Kódování a šifrování: Symetrická a asymetrická šifra, digitální podpis, certifikát

Informatika, ZŠ Broumovská

Petr Socha, 2022
petr.socha@zsbroumovska.cz

Druhy šifer

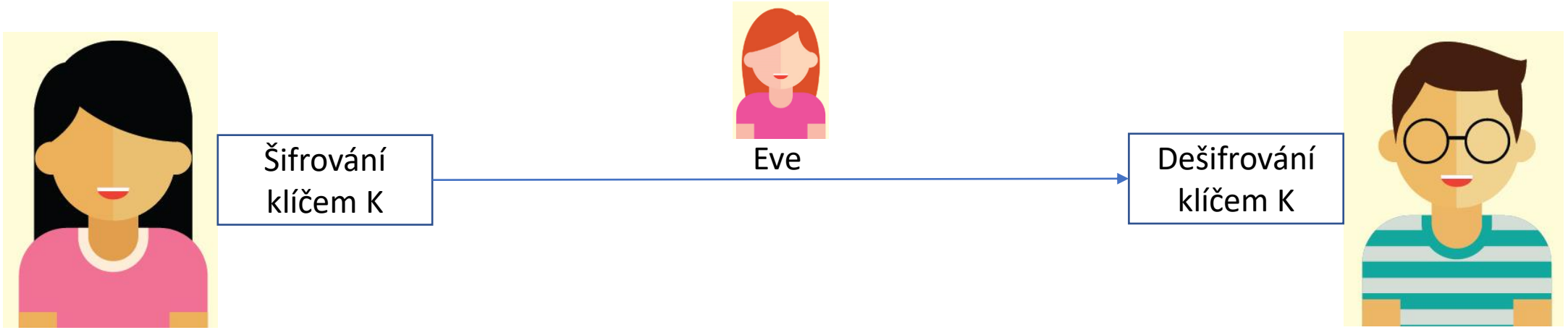
- Dnešní šifry dělíme do dvou skupin:
  - Symetrická šifra
  - Asymetrická šifra

Symetrická šifra

- Do skupiny symetrických šifer patří všechny, které jsme si ukázali: Caesarova, Vigenèrova i Vernamova šifra
- Symetrická šifra používá **1 klíč**
  - Jedním klíčem šifrujeme
  - Tím stejným klíčem zase dešifrujeme

Použití symetrické šifry

- Představíme si situaci, kdy Alice chce poslat zašifrovanou zprávu Bobovi



- Alice zprávu zašifruje klíčem K a odešle, Bob zprávu po přijetí klíčem K zase dešifruje a přečte
- Pokud někdo zprávu zachytí (Eve), zprávu nedokáže bez klíče přečíst

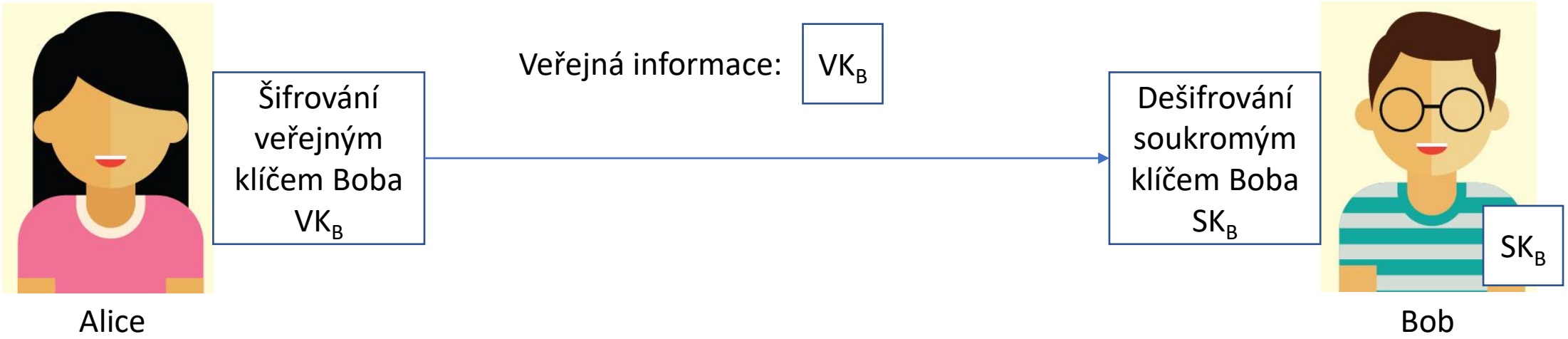
Problém symetrické šifry

- Problém scénáře, na minulém slajdu, je v klíči K
- Alice a Bob musí oba znát klíč K, aby spolu mohli komunikovat
- To znamená, že si Alice a Bob musí nejprve bezpečnou cestou klíč K vyměnit, než si začnou posílat šifrované zprávy
- Představte si, že se přihlašujete do svojí emailové schránky a chcete, aby heslo putovalo po internetu šifrovaně a nemohl ho nikdo (ani Eve) odposlechnout… museli byste si s provozovatelem svého emailu nejprve bezpečně vyměnit šifrovací klíče (což asi neděláte)
- Přesto komunikujete šifrovaně… tenhle problém totiž spolehlivě řeší asymetrická šifra…

Asymetrická šifra

- Na rozdíl od symetrické šifry, ta asymetrická používá vždy **2 klíče**
  - Jeden klíč se používá k šifrování
  - Druhý klíč se používá k dešifrování
- Když Bob chce, aby s ním ostatní mohli komunikovat šifrovaně, potřebuje k tomu dva klíče
  - První klíč, určený k šifrování, zveřejní všem (dá na internet, na nástěnku,…)
    - Budeme ho nazývat **Veřejný klíč** Boba, a zkráceně značit $\mathbf{VK_B}$
  - Druhý klíč, určený k dešifrování, si Bob pečlivě uschová sám pro sebe
    - Budeme ho nazývat **Soukromý klíč** Boba, a zkráceně značit $\mathbf{SK_B}$
- Text který zašifrujeme Veřejným klíčem, jde dešifrovat jen a pouze Soukromým klíčem; klíče jsou různé a z prvního nejde poznat jak vypadá ten druhý

Použití asymetrické šifry



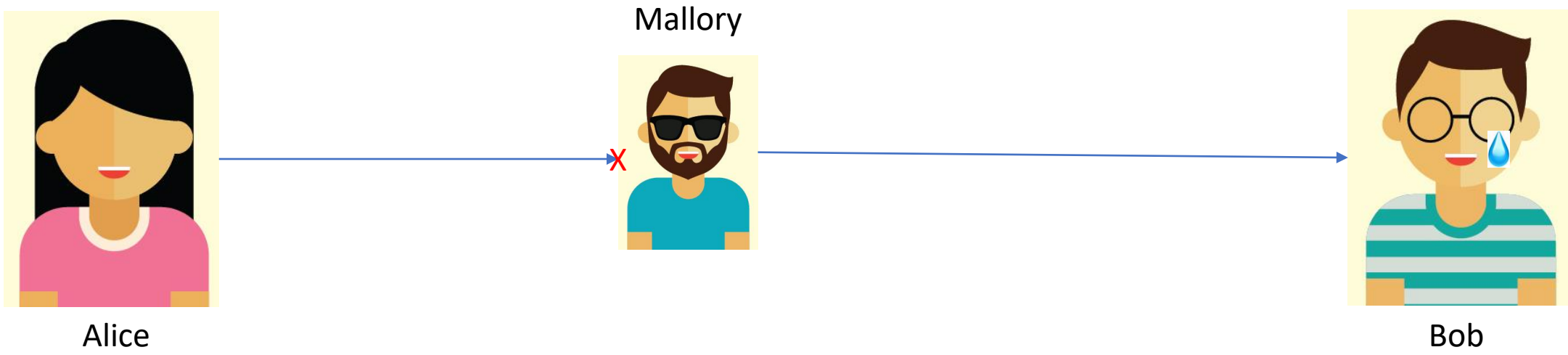
- Když chce Alice poslat Bobovi zprávu, najde si na Internetu jeho veřejný klíč VK_B, zašifruje s ním zprávu a pošle jí Bobovi
- Zprávu jde dešifrovat pouze Bobovým soukromým klíčem SK_B, který má Bob bezpečně schovaný u sebe
- Výhoda: **Alice a Bob si nemusí předat společný klíč K předem!**
- Aby mohla i Alice přijímat šifrované zprávy, potřebuje také svojí dvojici klíčů VK_A a SK_A… Bob svojí odpověď zašifruje jejím veřejným klíčem, Alice jí pak dešifruje svým soukromým klíčem

Digitální podpis

- Dvojice klíčů funguje i opačně: co Alice zašifruje svým soukromým klíčem, to jde dešifrovat jen jejím veřejným klíčem
- Toho využívá **digitální podpis:** cílem digitálního podpisu je zaručit, že autorem je skutečně ten, kdo se za něj vydává
  - Podobně jako u toho klasického podpisu… akorát ten digitální jde mnohem hůř zfalšovat
- Digitální podpis dnes použijete minimálně třeba při komunikaci se státní správou, s úřady, ale musí ho ze zákona přijmout namísto klasického třeba i škola…
- Představíme si jednoduchý scénář, kdy digitální podpis potřebujeme…

Na zprávu po cestě číhá útočník…

- Bob dluží Alici peníze, a Alice mu tedy posílá fakturu s číslem účtu

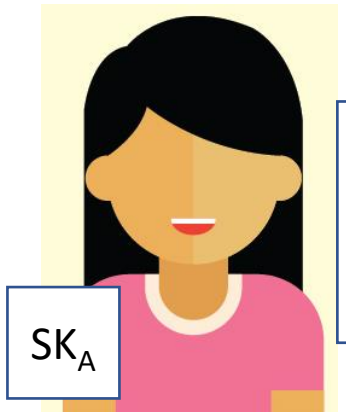


- Fakturu ale po cestě zachytí útočník Mallory, a změní na faktuře číslo účtu na svoje vlastní… Bob to nemá jak poznat, takže peníze místo Alici pošle Mallorymu (tohle se opravdu dnes stává, i u nás!)

Jak pomůže digitální podpis?

- Kdyby Alice připojila k faktuře svůj digitální podpis, Bob by ho mohl zkontrolovat a tím si ověřit, že zprávu opravdu poslala Alice (a ne někdo jiný, jako Mallory)
- Alice k tomu použije asymetrickou šifru
- Fakturu zašifruje svým Soukromým klíčem SK_A
- Každý, kdo její fakturu obdrží, ji dešifruje jejím veřejným klíčem VK_A
- Každý má potom jistotu, že má původní fakturu skutečně od Alice, protože jenom veřejný klíč Alice (VK_A) dokáže dešifrovat fakturu, kterou Alice zašifrovala svým soukromým klíčem (SK_A)
- Mallory nedokáže pozměnit číslo účtu a vydávat se za Alici, pokud nezná její soukromý klíč (ten si Alice dobře hlídá)

Použití digitálního podpisu



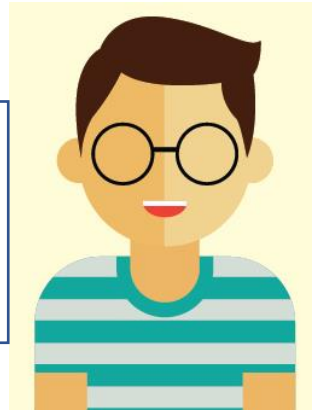
SK_A

Alice

Šifrování/podepsání soukromým klíčem Alice SK_A

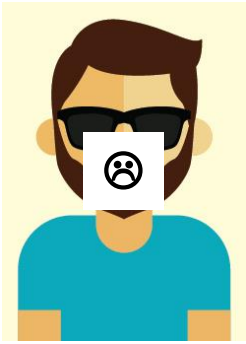
Veřejná informace: VK_A

Dešifrování/ověření podpisu veřejným klíčem Alice VK_A



Bob

- Když Bob obdrží od Alice zprávu, která je zašifrovaná/podepsaná jejím soukromým klíčem, tak podpis dešifruje/ověří jejím veřejným klíčem
- Pokud se to podaří, má Bob jistotu, že zpráva přišla opravdu od Alice
- Mallory má smůlu: kdyby zprávu pozměnil, neuměl by jí zašifrovat tak, aby vypadala jako od Alice



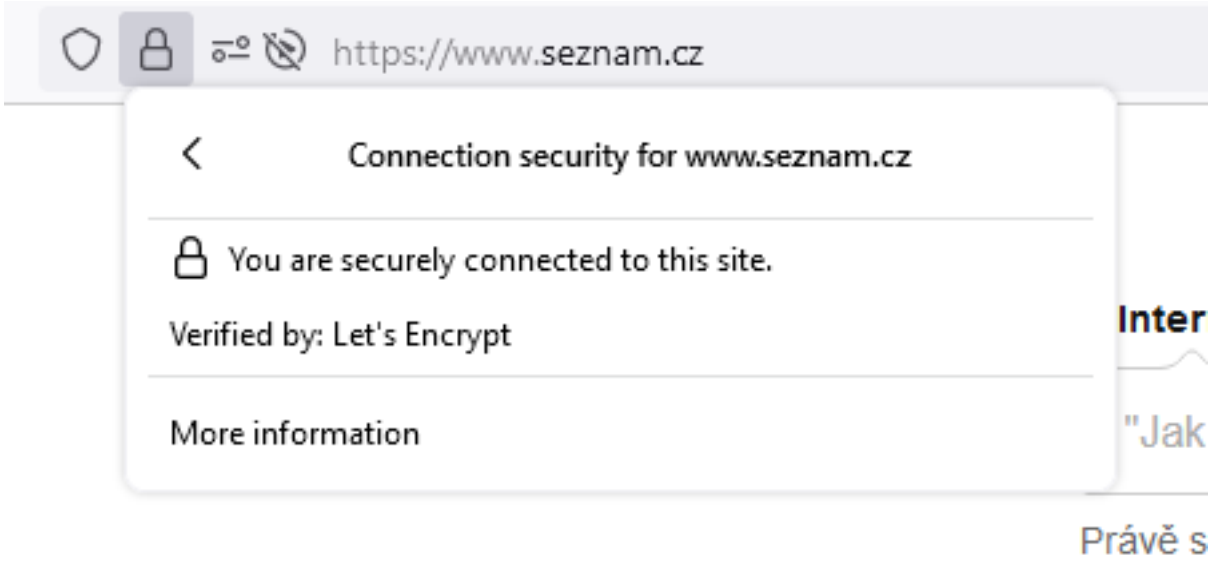
Ale Mallory na to může ještě vyzrát…

- Pokud se Mallorymu podaří přesvědčit Boba, že jeho vlastní veřejný klíč ve skutečnosti patří Alici, povede se mu podstrčit i svoje číslo účtu a Bob nic nepozná
- Jak má Bob jistotu, že veřejný klíč Alice, který našel veřejně na internetu, je skutečně její? Že to není ve skutečnosti Malloryho podstrčený klíč?

Řešením je certifikát

- V každém počítači/mobilu/… máme už od výrobce sadu veřejných klíčů, které patří velkým důvěryhodným firmám – nemusíme je nikde shánět, máme je od začátku a věříme jim
- Alice zaplatí velké firmě za to, že ta podepíše její veřejný klíč
- Bob si z Internetu stáhne veřejný klíč Alice, a pomocí veřejného klíče velké firmy si ověří, že skutečně patří Alici
  - Velká firma by Mallorymu nepodepsala klíč, u kterého je napsáno, že patří Alici
- Veřejný klíč, podepsaný velkou firmou (tedy ten, jehož pravost umíme ověřit) se nazývá **certifikát**

Ukázka certifikátu



- Když navštívíme web Seznam.cz, tak máme vedle adresy zámeček: to znamená, že komunikace je šifrovaná
- Když si zámeček rozklikneme, uvidíme, že pravost certifikátu pro Seznam.cz ověřila velká společnost Let’s Encrypt
- Veřejný klíč společnosti Let’s Encrypt máme všichni v počítači
- Prohlížeč nejdřív dešifruje klíč Seznamu klíčem Let’s Encrypt, tím ověří jeho pravost… až pak začne používat veřejný klíč Seznamu k (de)šifrování

Shrnutí

- Asymetrická šifra (asymetrická kryptografie) používá 2 klíče
- Co se zašifruje jedním klíčem, to se musí dešifrovat tím druhým
- Typicky jeden klíč zveřejníme (veřejný klíč) a druhý si necháme pro sebe (soukromý klíč)
- Díky tomu nám může kdokoliv poslat šifrovanou zprávu, kterou jen my dokážeme rozšifrovat
- Asymetrická šifra se používá také pro digitální podpis
- Certifikát zajišťuje, že ten, kdo používá náš veřejný klíč, má jistotu, že klíč je skutečně náš (že není falešný, nepatří útočníkovi)