# Kryptografické systémy s verejným kľúčom

Katedra matematiky a teoretickej informatiky, FEI TU

# Symetrické šifry - opakovanie

- Vymenujte **5 režimov symetrických blokových šifier**.
- Ktoré šifry patria medzi **najpoužívanejšie** symetrické šifry?
- Uveďte **vlastnosti** najpoužívanejších blokových šifier.

# Princíp kryptografie s verejným kľúčom:

**Slabé miesta v koncepcii symetrického šifrovania**

- bezpečná distribúcia kľúčov utajenými kanálmi obom komunikačným stranám $\Rightarrow$ proces výmeny šifrovaných dát sa môže začať až keď je distribúcia tajného kľúča ukončená

**Nový prístup v distribúcii kľúčov:**

- algoritmus Diffie–Hellman - umožnil realizovať výmenu tajných kľúčov cez verejný prenosový kanál $\Rightarrow$ *počiatok kryptografie s verejným kľúčom*, ale stále ešte vyžadoval postupnosť interaktívnych krokov medzi účastníkmi

# Princíp kryptografie s verejným kľúčom

**Kryptografia s verejným kľúčom:**

- je založená na asymetrickom šifrovaní - používa **dva kľúče** $\Rightarrow$ jeden kľúč sa používa na šifrovanie, druhý na dešifrovanie
- veľká **výhoda** - nevyžaduje žiadnu interakciu medzi účastníkmi pred výmenou zašifrovaného textu, resp. dát
- každý účastník vlastní dva kľúče - **súkromný kľúč** (utajuje sa) a **verejný kľúč** (môže sa zverejniť)
- **použitie dvoch kľúčov ovplyvňuje** stupeň bezpečnosti, spôsob distribúcie kľúčov a autentizáciu používateľov
- kryptografia s verejným kľúčom je univerzálna a umožňuje realizovať základné funkcie, ako sú **utajenie obsahu správy, autentizácia používateľov a autentizácia dát**

# Princíp kryptografie s verejným kľúčom

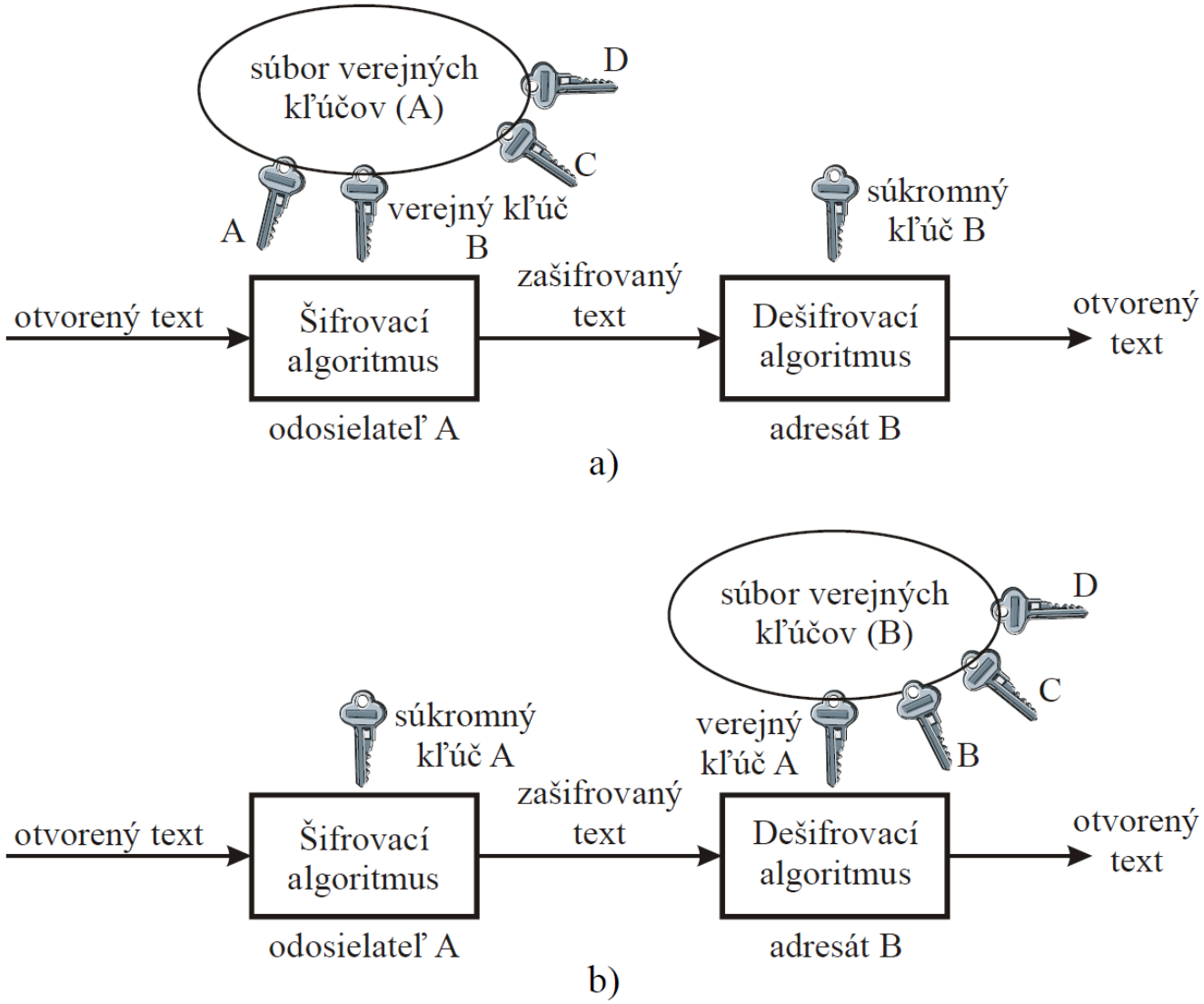
**Kryptografia s verejným kľúčom zahŕňa zložky:** 1. otvorený text $M$, 2. šifrovací algoritmus $E$, 3. súkromný kľúč $SK$, 4. verejný kľúč $VK$, 5. zašifrovaný text $C$, 6. dešifrovací algoritmus $D$

**Kryptografia s verejným kľúčom zabezpečuje funkcie:**

1. **šifrovanie** - utajenie obsahu správy, realizuje sa **verejným kľúčom** adresáta $\Rightarrow$ ak napr. odosielateľ A chce zaslať zašifrovanú správu (text) adresátovi B, na šifrovanie použije verejný kľúč B; dešifrovanie sa realizuje súkromným kľúčom B, ktorý vlastní iba adresát B
2. **autentizácia** - používateľov a dát; rieši sa inverzne $\Rightarrow$ ak otvorený text zašifruje odosielateľ A svojim **súkromným kľúčom**, dešifrovanie možno realizovať iba verejným kľúčom A, čo znamená, že správu zašifroval účastník A

# Princíp kryptografie s verejným kľúčom

**Kryptografia s verejným kľúčom**: a) šifrovanie, b) autentizácia:

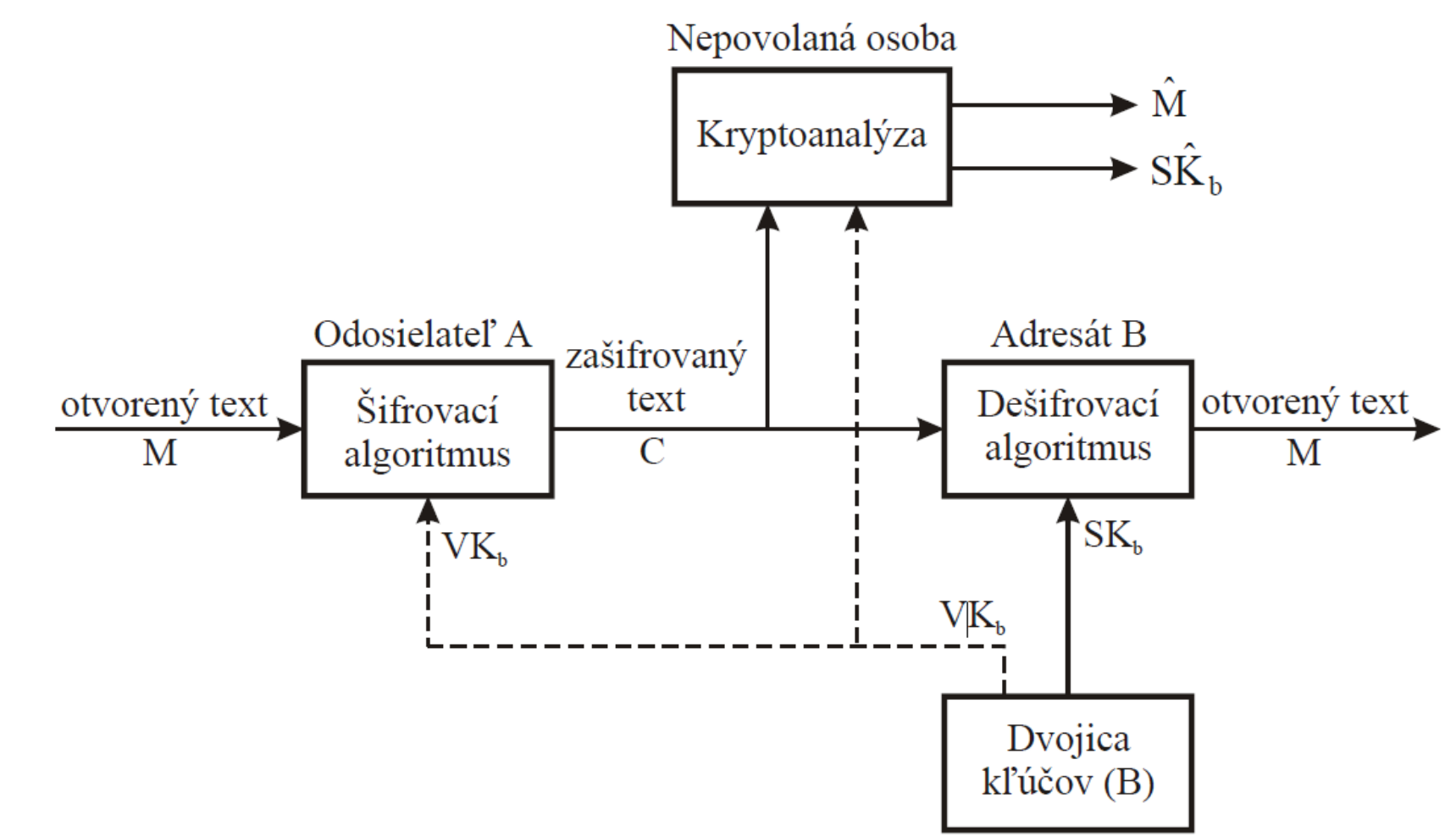


# Kryptografické systémy s verejným kľúčom

1. **Systémy zabezpečujúce utajenie:**
   - odosielateľ $A$ zašifruje otvorený text $M$ verejným kľúčom $VK_b$ adresáta $B$, ktorý je dostupný (zverejnený) $\Rightarrow$ šifrovanie možno vyjadriť v tvare: $\mathbf{C = E_{VK_b}(M)}$
   - zašifrovaný text $C$ sa prenáša k adresátovi $B$, ktorý prijatý zašifrovaný text dešifruje svojim súkromným kľúčom $SK_b$: $\mathbf{M = D_{SK_b}(C) = D_{SK_b}(E_{VK_b}(M))}$
   - nepovolaná osoba má prístup k verejnému kľúču $VK_b$ a môže získať zašifrovaný text $C$ $\Rightarrow$ **cieľom kryptoanalýzy** je odhad otvoreného textu $\hat{M}$ , resp. odhad súkromného kľúča $SK_b$
   - zároveň možno predpokladať, že nepovolaná osoba pozná aj šifrovací, resp. dešifrovací algoritmus $\Rightarrow$ **bezpečnosť systému** je založená na utajení $SK_b$ a obtiažnosti získania $SK_b$ zo známeho $VK_b$

# Kryptografické systémy s verejným kľúčom

## Systémy zabezpečujúce utajenie:



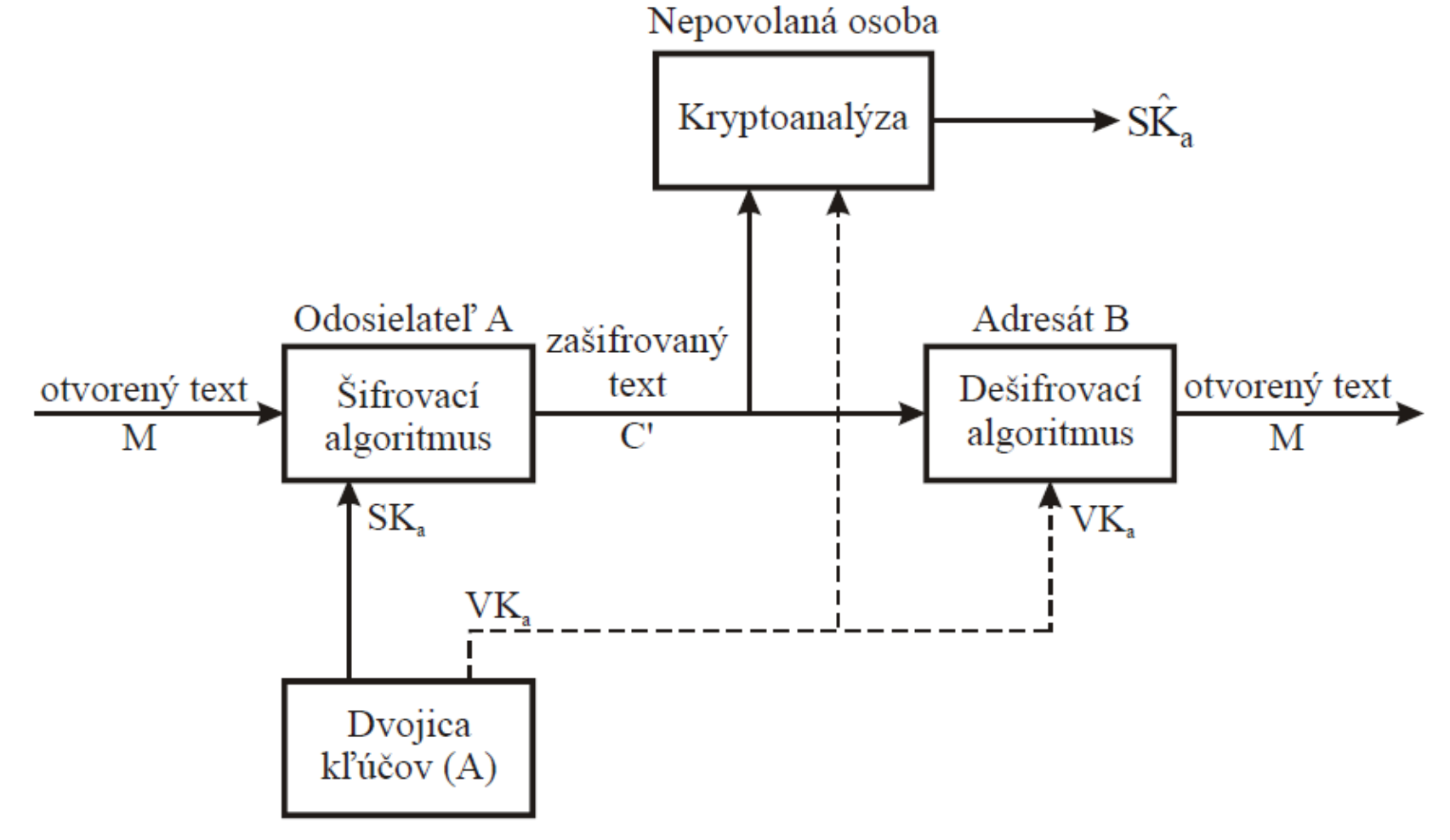
**2. Systémy zabezpečujúce autentizáciu:**

- odosielateľ zašifruje otvorený text $M$ svojím súkromným kľúčom $SK_a$, čím sa získa zašifrovaný text $C'$:
  $\mathbf{C' = E_{SK_a}(M)}$
- zašifrovaný text $C'$ sa prenáša k adresátovi $B$, ktorý prijatý zašifrovaný text dešifruje verejným kľúčom $VK_a$:
  $\mathbf{M = D_{VK_a}(C') = D_{VK_a}(E_{SK_a}(M))}$
- nepovolaná osoba, ktorá má prístup k $C'$ a k $VK_a$ sa **kryptoanalýzou** pokúša odhadovať $SK_a$
- pretože $M$ bol zašifrovaný $SK_a$ a možno ho dešifrovať iba $VK_a$, autorom správy je $A \Rightarrow$ zašifrovaný text $C'$ má v tomto prípade charakter **digitálneho podpisu**
- zároveň z toho vyplýva, že modifikácia správy bez prístupu k $SK_a$ je nemožná $\Rightarrow$ tento systém **zabezpečuje autentizáciu zdroja správy aj integritu prenášaných dát**

# Kryptografické systémy s verejným kľúčom

- uvedený prístup nezaručuje **dôvernosť správy**, pretože dešifrovanie správy $VK_a$ môže realizovať ľubovoľná osoba, ktorá vlastní $VK_a$
- nevýhodné je aj šifrovanie celej správy, najmä z hľadiska časových a pamäťových nárokov $\Rightarrow$ efektívnejší je postup, pri ktorom sa šifruje len určitý **výťah zo správy**, ktorý má podstatne menší rozsah
- tento výťah je funkciou úplného dokumentu a je zašifrovaný $SK_a$ - nazýva sa **autentifikátor** a má takú vlastnosť, že každá modifikácia pôvodného dokumentu vyvolá modifikáciu tohto identifikátora
- zašifrovaný identifikátor slúži ako digitálny podpis, ktorým sa **verifikuje pôvod a obsah** pôvodnej správy

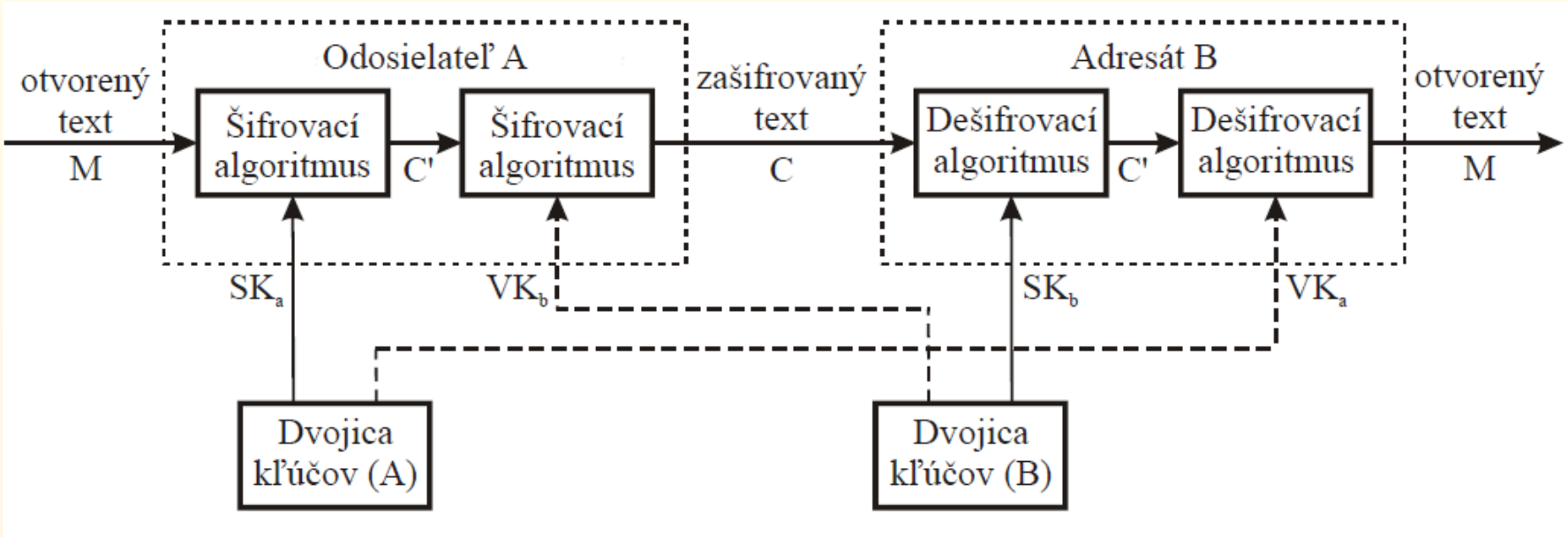
## Systémy zabezpečujúce autentizáciu:



### 3. Systémy zabezpečujúce utajenie aj autentizáciu:

- realizujú šifrovanie v dvoch krokoch: $\mathbf{C = E_{VK_b}(E_{SK_a}(M))}$
- šifrovanie otvoreného textu $SK_a$ plní funkciu digitálneho podpisu, v 2.kroku sa získaný zašifrovaný text opäť šifruje $VK_b$, čo zaručuje dôvernosť správy, pretože jej dešifrovanie je možné iba $SK_b$
- proces dešifrovania tiež vyžaduje dva kroky: $\mathbf{M = D_{VK_a}(D_{SK_b}(C))}$
- **nevýhodou** uvedeného kryptografického systému s verejným kľúčom je to, že proces šifrovania a dešifrovania je zložitejší a vyžaduje štyri kroky

**Systémy zabezpečujúce utajenie aj autentizáciu:**



# Podmienky realizovateľnosti KS s VK

**Kryptografické systémy (KS) s verejným kľúčom (VK):**

- sú založené na aplikácii **asymetrických algoritmov**, ktoré používajú dva vzájomne závislé kľúče
- ich realizácia vyžaduje formuláciu **podmienok**, ktoré musia algoritmy v týchto systémoch spĺňať

**Podmienky realizovateľnosti KS s VK:**

1. výpočtovo jednoduché **generovanie dvojice kľúčov** pre odosielateľa $A$ ($SK_a$ a $VK_a$) a pre adresáta $B$ ($SK_b$ a $VK_b$)
2. výpočtovo jednoduchá **realizácia šifrovania** správy $M$ odosielateľom $A$ pre adresáta $B$, na základe dostupnosti $VK_b$ $\Rightarrow$ jednoduché generovanie zašifrovaného textu $C = E_{VK_b}(M)$
3. výpočtovo jednoduchá **realizácia dešifrovania** prijatého zašifrovaného textu $C$ adresátovi $B$ s použitím $SK_b$ $\Rightarrow$ jednoduché získanie pôvodnej správy

$$M = D_{SK_b}(C) = D_{SK_b}(E_{VK_b}(M))$$

# Podmienky realizovateľnosti KS s VK

4. výpočtovo zložité **získanie súkromného kľúča** $SK_b$ zo známeho verejného kľúča $VK_b$ nepovolanou osobou
5. výpočtovo zložité **získanie pôvodnej správy** $M$ zo známeho zašifrovaného textu $C$ a známeho verejného kľúča $VK_b$ nepovolanou osobou
   **Dodatočná podmienka, ktorú nemusia spĺňať všetky algoritmy:**
6. funkcie šifrovania a dešifrovania sú **vzájomne zameniteľné**, t. j. môžu byť vykonané v ľubovoľnom poradí:

$$M = E_{VK_b}(D_{SK_b}(M)) = D_{VK_b}(E_{SK_b}(M))$$

$\Rightarrow$ uvedené **podmienky spĺňajú v plnom rozsahu** najmä dva algoritmy, a to RSA a algoritmy na báze eliptických kriviek

# Podmienky realizovateľnosti KS s VK

Všetky algoritmy pre KS s VK využívajú špeciálnu triedu matematických funkcií, ktoré sa označujú ako **jednocestné funkcie** $\Rightarrow$ ich **vlastnosti** možno sformulovať takto:

1. jednoduchý výpočet funkčnej hodnoty $Y = f(X)$ zo známeho argumentu $X$
2. obťažný výpočet argumentu $X$ zo známej funkčnej hodnoty $Y$, t. j. výpočet $X = f^{-1}(Y)$

Osobitnú triedu tvoria **jednocestné funkcie so skrytým vstupom**, v ktorých je výpočet inverznej funkcie podmienený znalosťou utajeného parametra $k$ $\Rightarrow$ ich **vlastnosti**:

1. jednoduchý výpočet $Y = f_k(X)$, ak $X$ a $k$ sú známe
2. jednoduchý výpočet $X = f_k^{-1}(Y)$, ak $Y$ a $k$ sú známe
3. obťažný výpočet $X = f_k^{-1}(Y)$, ak $Y$ je známe a $k$ nie je známe

# Kategorizácia KS s VK

**Z hľadiska použitých algoritmov** možno KS s VK rozdeliť do troch kategórií, a to na kryptografické systémy, ktoré realizujú:

1. **šifrovanie, resp. dešifrovanie** - na šifrovanie sa využíva verejný kľúč adresáta, dešifrovanie sa realizuje súkromným kľúčom adresáta
2. **digitálne podpisy** - šifrovanie správy súkromným kľúčom odosielateľa; šifrovanie sa aplikuje buď na celú správu alebo na výťah zo správy, t. j. malý blok dát, ktorý je funkciou celej správy
3. **výmenu kľúčov** - realizuje sa pomocou kľúča relácie, ktorý je k dispozícii obom stranám; niektoré prístupy využívajú súkromný kľúč jednej alebo oboch strán

# Algoritmy KS s VK

- **autormi myšlienky** kryptografie s VK sú Whitfield Diffie a Martin Hellman, pričom nezávisle na nich s uvedenou koncepciou prišiel aj Ralph Merkle
- **princíp** kryptografie s VK, ktorá používa pár vzájomne závislých kľúčov, bol **zverejnený** v roku **1977**
- od tohto roku bolo **navrhnutých veľa** KS s VK, ale mnohé z nich nie sú bezpečné
- **bezpečnosť** algoritmov s VK je založená na obťažnosti odvodenia SK z VK
- ak aj niektoré z algoritmov možno považovať za bezpečné, z hľadiska **praktickej implementácie** používajú príliš dlhý kľúč a generujú zašifrovaný text s oveľa väčšou dĺžkou ako je dĺžka otvoreného textu

# Algoritmy KS s VK

- algoritmy s VK, ktoré sa považujú za bezpečné, **sa líšia rozsahom zabezpečenia základných funkcií**, akými sú šifrovanie, digitálne podpisy a distribúcia kľúčov
- niektoré algoritmy s VK sú vhodné na realizáciu všetkých 3 funkcií, iné algoritmy sú schopné zabezpečiť len niektoré z nich
- medzi **univerzálne algoritmy s verejným kľúčom** patria algoritmy RSA, El Gamal a algoritmy na báze eliptických kriviek
- algoritmus Diffie – Hellman je **použiteľný len na výmenu kľúčov**

| Typ algoritmu | Šifrovanie/Dešifrovanie | Digitálny podpis | Výmena kľúčov |
|---|---|---|---|
| Diffie – Hellman | Nie | Nie | Áno |
| El Gamal | Áno | Áno | Áno |
| RSA | Áno | Áno | Áno |
| Eliptické krivky | Áno | Áno | Áno |

Ďakujem za pozornosť