evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

PSK2-16

Název školy:	Vyšší odborná škola a Střední průmyslová škola, Božetěchova 3
Autor:	Ing. Marek Nožka
Anotace:	Jak funguje asymetrická šifra a elektronický podpis
Vzdělávací oblast:	Informační a komunikační technologie
Předmět:	Počítačové sítě a komunikační technika (PSK)
Tematická oblast:	Vrstvy protokolu TCP/IP
Výsledky vzdělávání:	Žák popíše popíše základní rozdíl a funkci symetrické a asymetrické šifry
Klíčová slova:	symetrická a asymetrická šifra, Alice, Bob
Druh učebního materiálu:	Online vzdělávací materiál
Typ vzdělávání:	Střední vzdělávání, 3. ročník, technické lyceum
Ověřeno:	VOŠ a SPŠE Olomouc; Třída: 3L
Zdroj:	Vlastní poznámky, Wikipedia, Wikimedia Commons

Šifrování a elektronický podpis I

Šifrování dat je proces, kterým se nezabezpečená data převádí za pomoci kryptografie na data šifrovaná. Šifrovaná data jsou čitelná pouze pro majitele dešifrovacího klíče.

Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat i při jejich přenosu včetně telekomunikace.

Kryptografii můžeme rozdělit do dvou hlavních skupin:

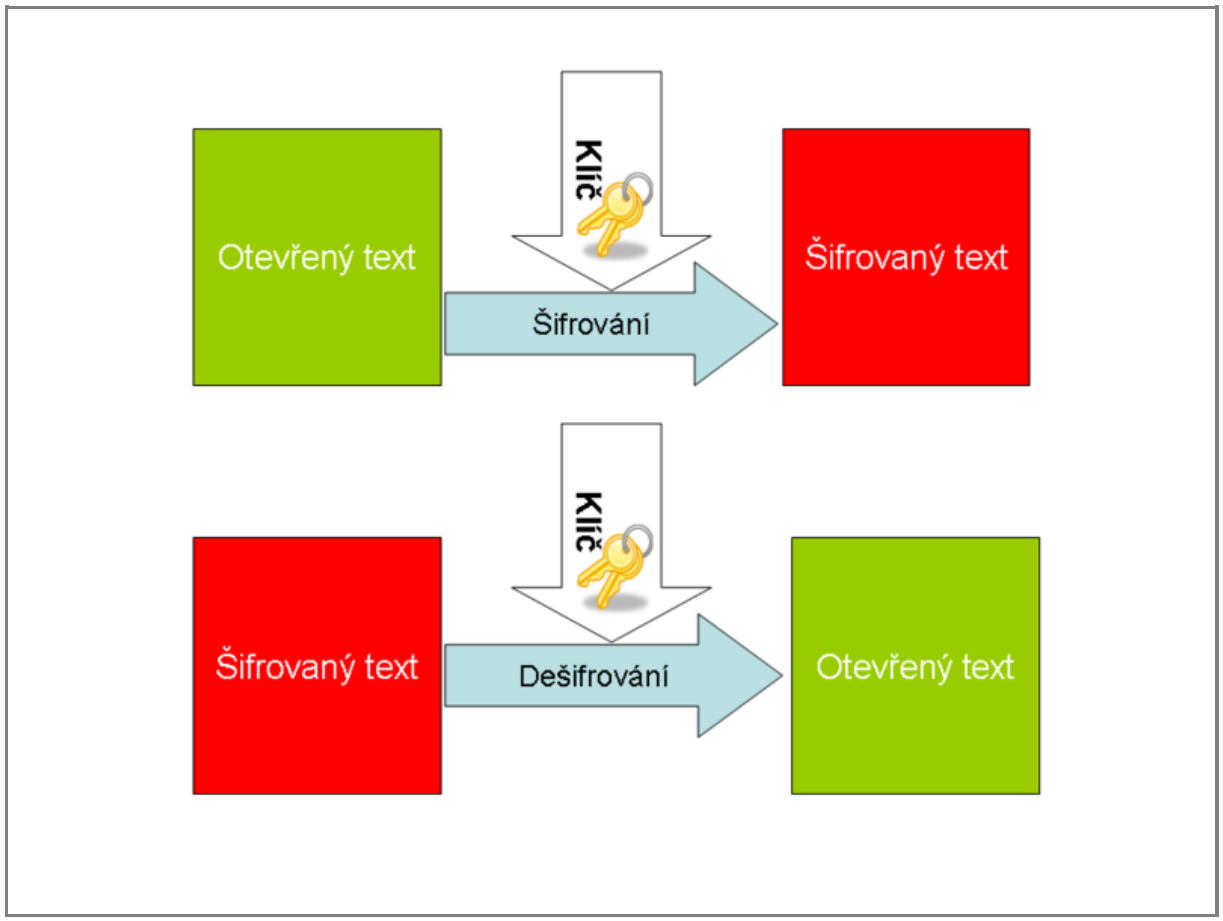
- Symetrická kryptografie
- Asymetrická kryptografie

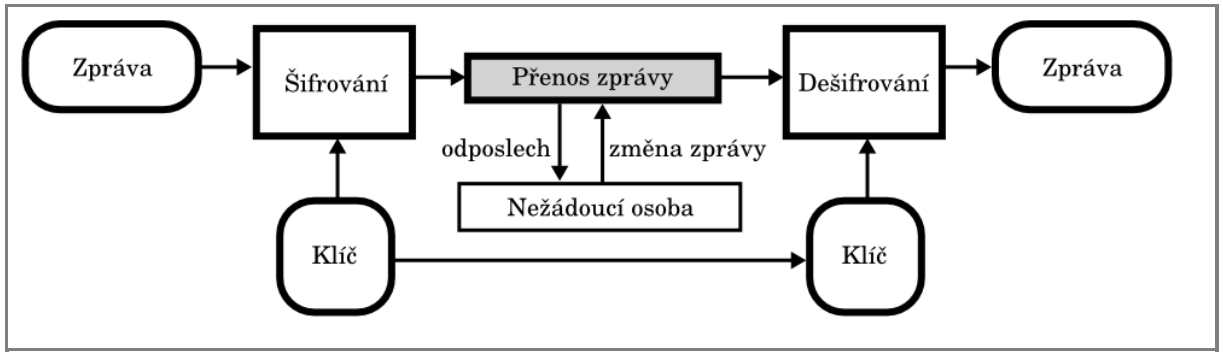
Obě skupiny používají při šifrování tzv. klíč. Jedná se vždy o velké náhodné číslo. Nedostatečné přítomnost náhody při generování klíče může vést až k prolomení šifry. Proto je nezbytné, aby pro jejich generování byl použit zdroj skutečně náhodných čísel. Tímto zdrojem může v praxi být například anténa zachytávající atmosferický šum

připojená na A/D převodník nebo snímání náhodných pohybů myši uživatele kryptografického programu.

Symetrická kryptografie

Symetrická šifra, někdy též nazývaná konvenční, je šifrovací algoritmus, který používá k šifrování i dešifrování jediný klíč. Klíč je stejný na obou dvou stranách komunikačního kanálu.





Podstatnou **výhodou** symetrických šifer je jejich nízká výpočetní náročnost a z toho vyplývající vysoká rychlost zpracování. Asymetrické algoritmy pro šifrování s veřejným klíčem můžou být i stotisíckrát pomalejší.

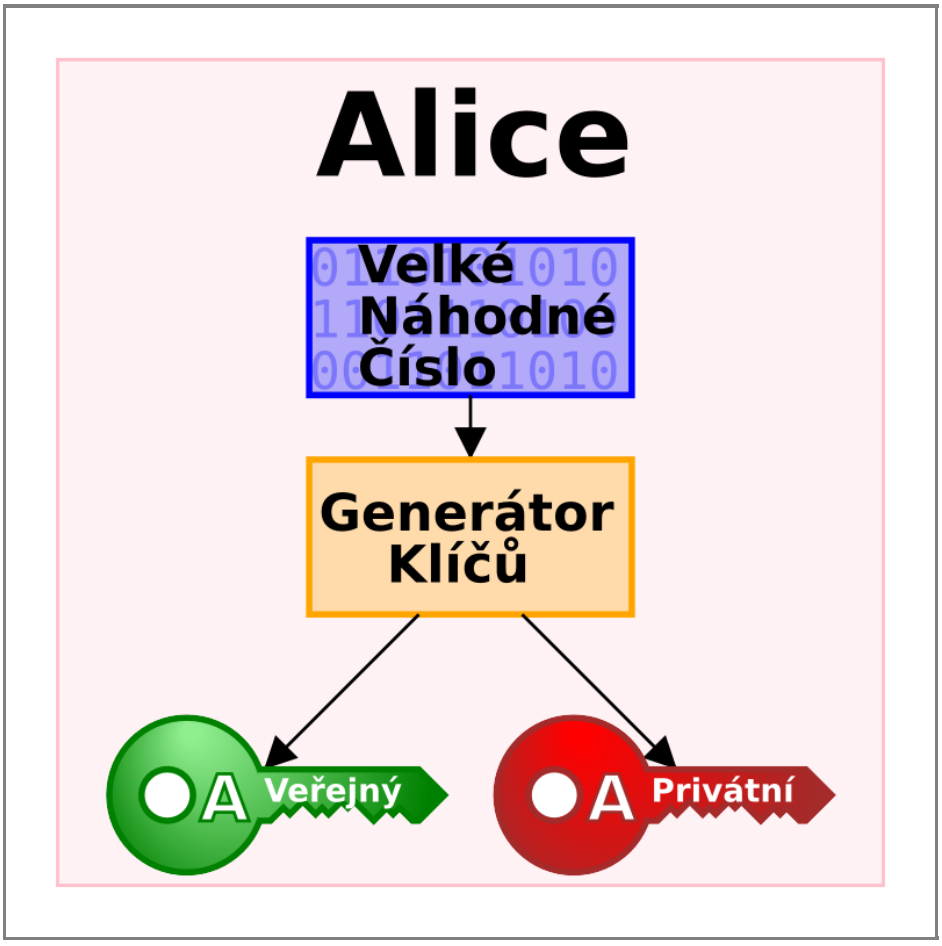
Na druhou stranu velkou **nevýhodou** je nutnost sdílení tajného klíče, takže se odesilatel a příjemce tajné zprávy musí předem domluvit na tajném klíči. To může být v mnoha případech velice obtížené nebo i nemožné.

Asymetrická kryptografie

Základem pro asymetrickou Kryptografii je dvojice komplementárně spojených klíčů, která se označuje jako Keypair. Jeden klíč je označován jako veřejný -- *public key*, druhý jako soukromý -- *privat key*. Jak názvy napovídají veřejný klíč je určen k distribuci dalším uživatelům kryptografického systému. Oproti tomu soukromý klíč je tajný, jeho majitel ho musí pečlivě střežit a jeho odhalení by vedlo k prolomení šifry.

Platí následující: **To co jeden z klíčů zašifruje to rozšifruje pouze ten druhý**.

- To co zašifruje veřejný klíč, rozšifruje pouze soukromý klíč. Toho se využívá při šifrování zpráv.
- To co zašifruje soukromý klíč rozšifruje pouze veřejný klíč. Toho se využívá u elektronického podpisu.



Názvosloví

Většinou se nepoužívá pojem veřejný a soukromý klíč, ale používá se dvojice pojmů **klíč** a **certifikát**.

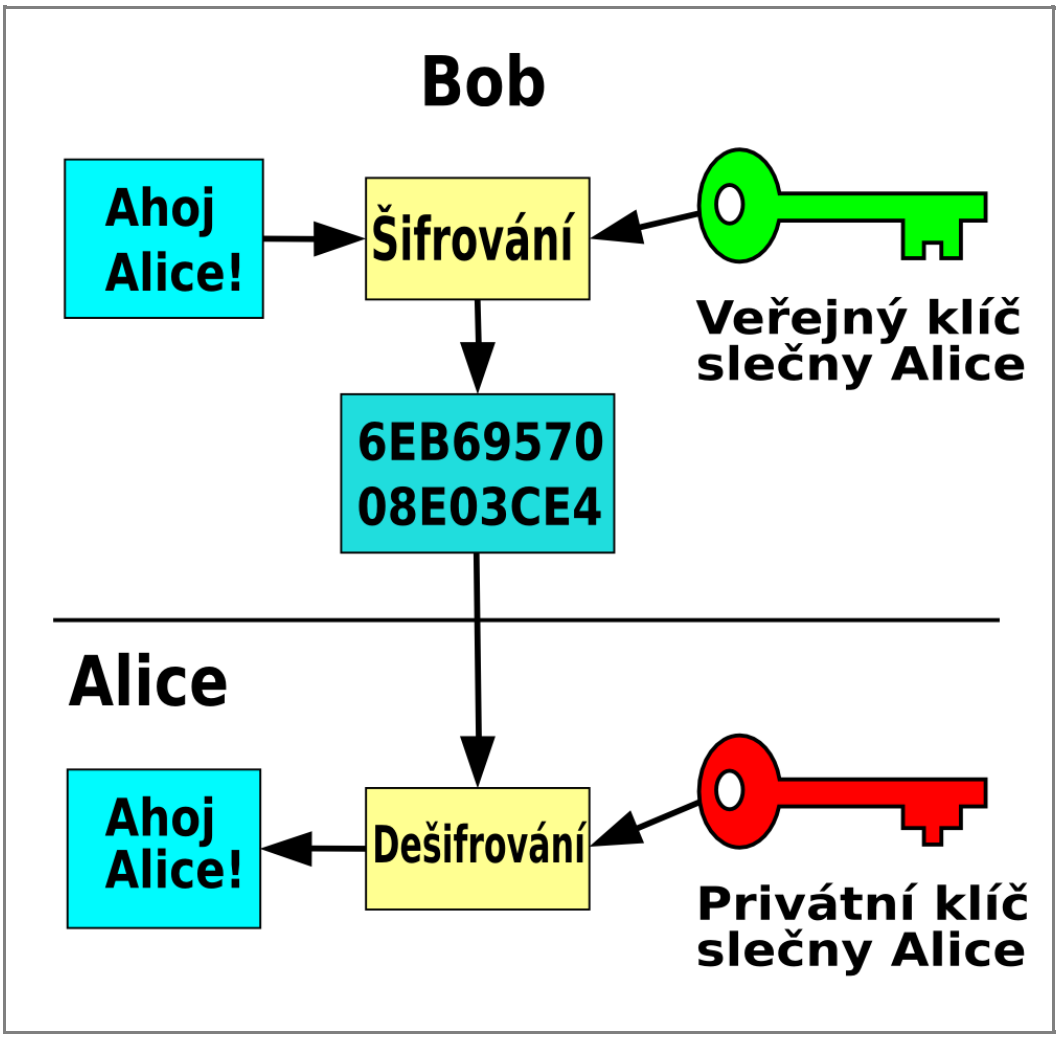
- **klíč = soukromý klíč**
- **certifikát = veřejný klíč**

Šifrování zpráv

Šifrování pomocí veřejného klíče neboli asymetrická kryptografie

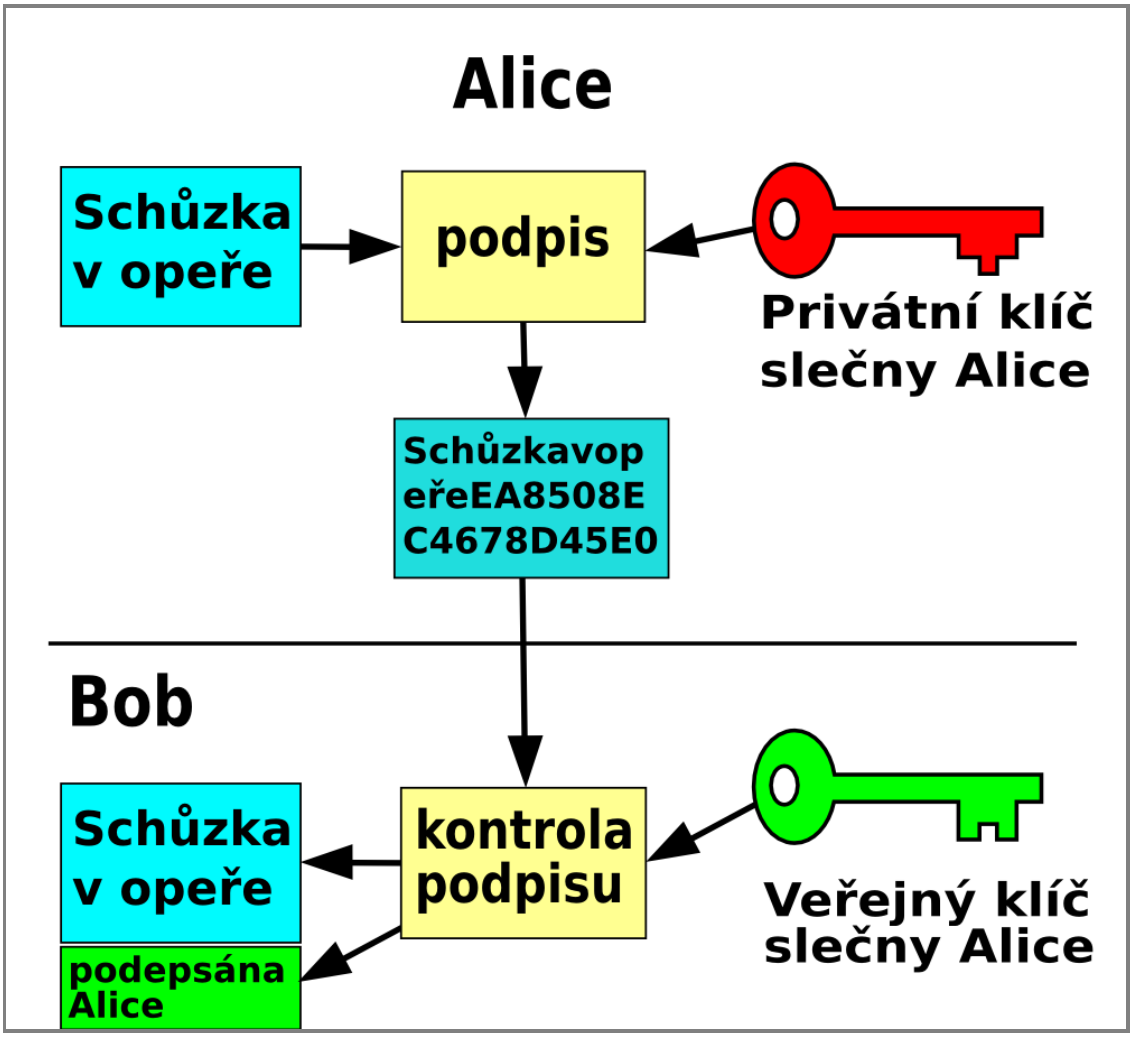
bývá někdy přirovnávána k poštovní schránce. Kdokoli může dopis hodit do schránky, ale existuje pouze jedna osoba, která má od schránky klíč, aby poštu vytáhla a přečetla.

Komunikaci ukážeme na příkladu Boba a Alice. Pokud Bob posílá zprávu Alici, zašifruje ji Aliciným veřejným klíčem. Veřejný klíč je veřejně k dispozici, proto nemá Bob problém ho získat. Tuto zprávu může dešifrovat pouze Alice, protože jen ona vlastní příslušný soukromý klíč, kterým lze zprávu dešifrovat.



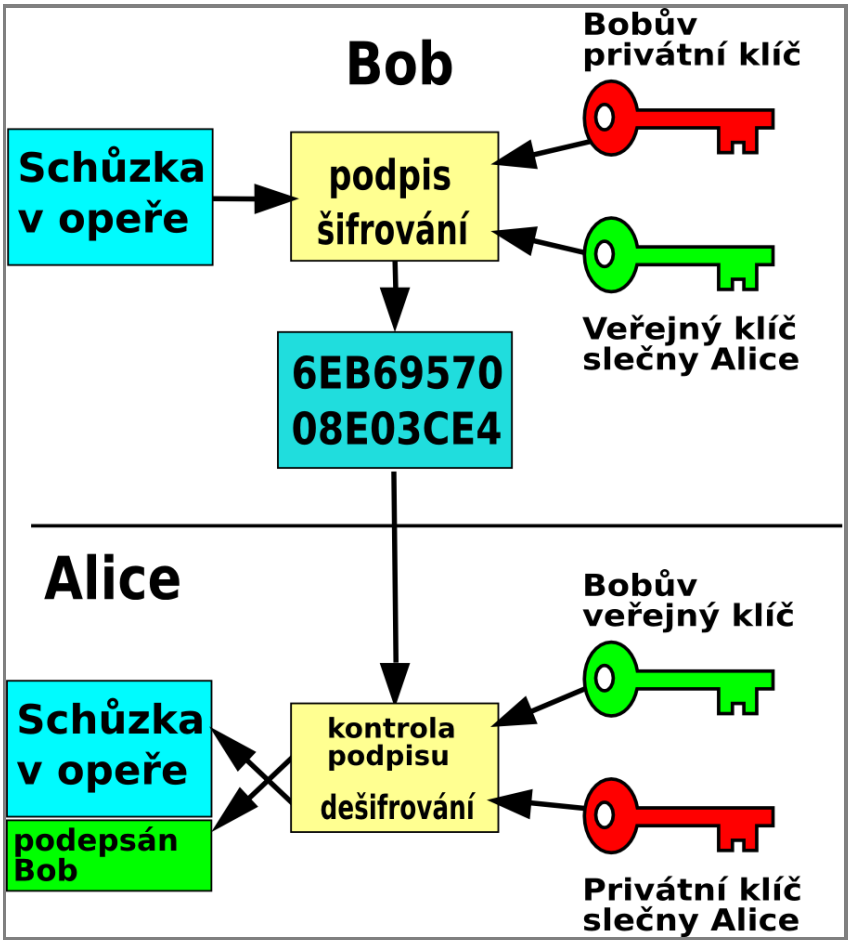
Elektronický podpis

U elektronického podpisu je problém opačný: Požadujeme, aby Alice svým podpisem potvrdila, že tuto zprávu psala opravdu ona -- to udělá svým soukromým klíčem. Ale každý, kdo má Alicin veřejný klíč může pravost podpisu ověřit.



Šifrování a podpis

Oba úkony (šifrování a podepisování) lze spojit do jednoho systému:


Bob
Bobův
privátní klíč
Schůzka
v opeře
podpis
šifrování
Veřejný klíč
slečny Alice
6EB69570
08E03CE4
Alice
Bobův
veřejný klíč
Schůzka
v opeře
kontrola
podpisu
dešifrování
podepsán
Bob
Privátní klíč
slečny Alice