředník (certifikační autorita), kterému důvěrujeme, se zaručuje, že konkrétní veřejný klíč, patří dané entitě.

Certifikační autorita Certifikační autorita (CA) je prostředník, který distribuuje certifikáty a které všechni důvěřují. CA negeneruje klíče uživatelům, ty si je generují samy.

Proces certifikace klíče CA podepíše veřejný klíč uživatele a jeho další údaje (jméno, doba vydání, doba platnosti, ...) svým soukromým klíčem. Tyto podepsané údaje se nazývají certifikát.



Obrázek 10.1: Příklad certifikátu.



Obrázek 10.2: Příklad navázání bezpečné komunikace mezi dvěma entitami, které mají stejnou certifikační autoritu.

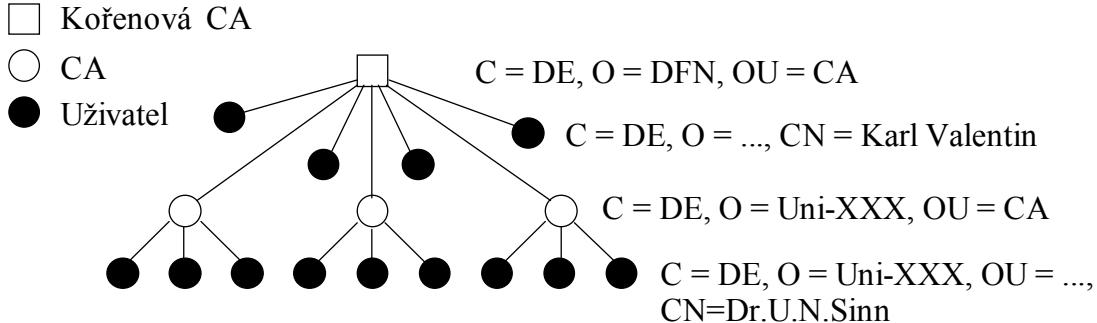
Navázání bezpečné komunikace Popis navázání bezpečné komunikace (viz obrázek 10.2):

1. Uzel 1 si vygeneruje soukromý a veřejný klíč.
2. Uzel 1 odešle veřejný klíč certifikační autoritě spolu se svým jménem (a dalšíma informacemi).
3. CA vytvoří certifikát pro uzel 1 – svým soukromým klíčem podepíše veřejný klíč a jméno uzlu 1. CA odešle certifikát uzlu 1. CA odešle svůj veřejný klíč uzlu 1.
4. Pokud uzel 2 chce také odesílat, provede také kroky 1-3.
5. Uzel 1 podepíše soubor a odešle ho uzlu 2 (soubor a podpis).
6. Uzel 2 si musí sehnat certifikát uzlu 1. Existují 3 způsoby jak to udělat.
 - Odesílatel zašle svůj certifikát společně se zprávou.
 - Příjemce si vyžádá certifikát odesílatele od certifikační autority.
 - Příjemce si vyžádá certifikát odesílatele od jiné služby (adresářové služby, LDAP).
7. Uzel 2 ověří podpis u certifikátu uzlu 1 veřejným klíčem certifikační autority.
8. Uzel 2 ověří podpis souboru pomocí veřejného klíče odesílatele (který je v certifikátu).

Strom certifikačních autorit Model s jednou globální CA je nemožný (příliš mnoho uživatelů, příliš velké vzdálosti, ...). Proto se používá strom certifikačních autorit. Veřejný klíč CA je certifikován jinou CA. CA nejvýše ve stromu se nazývá **kořenová certifikační autorita**.

- Certifikační autorita má svůj vlastní certifikát, který je podepsaný její certifikační autoritou.

- Koncový uživatel důvěřuje stále pouze jedné entitě – kořenové certifikační autoritě, ale přibývá jedna úroveň ověřování navíc.
- Příjemce dostane zprávu s podpisem. Musí znát certifikát odesílatele (podepsaný CA), certifikát certifikační autority (podepsaný CA_{root}) a veřejný klíč kořenové CA¹.
- Úrovní certifikačních autorit může být více (nejčastěji 1-2).



Obrázek 10.3: Příklad stromu certifikačních autorit. C, O, OU je identifikátor entity.

Certifikační cesta Posloupnost certifikátů od certifikátu kořenové CA přes certifikáty dalších CA až k certifikátu komunikující protistrany.

Zneplatnění certifikátu Jak zrušit platnost certifikátu? Normálně se zruší sám, až skončí jeho platnost. Pokud je potřeba certifikát zneplatnit před jeho vypršením je třeba využít tzv. revokační seznam (CRL, *certificate revocation list*). Důvody zneplatnění certifikátu:

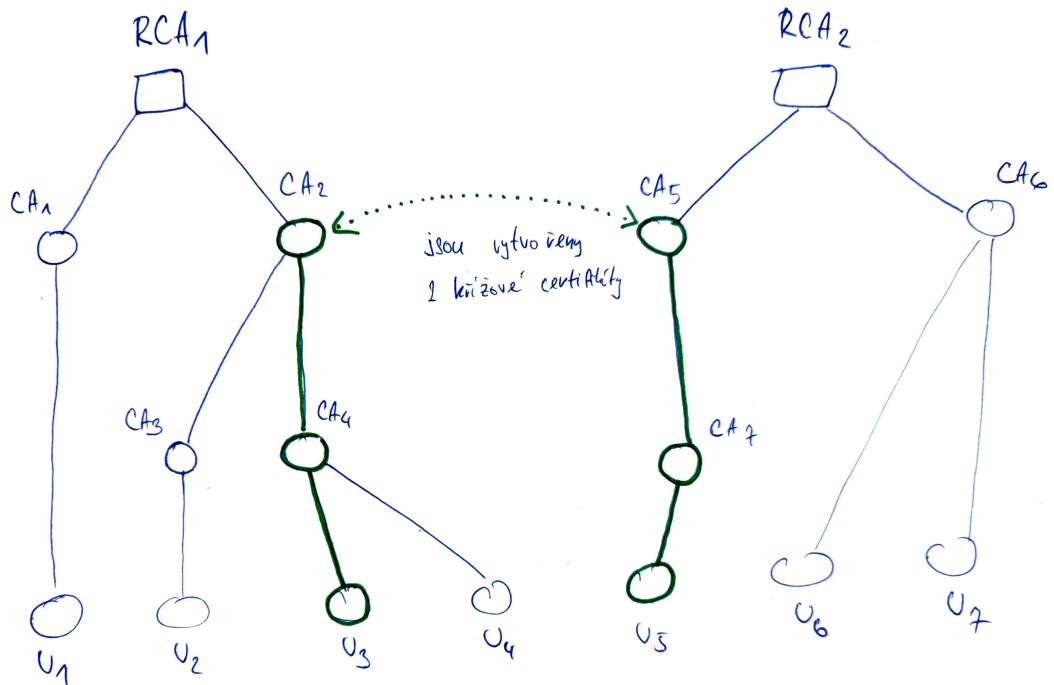
- soukromý klíč uživatele byl kompromitován,
- uživatel ztratil práva, která z certifikátu vyplývají (např. změna zaměstnavatele),
- soukromý klíč CA byl kompromitován (nikdy se nestalo).

CRL CRL (*certificate revocation list*) je seznam zneplatněných certifikátů, takových, kterým ještě nevypršela platnost, ale je třeba je zneplatnit. CRL je podepsán CA, které ho spravuje a periodicky aktualizuje (může se zkracovat i růst). Jak se distribuuje:

- *Pull model* – Příjemce certifikátu si dle potřeby stáhne CRL od CA.
- *Push model* – CA pravidelně posílá CRL příjemcům certifikátu.

Křížový certifikát V případě, že spolu komunikují uživatelé, kteří nemají společnou kořenovou CA (jejich CA si nedůvěřují), je třeba využít tzv. křížový certifikát. Tím se komplikuje sestavování certifikační cesty, protože je třeba zvážit všechny křížové certifikáty, které jsou k dispozici.

¹Veřejný klíč kořenové certifikační autority se z praktických distribuuje ve formě „fiktivního certifikátu“



Obrázek 10.4: Příklad křížového certifikátu. Uživatel U_3 chce navázat bezpečné spojení s uživatelem U_5 . Nemají společnou kořenovou CA, proto je třeba využít křížové certifikáty. CA2 vytvoří křížový certifikát pro CA_5 a CA_5 vytvoří křížový certifikát pro CA_2 . Příklad: U_3 pošle podepsanou zprávu U_5 , jak bude vypadat certifikační cesta?

$$U_3 \leftarrow CA_4 \leftarrow CA_2 \leftarrow CA_5 \leftarrow RCA_2.$$

10.5 Standard X.509

X.509 je standard pro systémy založené na veřejném klíči (PKI). Specifikuje formát certifikátů, formát CRL, parametry certifikátů, metody kontroly platnosti certifikátů, ...

```

1 Certificate ::= SIGNED SEQUENCE {
2     version [0] Version DEFAULT v1988,
3     serialNumber CertificateSerialNumber,
4     signature
5     AlgorithmIdentifier,
6     issuer
7     Name,
8     validity
9     Validity,
10    subject
11    Name,
12    subjectPublicKeyInfo SubjectPublicKeyInfo
13 }
14
15 Version ::= INTEGER {v1988(0) }
16
17 CertificateSerialNumber ::= INTEGER
18
19 Validity ::= SEQUENCE {notBefore UTCTime, notAfter UTCTime }
20
21 SubjectPublicKeyInfo ::= SEQUENCE {
22     algorithm
23     AlgorithmIdentifier,
24     subjectPublicKey
25     BIT STRING
26 }
27
28 AlgorithmIdentifier ::= SEQUENCE {
29     algorithm
30     OBJECT IDENTIFIER,
31     parameters
32     ANY DEFINED BY algorithm OPTIONAL
33 }

```

Výpis 10.1: Příklad definice certifikátu ve formátu X.509.

Význam položek Význam položek v definici certifikátu ve formátu X.509:

- Version – Standardně 0.
- Serial number – Sériové číslo certifikátu, spolu se jménem vydavatele jednoznačně identifikuje certifikát.
- Issuer – Jméno vydávající CA.
- Subject – Jméno vlastníka certifikátu.
- Validity – Doba platnosti certifikátu (`notBefore`, `notAfter`). Podpis je platný pouze pokud je datum podepsání v intervalu platnosti každého z certifikátů z certifikační cesty.
- SubjectPublicKeyInfo – Veřejný klíč vlastníka certifikátu a algoritmus, pro který je určen.
- Signature – Jakým algoritmem je certifikát podepsaný CA.

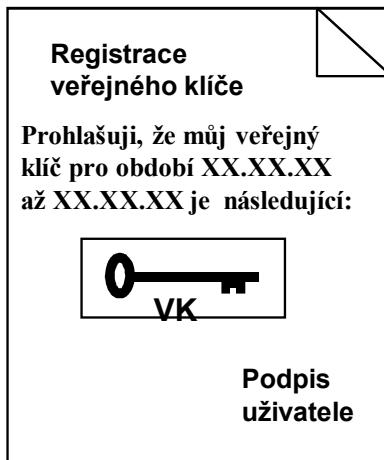
Prototypový certifikát Má strukturu certifikátu X.509. Uživatel si vygeneruje tzv. prototypový certifikát, který má standardní strukturu a vyplní informace na nějaké implicitní

hodnoty. Prototyp pošle CA spolu se svým veřejným klíčem, která certifikát dovyplní, podepíše a pošle zpět.

Registrační autorita Pokud chce uživatel vydat certifikát, kontaktuje tzv. registrační autoritu (nikoliv přímo CA).

Míra důvery v certifikát V praxi chceme více urovní důvěry, než pouze ostrý/žádný (např. chceme vytvořit testovací certifikát). To je řešeno jako rozšíření X.509 přidáním třídy certifikátu (*certification class*). Uživatel chce vydat certifikát od CA jisté třídy.

- Třída 1 – CA vůbec nekontroluje identitu žadatele. Lze jej získat anonymně. Používá se pro testovací certifikáty.
- Třída 2 – Identita žadatele musí být ověřena třetí stranou (notářsky ověřený formulář zasláný poštou).
- Třída 3 – Standardní certifikát. Žadatel musí osobně navštívit CA (resp. registrační autoritu). Osobní ověření totožnosti.
- Třída 4 – Stejně jako 3 a navíc je nutné prokázat oprávnění žadatele požadovat certifikát.



Obrázek 10.5: Příklad žádosti o certifikát.