Kryptografie
1. Úvod

Osnova

- Informace o výuce https://moodle.vutbr.cz/
- Předpokládané znalosti
- Kryptografické systémy
- Služby bezpečnosti,...

Kryptografický systém - formální definice

Kryptografický systém pro šifrování zpráv je pětice $(\mathcal{M},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$, kde

- $\mathcal{M}$ je prostor otevřených zpráv,
- $\mathcal{C}$ prostor šifrových zpráv,
- $\mathcal{K}$ prostor klíčů,
- $\mathcal{E},\mathcal{D}$ je dvojice zobrazení, které každému klíči $k \in \mathcal{K}$ přiřazují transformaci pro zašifrování zpráv E a transformaci pro dešifrování zpráv D, přičemž pro každé $k \in \mathcal{K}$ a $m \in \mathcal{M}$ platí $D(k(E(k,m)) = m$.

Definice šifer

- **Symetrická šifra** je taková šifra, kde pro každé $k \in \mathcal{K}$ lze z transformace zašifrování E_k určit transformaci dešifrování D_k a naopak.
- **Asymetrická šifra** je taková šifra, kde pro skoro všechna $k \in \mathcal{K}$ nelze z transformace pro zašifrování E_k určit transformaci pro dešifrování D_k. V praxi je u asymetrických šifer klíč k tajným nastavením, ze kterého se vhodnou transformací G vygeneruje dvojice parametrů (e, d), které se nazývají **veřejný** ($k_{pub} = e$) a **privátní** ($k_{pr} = d$) klíč. Ty potom parametrizují transformace zašifrování a dešifrování, takže pro jednoduchost nepíšeme E_k a D_k , ale přímo E_e a D_d.

Upřesnění pojmů

Šifra – algoritmus, zobrazení, funkce (***E***, ***D***)

- ***E*** **- encryption function,** (“*pravděpodobnostní*” polynomiální algoritmus)
- ***D*** **- decryption function,** (deterministický polynomiální algoritmus)
- otevřený text ***m*** - **message** = zpráva *Z*, někdy *P* plain text, *OT*,...
- šifrový text ***c*** - **cipher text** = šifrovaný text (*ŠT*)

$$c = E(k_1, m)$$
$$m = D(k_2, c) = D(k_2, E(k_1, m))$$

- klíč k - $k_1 = k_2$ - **symetrické algoritmy** - tajný klíč, **secret key**
- klíč k - $k_1 \neq k_1$ - **asymetrické algoritmy**
  - $k_1 = k_{pub}$ **public key**, veřejný klíč, slouží k **šifrování**
  - $k_2 = k_{prv}$ **private key**, soukromý klíč, slouží k **dešifrování**

Používané algoritmy - šifry

Tajný algoritmus, omezený algoritmus (restricted algorithm)

- bezpečnost algoritmu založena na jeho utajení
- je nemožné algoritmus utajit na delší dobu
- používá se v systémech s nízkým stupněm zabezpečení
- v komunikačních systémech se nepoužívají

Algoritmy s využitím klíčů

- **Kerckhoffsův princip** (Auguste Kerckhoffs 1835 – 1903)
- **bezpečnost šifrovacího systému má záviset pouze na utajení klíče**
- algoritmy jsou většinou známé
- bezpečnost je zaručena použitím klíčů

Základní typy kryptografických prostředků

Symetrické šifry

- proudové a blokové šifry, (AES, A5, RC5, CAST, 3DES, IDEA, Blowfish,...)

Asymetrické šifry

- pro šifrování (výměnu klíčů), (RSA, DH, ECC,...)
- pro digitální podpis, (RSA, DSA, ECDSA,...)

Hašovací funkce, (SHA-1, SHA-2, SHA-3,...)

Kvantová kryptografie

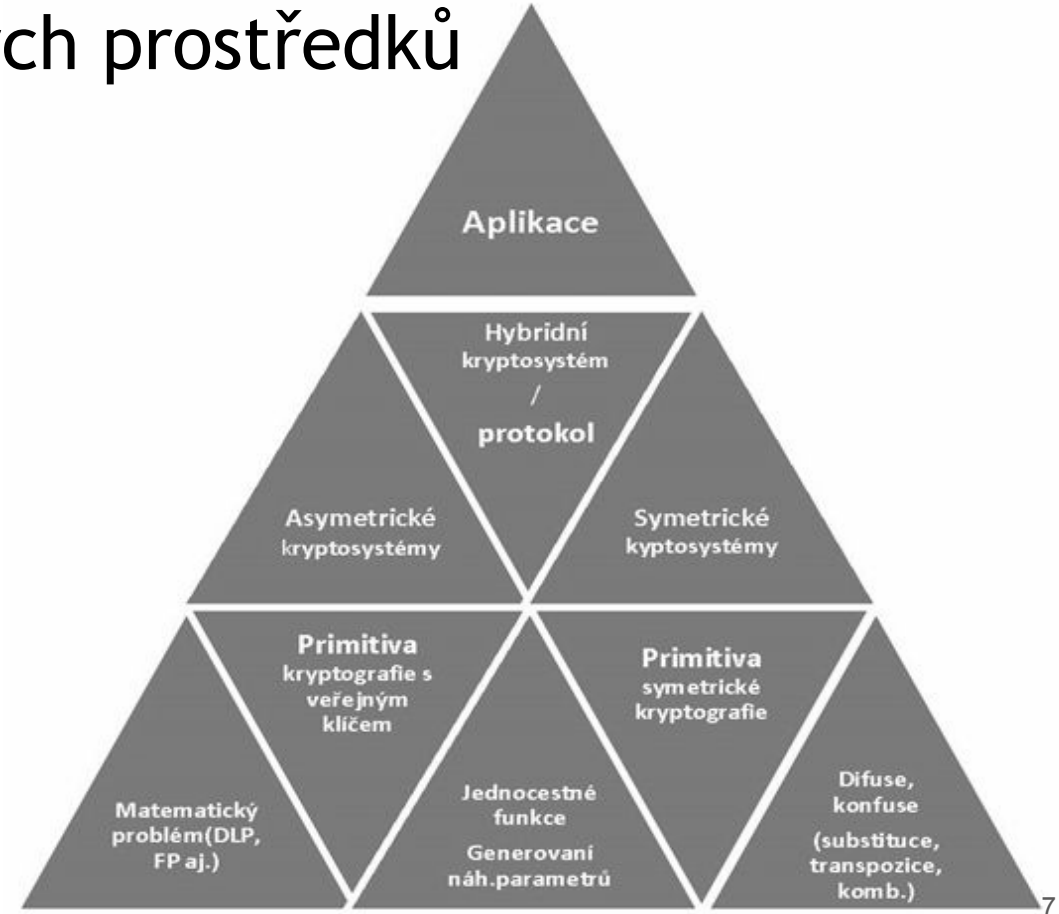
- přenos klíčů, (BB84,...), generátory náhodných čísel,

Další techniky

- generátory náhodných čísel (FIPS PUB 140-2,...)

Úrovně kryptografických prostředků

- Aplikace
- Kryptosystémy a protokoly
- Primitiva a základní algoritmy
- Matematické a implementační základy



Bezpečnost IT

- Pod pojmem bezpečnost IT obvykle rozumíme ochranu odpovídajících systémů a informací, které jsou v nich uchovávány, zpracovávány a přenášeny.
- Pro zajištění bezpečnosti je třeba
  - Bezpečnostní model - identifikace rizik.
  - Bezpečnostní politika - definice aktiv, která chceme chránit.
  - Bezpečnostní prostředky - určení konkrétních nástrojů pro ochranu.
- Prostředky zajišťující bezpečnost
  - Administrativní
  - **Elektronické - kryptografické**, …
  - Fyzické
  - …

Architektura bezpečnosti v RM OSI

- doporučení ITU-T X.800, ISO 7498-2 ISO/OSI Security Architecture

Obsahuje

- **služby bezpečnosti** – ***security services***,
  - definované postupy pro zabezpečení informačních systémů,
- **mechanismy bezpečnosti - *security mechanism***,
- **útoky na bezpečnost - *security attacks***.

Implementace bezpečnostních funkcí ve vrstvách RM OSI

- Pro implementaci bezpečnostní funkce je nejvhodnější
  - 7. vrstva – aplikační protokoly
  - 4. vrstva – transport dat
  - 3. vrstva - směrování
- Bezpečnostní mechanismy jsou zpravidla zabudovány do
  - aplikačních programů a operačních systémů (7. a 4. vrstva)
  - propojovacích zařízení 3. vrstvy (směrovače)
- existují řešení využívající i ostatních vrstev

Služby bezpečnosti - ISO 7498-2

Služba realizovaná protokolem příslušné vrstvy RM datové komunikace.

5 kategorií služeb

1. **autentizace - *authentication***
2. řízení přístupu - *access control*
3. **zabezpečení důvěrnosti dat - *data confidentiality***
4. **zabezpečení integrity dat - *data integrity***
5. **ochrana proti odmítnutí původu zprávy - *non-repudiation***

Vysvětlení pojmů

Autentizace (*authentication*)

- proces ověřování identity uživatele (entity).

Autorizace (*authorization*)

- přiřazení oprávnění pro práci v systému, specifikuje činnosti,
- autorizovaný uživatel – uživatel s oprávněním provést určitou operaci.

Kontrola přístupu (*access control*)

- možnost povolit nebo odepřít použití určitého zdroje určitému subjektu, řízení přístupu k materiálním, logickým, nebo digitálním zdrojům,
- často bývá tento pojem zaměňován za autorizaci.

Služby bezpečnosti - ISO 7498-2

1. **autentizace - *authentication***

- uživatelů - peer entity authentication
  - neeliminují útoky zopakováním zpráv
- zdroje dat - data origin authentication
  - provádí autentizaci všech dat
  - eliminují útoky zopakováním zpráv

2. **řízení přístupu - *access control***

- přístup do systému, k službám, ...
- ochrana před neautorizovaným přístupem (nejobvyklejší je implementace v operačním systému nebo v aplikačním programu)

Služby bezpečnosti - ISO 7498-2

3. **zabezpečení důvěrnosti dat - *data confidentiality***

- ochrana informačního obsahu dat, ochrana toku dat při přenosu proti analýze (zjištění odesilatele, adresáta, ...)
  - **služby pro důvěrnost přenosu zpráv**
  - **služby pro důvěrnost spojení** - ochrana důvěrnosti v rámci navázaného spojení
  - **služby pro důvěrnost toku dat** (chrání informace na základě atributů toku dat)
  - **služby selektivní důvěrnosti** - ochrana pouze určených částí informace

Služby bezpečnosti - ISO 7498-2

4. **zabezpečení integrity dat - *data integrity***

- zabezpečení proti neautorizované modifikaci
  - služby integrity přenosu zpráv (ochrana integrity všech přenášených zpráv)
  - služba integrity spojení (ochrana přenosů v rámci určitého navázaného spojení)
  - služby selektivní integrity spojení a selektivní integrity zpráv
- **„slabá“ integrita** – pro objektivní útoky (modifikace zprávy šumem, náhodná změna pořadí paketů, náhodná duplicita…) – aplikace kontrolních součtů, CRC, pořadová čísla paketů apod.
- **„silná“ integrita** – subjektivní (úmyslné, aktivní útoky) – podvržené zprávy, úmyslně pozměněné zprávy – prostředky pro zajištění slabé integrity + kryptografické prostředky
  - služba integrity bez oprav (detekce porušení integrity)
  - služba integrity s opravami – obnova integrity po detekci ztráty integrity

Služby bezpečnosti - ISO 7498-2

5. **ochrana proti odmítnutí původu zprávy - *nonrepudation***
- zajišťuje důkaz o původu dat
- prokázání původu (příjemce/odesílatel)
- prokázání doručení (odeslání/přijetí)

Autentizace a nepopiratelnost
- autentizace – vím s kým komunikuji
- nepopiratelnost – vím s kým komunikuji a lze mu to dokázat

	Vrstva, kde může být služba zajištěna						
Bezpečnostní služba	1	2	3	4	5	6	7
Autentizace spojení			A	A			A
Autentizace odesilatele			A	A			A
Řízení přístupu			A	A			A
Důvěrnost spojení	A	A	A	A		A	A
Důvěrnost přenosu zpráv		A	A	A		A	A
Selektivní důvěrnost						A	A
Důvěrnost toku dat	A		A				A
Integrita spojení s opravou				A			A
Integrita spojení bez opravy			A	A			A
Selektivní integrita spojení							A
Integrita přenosu zpráv			A	A			A
Selektivní integrita zpráv							A
Nepopiratelnost odesílatele							A
Nepopiratelnost doručení							A

Mechanismy bezpečnosti - ISO 7498-2

- **šifrování** - *encipherment*
- **digitální podpis** - *digital signature*
- **řízení přístupu** - *access control*
- **integrita dat** - *data integrity*
- **výměna autentizační informace** - *authentication exchange*
- **„výplň“** - *traffic padding*
- **řízení směrování** - *routing control*
- **ověření třetím subjektem** - *notarization*

	Bezpečnostní mechanismy							
Bezpečnostní služba	Šifr.	EP	Ř. příst.	Int. mech.	Aut.	Zar.	Ř. přen.	Not. sl.
Autentizace spojení	A	A			A			
Autentizace odesilatele	A	A						
Řízení přístupu			A					
Důvěrnost spojení	A							
Důvěrnost přenosu zpráv	A						A	
Selektivní důvěrnost	A						A	
Důvěrnost toku dat	A					A	A	
Integrita spojení s opravou	A			A				
Integrita spojení bez opravy	A			A				
Selektivní integrita spojení	A			A				
Integrita přenosu zpráv	A	A		A				
Selektivní integrita zpráv	A	A		A				
Nepopiratelnost odesílatele	A	A		A				A
Nepopiratelnost doručení	A	A		A				A

Bezpečná komunikace podle ISO 7498-2

- Komunikující strany věří na základě **vzájemné autentizace**, že komunikují s oznámeným partnerem nebo že přijali zprávu z **autentizovaného zdroje**,
- přenášená informace nemůže být odposlouchávána, neboť je zajištěna její **důvěrnost**,
- přenášená informace není změněna, neboť je zajištěna její **integrita**,
- komunikace je umožněna pouze **autorizované straně**, neboť je uplatněno **řízení přístupu**,
- komunikace nemůže být popřena, neboť je zajištěna **nepopiratelnost** odeslání i příjmu zpráv.

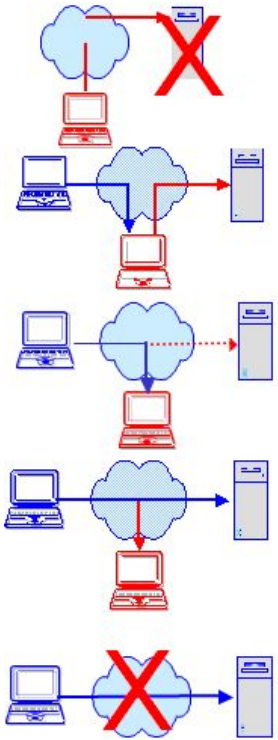
Bezpečná komunikace podle ISO 7498-2

Bezpečná spojovaná relace zahrnuje kroky

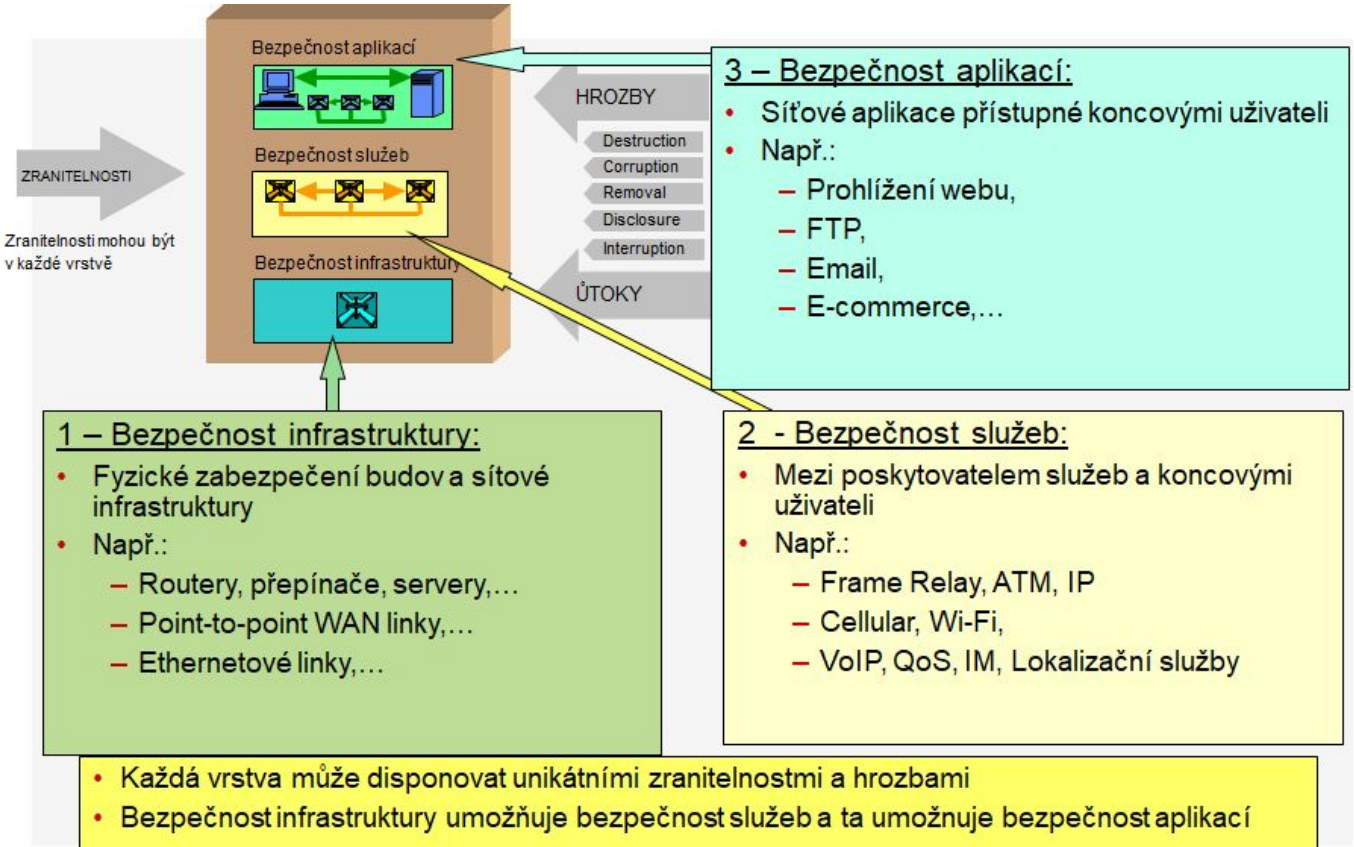
1. navázání spojení s **autentizací** prostřednictvím asymetrického kryptografického algoritmu
2. výměna symetrických klíčů pro zajištění **integrity a důvěrnosti** následné výměny zpráv
3. **bezpečná výměna zpráv**
4. zrušení spojení včetně všech zbytkových informací
5. **ověření autentičnosti, integrity a důvěrnosti** přijaté informace

Model hrozeb dle ITU-T X.800

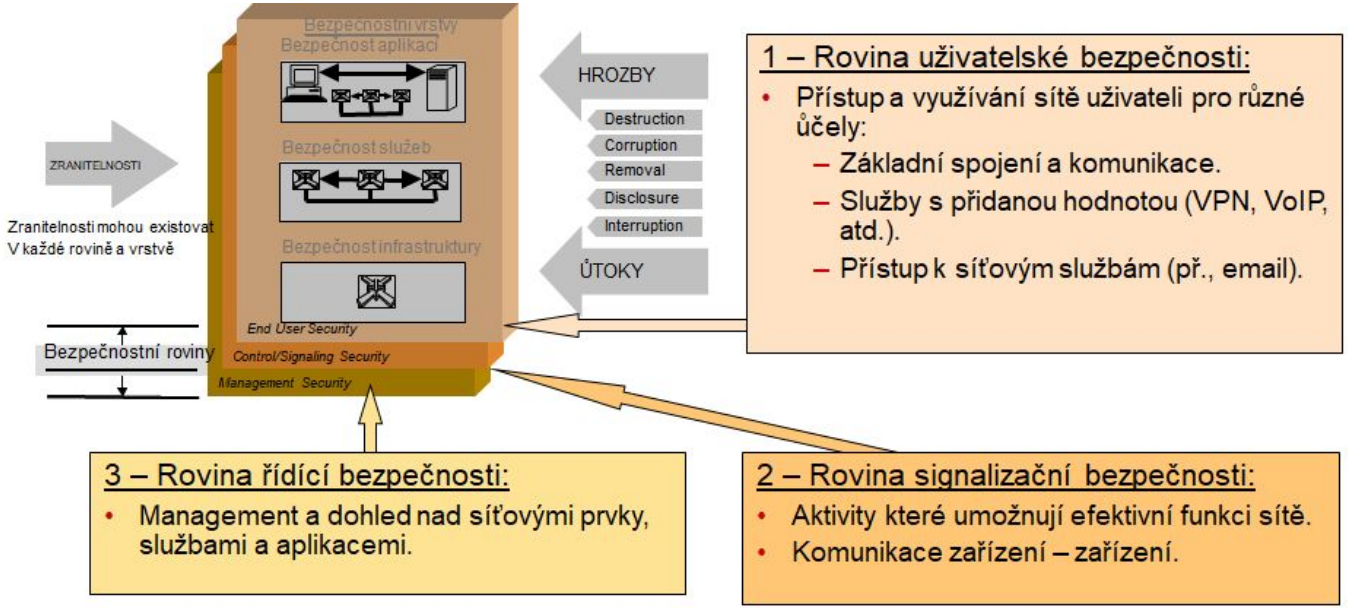
1. **Destruction** (útok na dostupnost): Zničení dat či síťových zdrojů.
2. **Corruption** (útok na integritu): Neautorizovaná modifikace aktiv/dat.
3. **Removal** (útok na dostupnost): Krádež, odebrání či ztráta informací nebo jiných zdrojů.
4. **Disclosure** (útok na důvěrnost): Neautorizovaný přístup k aktivům/datům.
5. **Interruption** (útok na dostupnost): Přerušení služeb. Spojení začne být nepoužitelné.



“Bezpečnostní vrstvy” Three Security Layers



“Bezpečnostní roviny” Three Security Planes



- Bezpečnostní roviny reprezentují jednotlivé činnosti v síti.
- Každá bezpečnostní rovina je aplikovaná na každou síťovou vrstvu a celkově tvoří 9 bezpečnostních perspektiv (3 x 3).
- Každá bezpečnostní perspektiva má unikátní zranitelnosti a hrozby.