KRYPTOGRAFIE

CO JE KRYPTOGRAFIE

- Kryptografie je matematický vědní obor, který se zabývá šifrovacími a kódovacími algoritmy.
- Dělí se na dvě skupiny – návrh kryptografických algoritmů a kryptoanalýzu, která se naopak snaží šifrovací algoritmy prolomit.
- **Šifrovací algoritmy** – algoritmus, který se snaží ochránit data šifrováním. K tomu využívá nějakého tajemství nazýváme ho šifrovacím klíčem. Více lidí díky tomu, může používat jeden šifrovací algoritmus, ale každý má svoje šifrovací a dešifrovací klíče.
- **Kódovací algoritmus** – algoritmus se stejnou funkcí – snaží se ochránit data před neoprávněním přečtením. Do procesu vůbec nevstupuje žádné tajemství, utajení má na starost vlastní algoritmus.
- **Prolomení algoritmu** – Algoritmus je prolomen, pokud je možné číst chráněná data bez znalosti šifrovacího klíče anebo kódovacího algoritmu.

ŠIFROVÁNÍ VERSUS PODEPISOVÁNÍ

- **Šifrování**
  - Úkolem šifrování je změnit data, tak aby je nemohla přečíst neoprávněná osoba.
  - Šifrování tedy zajišťuje důvěrnost přenášených dat.
- **Podepisování**
  - Podepisování má dva hlavní úkoly
    - **Nepopíratelnost** – jednoznačná identifikace identity podepisujícího
    - **Integritu** – má na starosti ověření toho, že data během přenosu nebyla pozměněna.

PROUDOVÉ A BLOKOVÉ ŠIFRY

- Kromě dělení šifrování na symetrické a asymetrické můžeme dělit dle šifrovacích algoritmů.
- Jedním z nich je dělení podle množství dat, které jsou schopni na jednou šifrovat.
- Šifrování po jednotlivých znacích nazýváme proudové šifry.
- Šifrování po jednotlivých blocích nazýváme blokové šifry.

MÓDY ČINNOSTI BLOKOVÝCH ŠIFER

- Blokové kryptografické algoritmy šifrují otevřený text po malých blocích.
- Kryptologové definovaly pět módů činností blokových šifer, které se liší zapojením základního šifrovacího bloku:
  - **Mód ECB**
  - **Mód CBC**
  - **Mód CFB**
  - **Mód OFB**
  - **Mód EDE**

MÓD ECB (ELECTRONIC CIPHER BOOK)

- Základní mód všech blokových šifer.
- Na vstupu se objeví blok otevřeného textu na konci blok šifrovaného textu.
- Pokud se objeví stejný blok výsledek je totožný blok šifrovaného textu.
- Celá šifra je jednoduše překladový slovník – každý blok otevřeného textu je přiřazen blok šifrovaného textu.

Nevýhody

- Princip útoku – útočník si postupně vytvoří vlastní slovník.
- Postupem času dokážeme odhalit větší a větší část otevřeného textu.
- Problém s bloky – bloky jsou šifrovány na sobě nezávisle.
- Kdykoli může být libovolný z přenášených bloků nahrazen jiným, aniž by to příjemce poznal.

MÓD CBC (CIPHER BLOCK CHAINING)

- Tento mód zavádí do blokové šifry jistotu nezávislosti mezi postupně šifrovanými bloky.
- Využívá k tomu logické funkce nonekvivalence (XOR).
- Po zašifrování prvního bloku otevřeného textu je získán blok šifrovaného textu.
- Tento blok se xoruje s druhým blokem otevřeného textu, teprve výsledek této operace vstupuje do šifrovacího algoritmu.
- Nepříjemnou vlastní je stále stejné šifrování prvního bloku, který se šifruje pomocí ECB módem. V řadě případů bývá úvod zprávy stále stejný.
- Aby se tomu zamezilo, používá se takzvaný inicializační vektor.
- Jedná se o náhodné číslo, které se použije ke xorování prvního bloku otevřeného textu.
- Inicializační vektor není tajný musejí ho znát obě strany.

DALŠÍ DVA MÓDY

- Následují dva módy přepínají blokovou šifru do proudové režimu.
- Aby nedošlo k problému se stejným šifrováním je do systému zaveden pseudonáhodný prvek.
- Vlastní data jsou šifrována posloupností pseudonáhodných čísel, jejich generování je řízeno zpětnou vazbou.
- Přesné zapojení zpětné vazby je odlišné pro jednotlivé módy:
  - Mód CFB
  - Mód OFB
  - Mód EDE

MÓD CFB (CIPHER FEEDBACK MODE

- Genrátor pseudonáhodných čísel je řízen výstupem samotného generátoru.
- Zpětná vazba je tedy zapojena až z úplného výstupu šifrovacího zařízení.

MÓD OFB (OUTPUT FEEDBACK MODE)

- Generátor pseudonáhodných čísel je řízen výstupem samotného generátoru.
- Zpětná vazba je v tomto případě zapojena již z výstupu generátoru pseudonáhodných čísel.
- Toto je zásadní rozdíl oproti módu CFB.

MÓD EDE (ENCRYPTION-DECRYPTION-ENCRYPTION)

- Jedná se o zapojení tři šifrovacích bloků do série.
- První a poslední blok data šifruje klíčem K1.
- Prostřední blok zašifrovaná data dešifruje klíčem K2.
- Délka klíče se tedy zdvojnásobí, existuje ale i varianta, která využívá tři různé klíče K1,K2,K3., což délku klíče ztrojnásobuje.

SYMETRICKÁ KRYPTOGRAFIE

- Algoritmy symetrické kryptografie pracují s jedním klíčem, který spolu sdílejí komunikační strany.
- Jeden klíč se používá pro šifrování i dešifrování.
- Výhodou symetrické kryptografie je její obrovská rychlost.
- Nevýhodou vyšší nároky na počet klíčů a jejich správu
- Ideálním řešením se jeví být hybridní kryptografie, kdy vlastní zpráva je zašifrována rychlým symetrickým algoritmem s náhodně vygenerovaným klíčem.
- Klíč je pak zašifrován asymetrickým algoritmem a přiložen ke zprávě.
- Při tvorbě symetrických kryptografických algoritmů se používají dvě základní techniky.
- První z nich je substituce, která nahrazuje znak otevřeného textu znakem šifrovaného textu podle předepsaného klíče.
- Druhou je pak transpozice, která zachovává hodnotu znaků, mění ale jejich pořadí.
- Řada algoritmů využívá kombinaci těchto technik.

SYMETRICKÁ KRYPTOGRAFIE SUBSTITUČNÍ ŠIFRY

- Substituce znamená nahrazení .
- Substituční šifry nahrazují znaky otevřeného textu jinými znaky, čímž vzniká šifrování.
- Přesné přiřazení znaků šifrovaného textu znakům otevřeného textu závisí na hodnotě šifrovacího klíče a řídí ji takzvaná substituční tabulka.
- Substituční šifry se dělí do několika skupin, od nejjednodušších monoalfabetických šifer, které najdou uplatnění u skautů nebo pionýrů.
- Až po propracované polyalfabetické algoritmy.

SYMETRICKÉ KRYPTOGRAFIE – MONOALFABETICKÁ SUBSTITUČNÍ ŠIFRA

- Jedna z nejjednodušších substitučních šifer.
- Existuje statická tabulka, která se používá k překladu znaků otevřeného textu na znaky šifrovaného textu a naopak.
- Vysoce primitivní kterou zvládají dešifrovat děti školou povinné.

SYMETRICKÉ KRYPTOGRAFIE – HOMOFONNÍ SUBSTITUČNÍ ŠIFRA

- Hlavní nevýhodou monoalfabetické substituční šifry – slabou odolnost proti frekvenční analýze – odstraňuje takzvané homofonní substituční šifra.
- Každá znak otevřeného textu se může šifrovat na několik různých znaků šifrovaného textu.
- Například znak A se může šifrovat jako jedno z písmen „XKZ“.
- Ani homofonní šifry nedokáží zakrýt všechny typické statistické znaky jazyka.
- Luštění těchto šifer je triviální záležitost.

SYMETRICKÉ KRYPTOGRAFIE – POLYGRAMOVÁ SUBSTITUČNÍ ŠIFRA

- Substituční tabulka v tomto případě obsahuje celé skupiny znaků.
- Například skupina ABC v otevřeném textu se zamění za skupiny XYZ v šifrovaném textu.

SYMETRICKÉ KRYPTOGRAFIE – POLYALFABETICKÁ SUBSTITUČNÍ ŠIFRA

- Nejpokročilejší ze substitučních šifer jsou víceabecedové šifry.
- Ve své podstatě se jedná o skupinu monoalfabetických šifer, které jsou aplikovány na jednotlivé znaky otevřeného testu postupně.
- První znak je zašifrován první monoalfabetickou šifrou, druhý znak druhou, třetí znak třetí.
- Počet šifer je omezený nějakým vhodným číslem např. pátý znak opět šifrován první šifrou.
- Základem této šifry je tabulka o rozměrech 26 x 26 políček.
- V první sloupci je vepsána klasická anglická abeceda, v dalším je tatáž abeceda posunuta o jeden znak a dále.
- Zvolené heslo pak určuje, které sloupce se při jednotlivých krocích šifrovaní použijí.

NEROZLUŠTITELNÁ ŠIFRA – VERNAMOVA ŠIFRA

- Tato šifra je z hlediska kryptoanalýzy nerozluštitelná.
- Jedná se o takzvaný jednorázový heslař (one-time).
- Jakákoliv šifra pokud využívá naprosto náhodný šifrovací klíč o stejné délce, jako má otevřený text, je bezpečný.
- Musí platit jedno pravidlo každý klíč smí být použít pouze jednou.
- Její podstatou je blok provádějící bitovou operaci nenokvivalence (xor).
- Jednotlivé znaky otevřeného textu jsou xorovány se znaky jednorázového klíče, pro dešifrovaní se používá naprosto identický postup.
- Hlavním problémem je tady šifrovací klíč.
- Pokud se už podaří nějaký vhodný vyrobit, musí být bezpečným způsobem distribuován oběma stranám.
- Kromě toho, po použití musí být bezpečně zničen, aby ho už nikdo nikdy nepoužil.

TRANSPOZIČNÍ ŠIFRY

- Transpozice mění pouze pozici znaků ve zprávě.
- V matematice je používán tento termín „**Permutace**“
- Mezi nejjednodušší transpozice patří rozepsání šifrovaného textu do sloupců s danou délkou.
- Pokud má text o délce sto znaků, rozepíšeme ho do matice 10x10 po řádcích a přepíšeme ho po sloupcích.
- Obecně je možné použít jakýkoliv permutační algoritmus, který je reverzibilní (text rozházet a opět srovnat).
- Výhodou transpozičních šifer je rozbití větších struktur – bigranů a trigramů.

ŠIFROVACÍ ALGORITMUS DES

- DES je bloková šifra o velikosti bloků 64 bitů.
- Stejnou délku má i šifrovací klíč a každý 8bit klíče je paritní, efektivní délka klíče je 56 bitů.
- Paritní bity se ve většině případů rovnou ignorují. Jedná se o nejméně významné bity.
- DES je kombinací substitučních a transpozičních šifer.
- Na blok otevřeného textu se nejdříve použije jednoduchá substituce a poté transpozice.
- Tento krok se opakuje 16x jedno opakování se označuje jako runda.

ŠIFROVACÍ ALGORITMUS AES

- AES (Advanced Excryption Standard).
- Bloková šifra s délkou klíče, které může nabývat tří hodnot 128,192, 256 bitů.
- Délka bloků je ve všech případech 128 bitů, podle délka se však mění počet rund.
- Pro nejkratší postačuje 10 rund, střední mí dvacet rund a pro největší čtrnáct rund.
- Postup-
  - Nejprve je provedena substituce přichází ke slovu S-box.
  - Poté následuje dva speciální transpoziční kroky.
  - Blok je uspořádán do matice, nejprve jsou rotovány jednotlivé řady
  - Následují sloupce pomocí vynásobení speciální maticí.
  - Na závěr jsou data zkombinována s šifrovacím klíčem
  - Klíč se samozřejmě, stejně jako u DESu, pro každou rundu mění.

DALŠÍ SYMETRICKÉ ALGORITMY

- **RC2**: bloková šifra. Vyvinuta společností RSA, která ho tají jako firemní tajemství. Pracuje s 64 bitovými bloky dat, délka klíče se může měnit.
- RC4: proudová šifra patřící firmě RSA.
- IDEA: jedná se o blokovou šifru s blokem o délce 64 bitů. Klíč má délku dvojnásobnou (tedy 128 bitů).

ASYMETRICKÁ KRYPTOGRAFIE

- Asymetrická kryptografie existuje na dvou klíčích tzv. klíčový pár.
- Jedním klíčem zašifrujeme data a druhým dešifrujeme data.
- Zašifrováním jedním klíčem není možné tímto klíčem dešifrovat.
- Je jedno jaký klíč k čemu použijete.
- Klíče se rozdělují na veřejný a soukromý klíč.
- Veřejný klíč normálně distribuujeme, pro potřeby šifrování a soukromý klíč, který je tajný si uživatel uschová a tají za účelem dešifrování.

ALGORITMUS RSA I

- Algoritmus RSA (Rivestu, Shamirovi a Alemanovi). Jedná se o zatím nepokořený algoritmus založený na složitosti faktorizace velkých prvočísel.
- Před šifrováním se vytvoří pár klíčů. Pro tyto účely vytvoříme náhodná čísla p a q, která musí být prvočísla.
- Vygeneruje se náhodné číslo, které se následně podrobí textu prvočíselnosti.
- Test prvočíselnosti spočívá v postupném dělení čísla malými prvočísly, což by mělo ve většině případů odhalit jeho neprvočíselnost.
- Obě prvočísla jsou vynásobena, dostáváme číslo n= p . Q. veřejný klíč nyní generujeme jako náhodné číslo e, které nemá žádné společné součinitele s číslem (p-1)(q-1)..
- Soukromý klíč vzniká mnohem složitější matematickou operací. Získáme ho podle vztahu $d = e^{-1}$ mód ((p-1)(q-1)).
- Veřejný klíč je tvořen dvojicí { n, e}, soukromý má dvojici {n, d}. Čísla p a q jsou nyní nepotřebná, můžeme je zničit.

ALGORITMUS RSA II

- Zbývá definovat šifrování a dešifrování:
  - **Šifrování** ŠT = OT^e mod n
  - **Dešifrování** OT = $ŠT^d$ mod n.
- Jelikož je jedno jakým klíčem se šifruje a kterým dešifruje, můžeme oba vztahy klidně přepsat do této podoby:
  - Šifrování ŠT = OT^d mod n.
  - Dešifrování OT = $ŠT^e$ mod n.