# 20. Kryptografie

## Teoretická část

**Vysvětlete funkci a účel kryptografie. Popište druhy moderní elektronické kryptografie. Popište historii kryptografie.**

## Praktická část

1. **Popište symetrické a asymetrické způsoby kryptografie.**
2. **Popište, kde se dnes moderní kryptografie používá?**
3. **Popište proudové a blokové šifry symetrické kryptografie.**
4. **Vysvětlete funkci a druhy certifikátů a certifikačních autorit.**

## Doplňující otázky

1. **Popište použití RSA šifry** ve vícenásobném šifrování.
2. **Popište funkci otisku hash.**
3. **Popište funkci digitálního podpisu.**

# Kryptografie

Věda zabývající se šifrováním, tedy utajováním informací, se nazývá kryptografie. Naproti tomu věda, která se zabývá luštěním šifer je kryptoanalýza. Nadřazeným pojmem pro oba dva obory je kryptologie. Šifrujeme tak, aby se útočníkovi nevyplatilo šifru prolomit

# Druhy kryptování

### První rozdělení

jednosměrné - z výsledku nelze získat originál, k ověřování nebo porovnávání (hash, dig. podpis)   
obousměrné - při znalosti správného klíče jsme schopni dešifrovat výsledek a získat tak opět originál   
  
Druhé rozdělení   
s privátním klíčem (symetrické)   
 **bloková** - zpracovávají více znaků (blok) otevřeného textu najednou   
 **proudová** - pokud chceme zašifrovat jen několik bitů otevřeného textu, nebo v případech, kdy jsou data získávána jako proud bitů a je potřeba je okamžitě šifrovat (RC4)   
s veřejným klíčem (asymetrické)

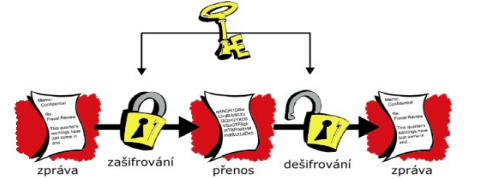
## Historie Kryptografie

První zmínky o [kryptografii](https://cs.wikipedia.org/wiki/Kryptografie) můžeme nalézt před několika tisíci lety. Celé období můžeme rozdělit do dvou částí, tou první je [klasická kryptografie](https://cs.wikipedia.org/w/index.php?title=Klasick%C3%A1_kryptografie&action=edit&redlink=1), která přibližně trvala až do první poloviny [20. století](https://cs.wikipedia.org/wiki/20._stolet%C3%AD). Tato epocha se vyznačovala tím, že k šifrování stačila tužka a papír. Během první poloviny [20. století](https://cs.wikipedia.org/wiki/20._stolet%C3%AD) ale začaly vznikat různé sofistikované přístroje, které umožňovaly složitější postup při šifrování, například [Enigma](https://cs.wikipedia.org/wiki/Enigma). Tím přibližně začala druhá část, kterou nazýváme [moderní kryptografie](https://cs.wikipedia.org/w/index.php?title=Modern%C3%AD_kryptografie&action=edit&redlink=1). V dnešní době se k šifrování z pravidla nepoužívají žádné zvlášť vytvářené přístroje, ale klasické [počítače](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D).

# Popište symetrické a asymetrické způsoby kryptografie.

### Symetrické šifrování

Symetrické (nebo konvenční) šifrování je metoda, při které je text zašifrován s pomocí jistého klíče a může být obnoven jen se znalostí tohoto klíče, což je zároveň jeho největší slabina. Symetrické kódy mají jako hlavní výhodu rychlost algoritmu. Na druhou stranu je nutné, aby se příjemce i odesílatel dohodli na jednom klíči, který si musí nějakým bezpečným způsobem vyměnit a který budou znát pouze oni dva. Problémem je tedy distribuce klíče - jak dostat klíč k příjemci aniž by se ho chopil někdo nepovolaný? Samotné symetrické šifrování nemůže nikdy problém předání klíče vyřešit.



Kromě problému distribuce klíče má tento typ šifrování další nevýhodu: pokud je účastníků komunikace víc. Pokud chceme mít pro každou dvojici komunikujících stran jiný klíč, potřebujeme pro n účastníků n(n-1)/2 klíčů (jestliže je počet komunikujících malý, příliš to nevadí). Symetrické šifrování je mnohem jednodušší než asymetrické šifrování. Jednak nepotřebuje tak výkonné počítače, jednak je jednodušší jeho princip. Vzniklo mnohem dříve.

### Asymetrické šifrování

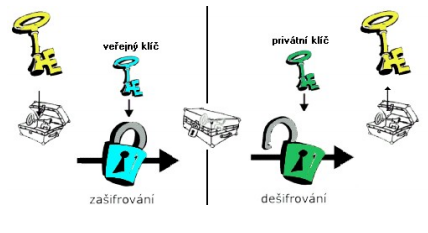
Asymetrické šifrování neboli kryptografie veřejného klíče je metoda vyvinutá Whitfieldem Diffiem a Martinem Hellmanem v roce 1975. Každý účastník komunikace má dva klíče. První z nich je veřejný (přístupný všem) a druhý je privátní (soukromý). Cokoli zašifrováno jedním klíčem, lze dešifrovat pouze druhým klíčem a naopak. Velkou výhodou tohoto přístupu je, že jeden z klíčů můžeme dát k dipozici komukoliv (tedy zveřejnit ho). Kdokoli nám pak chce napsat zprávu, použije k jejímu zašifrování tento veřejný klíč. Ani on sám, ani žádný jiný vlastník našeho veřejného klíče ji nebude schopen dešifrovat. Toho bude schopen pouze držitel druhého páru - privátního klíče, jímž bychom měli být pouze my. Chceme-li poté adresátovi poslat odpověď, nemůžeme ji zašifrovat svým privátním klíčem, neboť by ji byl schopen dešifrovat kdokoli, ale musíme použít veřejný klíč adresáta. Hlavní výhodou asymetrického šifrování je, že soukromé klíče jsou pouze u jejich majitelů a vně se pohybují pouze veřejné klíče. Asymetrické šifrování má jednu velkou nevýhodu - je velmi náročné na matematické operace, tedy i na výkon počítače.



Odesilatel tedy zašifruje zprávu veřejným klíčem adresáta. Ten přijme zašifrovanou zprávu a dešifruje ji svým privátním klíčem. Protože je jediný, kdo má tento privátní klíč, zprávu nemůže nikdo cizí přečíst. (Při použití jiného klíče, který nepatří ke klíči, kterým se šifrovalo, dostaneme samozřejmě nesmysl). Při komunikaci více účastníků je potřeba celkem 2n klíčů, tedy počet přímo úměrný počtu účastníků n.

### Hybridní šifrování

Hybridní šifrování je kombinací obou výše zmíněných. Pomalé asymetrické algoritmy se použijí k výměně symetrického klíče, který slouží ke kódování další komunikace pomocí symetrických šifer. V praxi se proto používá kombinace symetrického a asymetrického šifrování. Tomuto způsobu se říká „hybridní šifrování“. Využijeme výhod obou: rychlost symetrického šifrování a „použitelnost" asymetrického šifrování.



Odesilatel zvolí symetrický klíč, který zašifruje veřejným klíčem adresáta a pošle mu ho. Adresát tedy dostane asymetricky zašifrovaný symetrický klíč, který dešifruje svým privátním klíčem. Tím zaniká problém distribuce klíče při symetrickém šifrování a zároveň se celý proces zrychlí. (Asymetrické šifrování je pro dlouhé zprávy pomalé).

# Popište, kde se dnes moderní kryptografie používá?

Při posílání zpráv, ke kterém by neměl mít jen tak někdo přístup.

U webových stránek při přihlašování.

U bankovních převodů a přihlašování.

U VPN.

U utajování dat na HDD.

# Vysvětlete funkci a druhy certifikátů a certifikačních autorit.

Digitální certifikát je v [asymetrické kryptografii](https://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie) [digitálně podepsaný](https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis) veřejný [šifrovací klíč](https://cs.wikipedia.org/wiki/%C5%A0ifrovac%C3%AD_kl%C3%AD%C4%8D), který vydává [certifikační autorita](https://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita). Obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu (tvůrci digitálního podpisu, tj. certifikační autoritě). Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení ([HTTPS](https://cs.wikipedia.org/wiki/HTTPS), [VPN](https://cs.wikipedia.org/wiki/Virtu%C3%A1ln%C3%AD_priv%C3%A1tn%C3%AD_s%C3%AD%C5%A5) atp.). Na základě principu [přenosu důvěry](https://cs.wikipedia.org/w/index.php?title=P%C5%99enos_d%C5%AFv%C4%9Bry&action=edit&redlink=1) je možné důvěřovat neznámým certifikátům, které jsou podepsány důvěryhodnou certifikační autoritou.

**Certifikační autorita** (zkratka CA) je v [asymetrické kryptografii](https://cs.wikipedia.org/wiki/Asymetrick%C3%A1_kryptografie) subjekt, který vydává [digitální certifikáty](https://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t).

## Self-signed certifikát

Při vytvoření páru šifrovacích klíčů je možné veřejný klíč obratem podepsat odpovídajícím privátním klíčem. Vznikne tak Self-signed certifikát (certifikát podepsaný sám sebou). V takovém případě není možné využít princip přenosu důvěry a je nutné certifikát ověřit jiným způsobem (např. telefonicky podle jeho otisku). Self-signed certifikáty jsou využívány v uzavřeném prostředí (např. jedna firma) nebo pro testování.

## Kvalifikovaný certifikát

V České republice je zákonem definován tzv. kvalifikovaný certifikát, který může vydat pouze akreditovaná kvalifikovaná certifikační autorita řídící se Zákonem o elektronickém podpisu a je také standardizován v rámci Evropské unie. Kvalifikovanému certifikátu se v České republice často říká elektronický podpis. To proto, že nahrazuje klasický ověřený podpis a jednoznačně tak prokazuje totožnost dané osoby. Je určen primárně k identifikaci uživatele a je nutné chápat jej jako podpis, tj. projev vůle vztahující se ke konkrétním datům.

Jde o standardní digitální certifikát, který je však výše zmíněným zákonem uznáván v rámci komunikace se státními institucemi České republiky. Kvalifikovaný certifikát je ze zákona akceptován stejně jako občanský průkaz, avšak možnost využití kvalifikovaného certifikátu je omezena na vyjmenované případy:

* komunikace elektronickou cestou se státní správou pomocí emailu
* pro ověřování elektronických podpisů
* pro bezpečné ověřování elektronických podpisů

# Popište použití RSA šifry ve vícenásobném šifrování.

RSA (iniciály autorůp je [šifra](https://cs.wikipedia.org/wiki/%C5%A0ifra) [s veřejným klíčem](https://cs.wikipedia.org/wiki/Kryptografie_s_ve%C5%99ejn%C3%BDm_kl%C3%AD%C4%8Dem), jedná se o první [algoritmus](https://cs.wikipedia.org/wiki/Algoritmus), který je vhodný jak pro [podepisování](https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis), tak [šifrování](https://cs.wikipedia.org/wiki/%C5%A0ifrov%C3%A1n%C3%AD). Používá se i dnes, přičemž při dostatečné délce [klíče](https://cs.wikipedia.org/wiki/%C5%A0ifrovac%C3%AD_kl%C3%AD%C4%8D) je považován za bezpečný.

# Popište funkci otisku hash.

Jednocestá funkce která vytvoří kratší "odraz" původních dat. Tyto nemohou žádným způsobem být navrácena v původní data, pouze lze takto ověřovat pravost dat. Součástí kryptologie jsou tzv. výtahy zpráv (message digest) označované jako kryptografické hash kódy. Nejvýstižnějším názvem je však kryptografický kontrolní součet.

# Popište funkci digitálního podpisu.

**Elektronický podpis** (též **digitální podpis**, oficiálně kvalifikovaný certifikát) je v [informatice](https://cs.wikipedia.org/wiki/Informatika) označení specifických dat, které v [počítači](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8D) nahrazují klasický vlastnoruční [podpis](https://cs.wikipedia.org/wiki/Podpis), respektive [ověřený podpis](https://cs.wikipedia.org/wiki/%C3%9A%C5%99edn%C4%9B_ov%C4%9B%C5%99en%C3%BD_podpis).

**Elektronický podpis** je vytvořen pro konkrétní [data](https://cs.wikipedia.org/wiki/Data) a je možné pomocí počítače ověřit, zda je platný a zda jsou data v té podobě, ve které byla podepsána. Součástí elektronického podpisu je identifikace toho, kdo podpis vytvořil. Ověření elektronického podpisu zahrnuje kromě matematických operací i přenos důvěry z [důvěryhodné třetí strany](https://cs.wikipedia.org/wiki/D%C5%AFv%C4%9Bryhodn%C3%A1_t%C5%99et%C3%AD_strana) na tvůrce podpisu a následně na důvěryhodnost elektronicky podepsaného dokumentu. K tomu se využívá [digitální certifikát](https://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t) a [certifikační autorita](https://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita) nebo [síť důvěry](https://cs.wikipedia.org/wiki/S%C3%AD%C5%A5_d%C5%AFv%C4%9Bry).

V České republice existují v současnosti ([2014](https://cs.wikipedia.org/wiki/2014)) pouze tři subjekty oprávněné vydávat elektronický podpis.