10. Kryptografie, PKI a legislativa v IT

* Bez šifrování by byla síťová komunikace nebo jakákoliv data viditelná jako tzv, *plaintext*. - data může kdokoliv odchytit a přečíst je.
* Právě toto znemožní šifra, ta vytvoří text, který se dá zobrazit jen po rozšifrování.
* Šifrovací algoritmus většinou generuje pseudonáhodná čísla.

# Hashovací funkce

* Jednosměrná funkce
* Jakékoliv množství vstupních dat poskytuje stejně dlouhý výstup (otisk)
* Malou změnou vstupních dat dosáhneme velké změny na výstupu (tj. výsledný otisk se od původního zásadně na první pohled liší),
* Z hashe je prakticky nemožné rekonstruovat původní text zprávy
* v praxi je vysoce nepravděpodobné, že dvěma různým zprávám odpovídá stejný hash, jinými slovy pomocí hashe lze v praxi identifikovat právě jednu zprávu (ověřit její správnost).

## MD5

* Vytváří 16 bytové hashovací hodnoty v hexadecimálních číslech po 32 číslicích
* V dnešní době už není bezpečné
* Využití dnes už jen jako kontrolní součet pro ověření datové integrity

## SHA

* Obsahuje 3 různé SHA algoritmy (SHA-0; SHA-1; SHA-2)
* SHA-0 je velmi vzácně využíván
* SHA-1 je nejvyužívanější (produkuje 20 bytové hashovací hodnoty)

## SHA2

* Set 6 hashovacích algoritmů (pokládán za nejsilnější)
* Je doporučen SHA-256 nebo vyšší pro nejlepší bezpečnost
* SHA-256 vytváří 32 bytové hashovací hodnoty

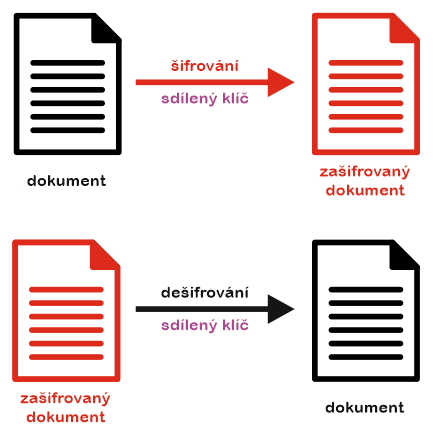
## Prolomení

* *Brute force attack*
* Postupné zkoušení všech známých použitých znaků, jejichž otisky se porovnávají s originálem
* Použití slovníkových hesel
* Vygooglovat hash

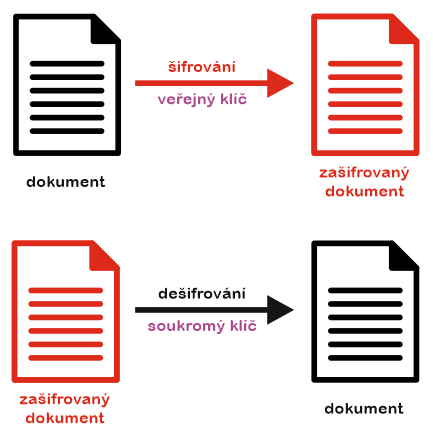
## Solení hesel

* K heslu se přidá ještě nějaký řetězec (sůl) a až potom se udělá HASH

# Symetrická kryptografie

* 
* Toto šifrování funguje pomocí jednoho klíče. Tento klíč musí být tajný (Private Key).
  + -> Obě strany ho musí získat dopředu (tzv. Pre-sharedKey/Secret).
* Předání buď proběhne fyzicky, nebo ho také můžete získat díky: Diffie–Hellman Key Exchange či Asymetrické kryptografii s veřejných klíčem
* Pokud nezískáme tento bezpečný kanál, tak nemůžeme komunikovat.
* V případě symetrického šifrování se tentýž klíč používá jak pro šifrování, tak i pro dešifrování
* Náročnost algoritmů není vysoká, takže výpočet není tak složitý
* Tento typ kryptografie je docela náchylný na útoky.
* Je o hodně rychlejší než asymetrické šifrování. (AES 256 x RSA 4,096)
* Block – zpracovávají data po stanovených celcích (64 bit nebo 128 bit)

# Asymetrická kryptografie

* 
* Zde se pro šifrování a dešifrování využívají dva klíče – Veřejný a soukromý klíč (Public, Private Key).
* Veřejný klíč a soukromý klíč jsou vzájemně spojeny a tvoří tzv. klíčový pár.
* Nejpoužívanější technika asymetrického šifrování se nazývá RSA.
* Veřejný klíč šifruje a soukromý klíč rozšifruje data.
  + Tyto klíče musí být párové, pouze jeden soukromý klíč je schopný získat původní data.
  + Složitost závisí na náročnosti veřejného klíče.  
    Veřejný klíč klidně může být volně k přístupu, aniž by to ovlivňovalo bezpečnost.
* Často se používá pro získání společného tajemství (Pre-shared secret), aby přenos byl rychlejší.
* Asymetrické šifrování je mnohem pomalejší. (AES 256 x RSA 4,096)
* Tento princip se používá při podepisování zpráv elektronickým podpisem.

# Šifrovací algoritmy

## AES

* Používá se k zabezpečení dat v sítí
* Pevně daná velikost bloku (128 bitů)
* Klíč velikost 128, 192, 256 bitů
* Používá se k zašifrování důležitých dat jako jsou dokumenty, informace o kreditní karty
* Náročný

### Inicializační část

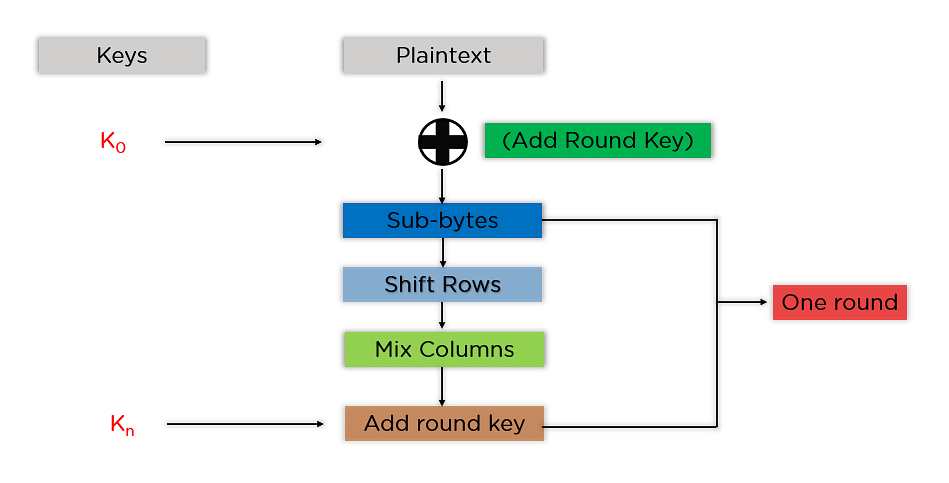
* Přidání podklíče (Add Round Key) − každý byte stavu je zkombinován s podklíčem za pomoci operace xor nad všemi bity

### Iterační část - 9, 11 nebo 13 iterací (v závislosti na délce klíče)

* Záměna bytů (SubBytes) − nelineární nahrazovací krok, kde je každý byte nahrazen jiným podle vyhledávací tabulky (S-Box)
* Prohození řádků (Shift Rows) − provedení kroku, ve kterém je každý řádek stavu postupně posunut o určitý počet kroků
* Kombinování sloupců (Mix Columns) − zkombinuje čtyři byty v každém sloupci
* Přidání podklíče (Add Round Key)

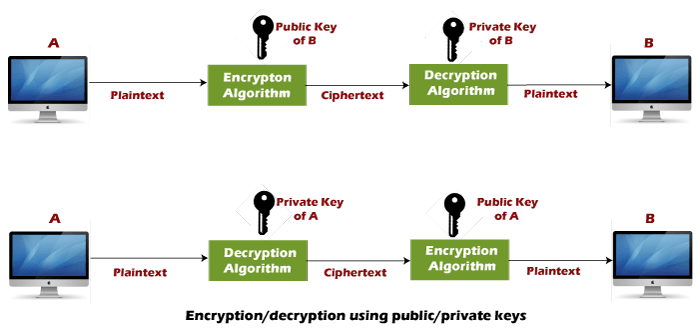
### Závěrečná část (nekombinují se sloupce)

* Záměna bytů (SubBytes)
* Prohození řádků (Shift Rows)
* Přidání podklíče (Add Round Key)



## RSA

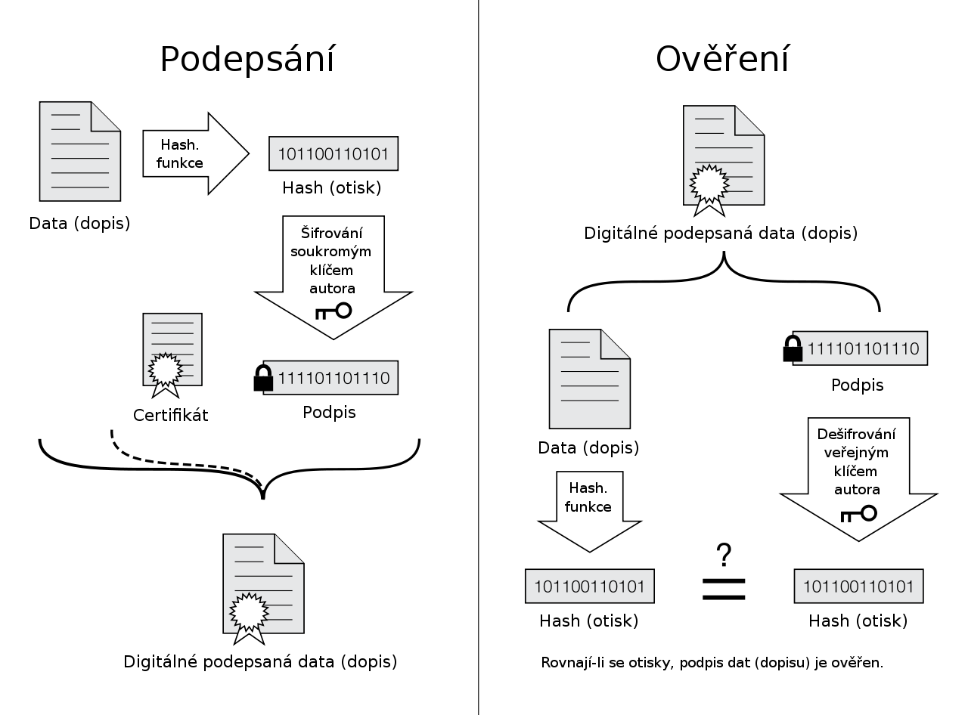
* Asymetrické šifrování
* Skládá se ze dvou klíčů (veřejný a soukromý)
* Veřejný klíč slouží k šifrování dat a soukromý klíč k dešifrování. Data zašifrovaná veřejným klíčem mohou být dešifrována pouze se soukromým klíčem. Používá se mod



## Césarova šifra

* Posun písmem o nějaký počet
* Příklad: Posun o 3 „A“ = „D“
* Je snadná k prolomení

# Elektronický podpis

* 
* Je to označení dat, které v počítači nahrazují vlastnoruční podpis
* Je připojen k datové zprávě nebo je s ní logicky spojen -> umožňuje ověření totožnosti podepsané osoby ve vztahu k datové zprávě.
* Ověření identity odesílatele.
* Je vytvořen pro konkrétní data a je možné počítačem ověřit, zda je platný a jestli jsou data ve stejné podobě, ve které byla odeslána. Součástí toho je identifikace, kdo podpis vytvořil.

## Autenticita

* Lze ověřit identitu subjektu, kterému patří elektronický podpis

## Integrita

* Lze prokázat, že nedošlo k žádné změně v podepsaném dokumentu, tj. že dokument není úmyslně či neúmyslně poškozen

## Nepopiratelnost

* Autor nemůže tvrdit, že elektronický podpis příslušný k dokumentu nevytvořil. Důvodem je fakt, že po vytvoření el. podpisu je potřeba privátní klíč.

## Časové ukotvení

* Elektronický podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu.
* Časové razítko vydává důvěryhodná třetí strana, a protože je součástí elektronického podpisu, lze ji ověřit stejným postupem, jako elektronický podepsaný dokument.

## Princip

* 1. Spočte se kontrolní součet (hash) z dokumentu.
* 2. Výsledný kontrolní součet se šifruje soukromým klíčem uživatele, který podpis vytváří.  
  Soukromým klíčem šifrovaným hash ze zprávy se nazývá elektronický podpis zprávy.

## Verifikace

* 1. Příjemce samostatně spočte kontrolní součet z přijaté zprávy.
* 2. Příjemce dešifruje přijatý elektronický podpis veřejným klíčem odesílatele.
* 3. Příjemce porovná výsledek získaný z bodu 1 s výsledkem získaného z bodu 2. Pokud jsou stejné, pak elektronický podpis mohl vytvořit pouze ten kdo vlastní soukromý klíč odesílatele --> odesílatel.
* Je nutné si svůj soukromý klíč střežit a chránit.
* Na rozdíl od šifrování elektronický podpis použije klíč odesílatele, ale odesílatel pro podpis použije svůj soukromý klíč.

# PKI

* správy a distribuce veřejných klíčů z asymetrické kryptografie

## Certifikát

* Certifikát obsahuje mj.: informace o tom, kdo jej vydal, sériové číslo certifikátu, identifikační údaje uživatele, platnost certifikátu a pochopitelně veřejný klíč uživatele.
* Certifikát je digitálně podepsán za využití soukromého klíče certifikační autority.

## Certifikační autorita

* Subjekt, který vydává certifikáty, funguje na principu důvěry
* Tyto certifikáty obsahují identifikační údaje svého majitele
* Při žádosti musí přesvědčit to, že je to skutečně on (fyz. osoba --> občanský průkaz  
  práv. osoba --> ověření výpisu z obchodního rejstříku)

# eIDAS

* Nařízení evropské unie
* Vytvořilo standardy pro elektronický podpis, kvalifikované digitální certifikáty, elektronické pečeti, časová razítka
* Zajištění bezpečnosti pro uživatele podnikající on-line, například při elektronickém převodu finančních prostředků nebo při komunikaci s veřejnými službami.

# GDPR

* Je obecné nařízení o ochraně osobních údajů, které stanovuje pravidla pro zpracování osobních údajů v Evropské unii.
* Cílem GDPR je poskytnout osobám v EU větší kontrolu nad svými osobními údaji a zajistit, aby byla dodržována stejná pravidla pro zpracování osobních údajů po celé EU.

# NIS

* Je evropskou směrnicí, která se zabývá bezpečností informačních systémů v celé Evropské unii.
* Směrnice NIS stanovuje minimální požadavky na bezpečnost informačních systémů a povinnosti pro vlády, poskytovatele služeb kritických pro společnost a velké podniky. (Cloud computing)
* Cílem směrnice NIS je zlepšit celkovou úroveň bezpečnosti informačních systémů v Evropské unii a snížit riziko škod způsobených výpadky v těchto systémech.