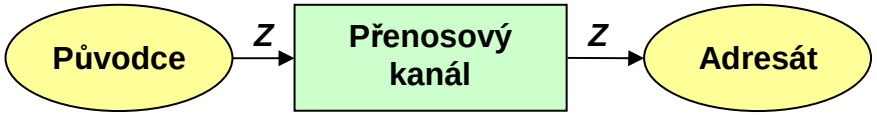
Matematika v kryptografii

Doc. Ing. Karel Burda, CSc.

FEKT VUT v Brně

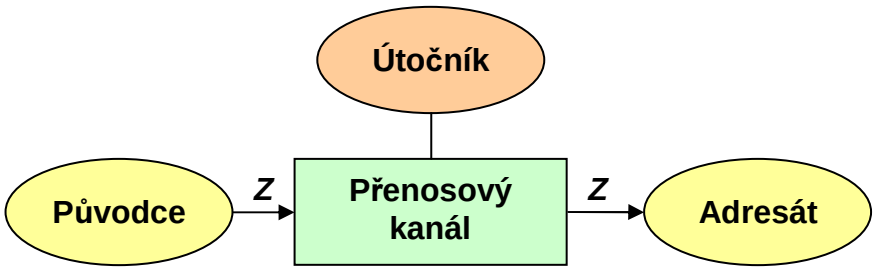
Přenos zpráv

- Zpráva *Z*: posloupnost čísel, ve které je všeobecně známým kódem zakódována nějaká informace.
- Původce zprávy: zdroj zpráv (osoba nebo zařízení).
- Adresát zprávy: zamýšlený příjemce zpráv.
- Přenosový kanál: technický systém, který umožňuje buď přenos zpráv prostorem (komunikační kanál) nebo přenos zpráv časem (paměťový kanál).



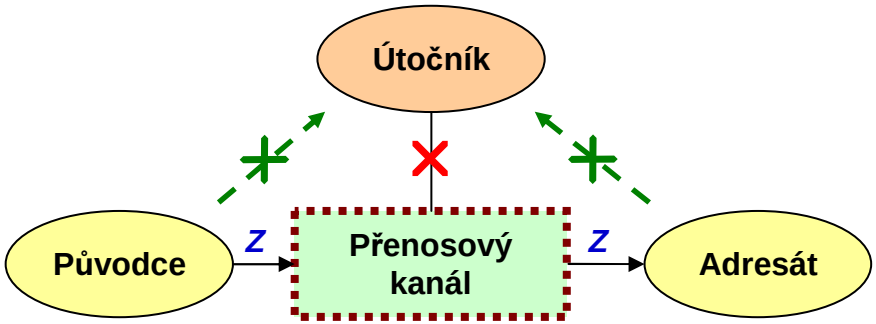
Důvěrnost a autentičnost zpráv

- Útočník: subjekt, který přenášené zprávy buď odposlouchává (tzv. pasivní útočník) nebo je modifikuje (tzv. aktivní útočník).
- Odposlechem zpráv může útočník získat důvěrné informace (např. výrobní tajemství) a ty pak využít ve svůj prospěch. Modifikací předávaných zpráv (např. platební příkaz bance) může útočník dosáhnout takového chování adresáta, které mu přinese prospěch.
- Důvěrnost zprávy: stav, kdy informace v přenesené zprávě je známa pouze oprávněným subjektům.
- Autentičnost zprávy: stav, kdy zpráva zaručeně pochází od udávaného původce, vznikla v udávaném čase a během svého přenosu nebyla pozměněna.



Ochrana zpráv

- Ochrana zpráv: opatření k zajištění důvěrnosti a autentičnosti zpráv.
- Typy ochran:
  - řízení přístupu ke kanálu (access control),
  - skrytí přenosového kanálu (steganografie),
  - eliminace parazitních kanálů (EMSEC resp. TEMPEST),
  - transformace zpráv:
    - -- překladové (např. kódová kniha),
    - -- matematické (kryptografie).



Kryptologie

- Matematická transformace zprávy: zpráva je chápána jako posloupnost čísel a s těmito čísly jsou prováděny matematické transformace.
- K praktickému provedení těchto a případně inverzních transformací je nutná znalost nějakého tajného parametru, tzv. klíče.
- Útočník, který klíč nezná, není schopen transformované zprávě porozumět nebo ji cílevědomě modifikovat.
- Kryptografie: věda o konstrukci matematických metod určených k zajištění důvěrnosti a autentičnosti zpráv.
- Kryptoanalýza: věda o překonávání matematických metod určených k zajištění důvěrnosti a autentičnosti zpráv.
- Kryptologie: věda zastřešující kryptografii i kryptoanalýzu.

Kryptografický systém pro zajištění důvěrnosti zpráv

- Utajovací kryptosystém (šifra): kryptografický systém pro zajištění důvěrnosti zpráv.
- Kryptogram *C*: transformovaná zpráva *Z*.
- K_E: šifrovací klíč.
- K_D: dešifrovací klíč.
- Transformace E (šifrování): prostá funkce $C = E(Z, K_E)$.
- E je konstruována tak, aby útočník s předpokládanou úrovní možností nebyl schopen z kryptogramu odvodit zprávu dříve, než-li je stanovená doba *T* rezistence kryptogramu.
- Transformace D (dešifrování): funkce $Z = D(C, K_D)$. Inverzní funkce k šifrování.

Typy utajovacích kryptosystémů

- Platí, že $K_D = f(K_E)$, respektive $K_E = f^{-1}(K_D)$.
- Typy utajovacích kryptografických systémů:

  - symetrické utajovací kryptosystémy,

  - asymetrické utajovací kryptosystémy.
- Symetrický kryptosystém (kryptosystém s tajným klíčem): K_D lze z K_E odvodit v rámci doby T. Oba klíče musí proto být tajné. Zpravidla platí $K_D = K_E = K$.
- Asymetrický kryptosystém (kryptosystém s veřejným klíčem): K_D nelze z K_E odvodit v rámci doby T. Klíč K_E tak může být veřejný (tzv. veřejný klíč *VK*) a utajit je zapotřebí jen dešifrovací klíč K_D (tzv. soukromý klíč *SK*).
- Vlastnosti:

  - symetrické: (+) rychlé (šifrování/dešifrování až Gb/s),

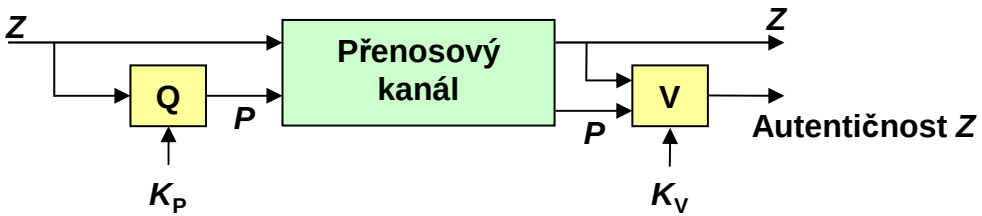
    (-) složitější distribuce klíčů (oba musí zůstat tajné),

  - asymetrické: (+) jednodušší distribuce klíčů (jen veřejný),

    (-) pomalejší než symetrické (cca 10^3-krát).

Kryptografický systém pro zajištění autentičnosti zpráv

- Autentizující kryptosystém: kryptografický systém pro zajištění autentičnosti zpráv.
- Pečeť *P*: posloupnost čísel umožňující ověřit autentičnost zprávy *Z*. Pro pečeť se používají různá označení (MAC, MIC, ICV, DS ...).
- K_P: pečetící klíč.
- K_V: verifikační klíč.
- Transformace Q (pečetění): funkce $P = Q(Z, K_P)$.
- Q je konstruována tak, aby útočník s předpokládanou úrovní možností nebyl schopen k libovolné zprávě odvodit správnou pečeť dříve, než-li je stanovená doba *T* rezistence.
- Transformace V (ověření): funkce $V(Z, P, K_V)$ = Ano/Ne. Umožňuje ověřit zda je přijatá zpráva autentická, či nikoliv.



Typy autentizujících kryptosystémů

- Platí, že $K_P = f(K_V)$, respektive $K_V = f^{-1}(K_P)$.
- Typy autentizujících kryptografických systémů:

  - symetrické autentizující kryptosystémy,

  - asymetrické autentizující kryptosystémy.
- Symetrický kryptosystém (kryptosystém s tajným klíčem): K_P lze z K_V odvodit v rámci doby T. Oba klíče musí proto být tajné. Zpravidla platí $K_P = K_V = K$.
- Asymetrický kryptosystém (kryptosystém s veřejným klíčem): K_P nelze z K_V odvodit v rámci doby T. Klíč K_V tak může být veřejný a utajit je zapotřebí jen pečetící klíč K_P (soukromý klíč).
- Vlastnosti:

  - symetrické: (+) výpočetně nenáročné,

    (-) složitější distribuce klíčů (oba musí zůstat tajné),

  - asymetrické: (+) jednodušší distribuce klíčů (jen veřejný),

    (+) nepopiratelnost zodpovědnosti,

    (-) výpočetně náročnější.

Typy autentizujících kryptosystémů

- Platí, že $K_P = f(K_V)$, respektive $K_V = f^{-1}(K_P)$.
- Typy autentizujících kryptografických systémů:

  - symetrické autentizující kryptosystémy,

  - asymetrické autentizující kryptosystémy.
- Symetrický kryptosystém (kryptosystém s tajným klíčem): K_P lze z K_V odvodit v rámci doby T. Oba klíče musí proto být tajné. Zpravidla platí $K_P = K_V = K$.
- Asymetrický kryptosystém (kryptosystém s veřejným klíčem): K_P nelze z K_V odvodit v rámci doby T. Klíč K_V tak může být veřejný a utajit je zapotřebí jen pečetící klíč K_P (soukromý klíč).
- Vlastnosti:

  - symetrické: (+) výpočetně nenáročné,

    (-) složitější distribuce klíčů (oba musí zůstat tajné),

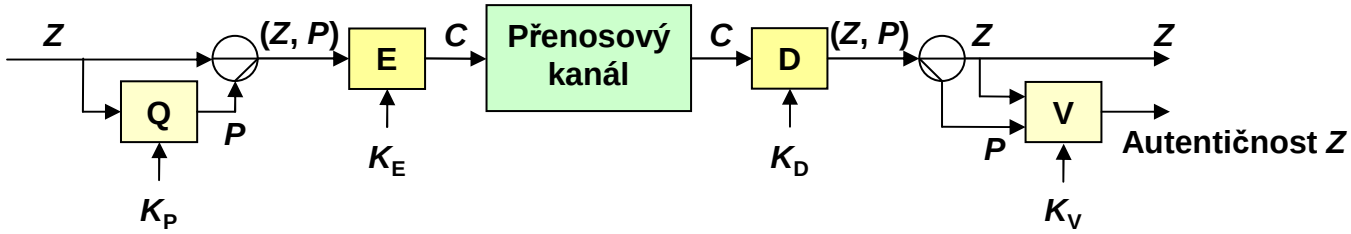
  - asymetrické: (+) jednodušší distribuce klíčů (jen veřejný),

    (+) nepopiratelnost zodpovědnosti,

    (-) výpočetně náročnější.

Utajovací a autentizující kryptosystém

- Utajovací a autentizující kryptosystém: zajišťuje jak důvěrnost tak i autentičnost přenášených zpráv.
- Zpravidla se realizuje jako kombinace utajovacího a autentizujícího kryptosystému.
- Nejčastější varianta je šifrování autentizované zprávy, kdy se zpráva *Z* nejprve opatří pečetí *P* a adresátovi se zašle zašifrovaná dvojice (*Z*, *P*).



- Někdy se požívá i varianta autentizování zašifrované zprávy, kdy se zpráva *Z* nejprve zašifruje do podoby kryptogramu *C* a ten se opatří pečetí *P.*

Matematika v kryptografii

- Kryptografie je věda o konstrukci matematických metod určených k zajištění důvěrnosti a autentičnosti zpráv.
- Kryptografie má v praktickém životě řadu aplikací (internetové bankovnictví, autentizace uživatelů v mobilních sítích, digitální podepisování dokumentů, šifrování filmů na DVD apod.).
- Kryptografie tak nabízí spoustu příležitostí jak zatraktivnit výuku matematiky.
- Zakomponování kryptografických aplikací do výuky matematiky umožní studentům matematické poznatky hlouběji pochopit.
- Zároveň je může motivovat k dalšímu studiu matematiky s cílem porozumět praktickým aplikacím kryptografie.
- Potenciál kryptografie pro výuku matematiky lze ilustrovat na kryptosystému RSA.

Asymetrický kryptosystém RSA

- Jeden z nejčastěji používaných asymetrických kryptosystémů.
- Tvorba kryptosystému RSA:

1) Volba dvou velkých prvočísel p a q ($>10^{115}$),
2) Výpočet modula $n = p \cdot q$,
3) Výpočet čísla $r = (p-1) \cdot (q-1)$,
4) Volba veřejného klíče VK. Musí být nesoudělný s r.
5) Výpočet soukromého klíče SK z podmínky: $(VK \cdot SK) \bmod r = 1$.
6) Zveřejnění VK a n. Ostatní parametry jsou tajné.

- Varianta utajovacího kryptosystému:
  - šifrování: $C = Z^{VK} \bmod n$, přičemž $Z < n$,
  - dešifrování: $Z = C^{SK} \bmod n$.
- Varianta autentizujícího kryptosystému (digitální podpis):
  - podepsání Z: $S = Z^{SK} \bmod n$, přičemž $Z < n$,
  - ověření podepsané zprávy (Z, S): $S^{VK} \bmod n = Z$.

Bezpečnost RSA

- Útočník:

  1) zná veřejné parametry VK a n,

  2) ví, že $(VK \cdot SK) \bmod r = 1$,

  3) ví, že $r = (p-1)\cdot(q-1)$,

  4) a, že $n = p \cdot q$.

  (Pozn.: modré parametry jsou známé a červené jsou neznámé.)
- Pokud je útočník schopen ze 4) faktorizovat číslo n na prvočísla p a q, tak je ze 3) schopen určit r a nakonec ze 2) i soukromý klíč SK.
- Bezpečnost kryptosystému RSA tedy závisí na praktické nemožnosti faktorizovat velká čísla n (Integer Factorization - IF).
- Za bezpečné se v současné době považuje n = 768/1024/2048 bit.

- RSA tak lze využít u výkladu prvočísel, faktorizace čísel, modulární aritmetiky, malé Fermatovy věty, rozšířeného Euklidova algoritmu atd.

Závěr

- Kryptografie se zabývá konstrukcí matematických metod pro zajištění důvěrnosti a autentičnosti zpráv.
- S aplikacemi kryptografie se studenti běžně ve svém životě setkávají (autentizace uživatele v počítačové síti, digitální podpis e-mailu, internetové bankovnictví apod.).
- Kryptografie tak nabízí zajímavou možnost jak zatraktivnit středoškolskou i vysokoškolskou výuku matematiky.

- Využitelná literatura:

[1] A. J. Menezes - P. C. Oorschot - S. A. Vanstone: Handbook of Applied Cryptography.CRC Press, N. York 1996.

http://www.cacr.math.uwaterloo.ca/hac/

[2] Stallings, W.: Cryptography and Network Security. Pearson Education, Upper Saddle River 2006.

[3] Levický, D.: Kryptografia v informačnej bezpečnosti. Elfa, Košice 2005.