EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Symetrická, asymetrická a hybridní kryptografie. Klasifikace šifer.

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

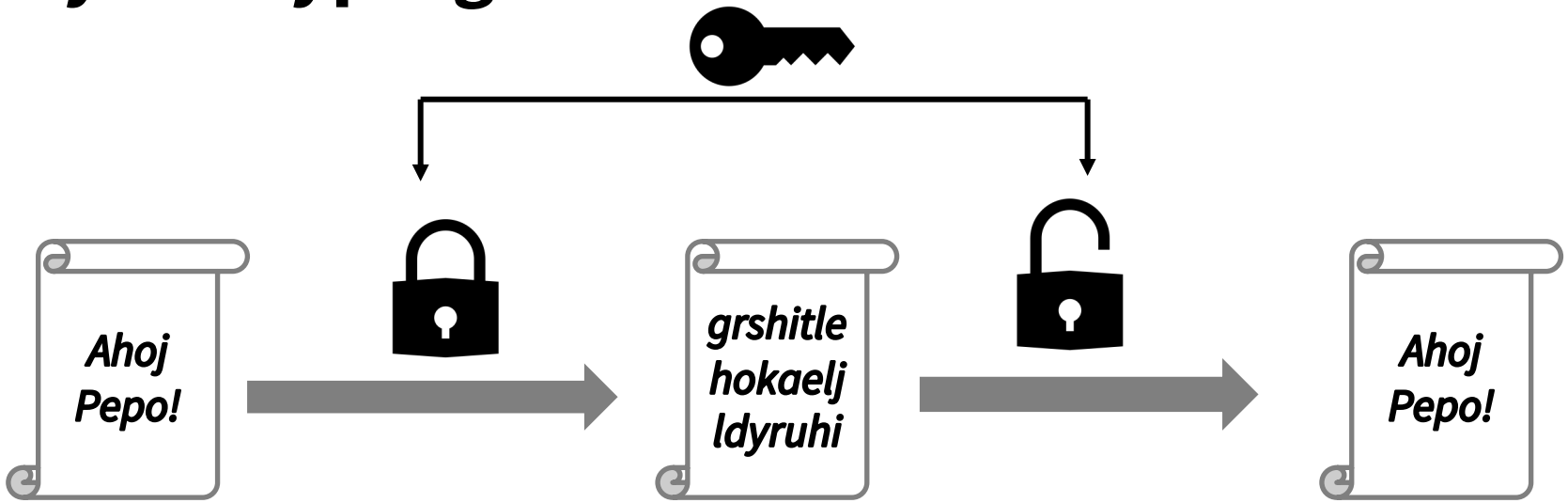
Doc. Ing. Roman Šenkeřík, Ph.D. FAI,
Ústav informatiky a umělé inteligence

Obsah prezentace

- Symetrická kryptografie.
- Asymetrická kryptografie.
- Hybridní kryptografie.
- Rozdělení šifer.

1. Symetrická kryptografie

Schéma sym. kryptografie



- Symetrická kryptografie představuje nejstarší a nejjednodušší systém.
- Jeden klíč (symetrický, konvenční) je použit pro obě operace – tedy šifrování i dešifrování, které je většinou jen přímou inverzí šifrovacího algoritmu.
- Všechny historické klasické šifry jsou symetrické.

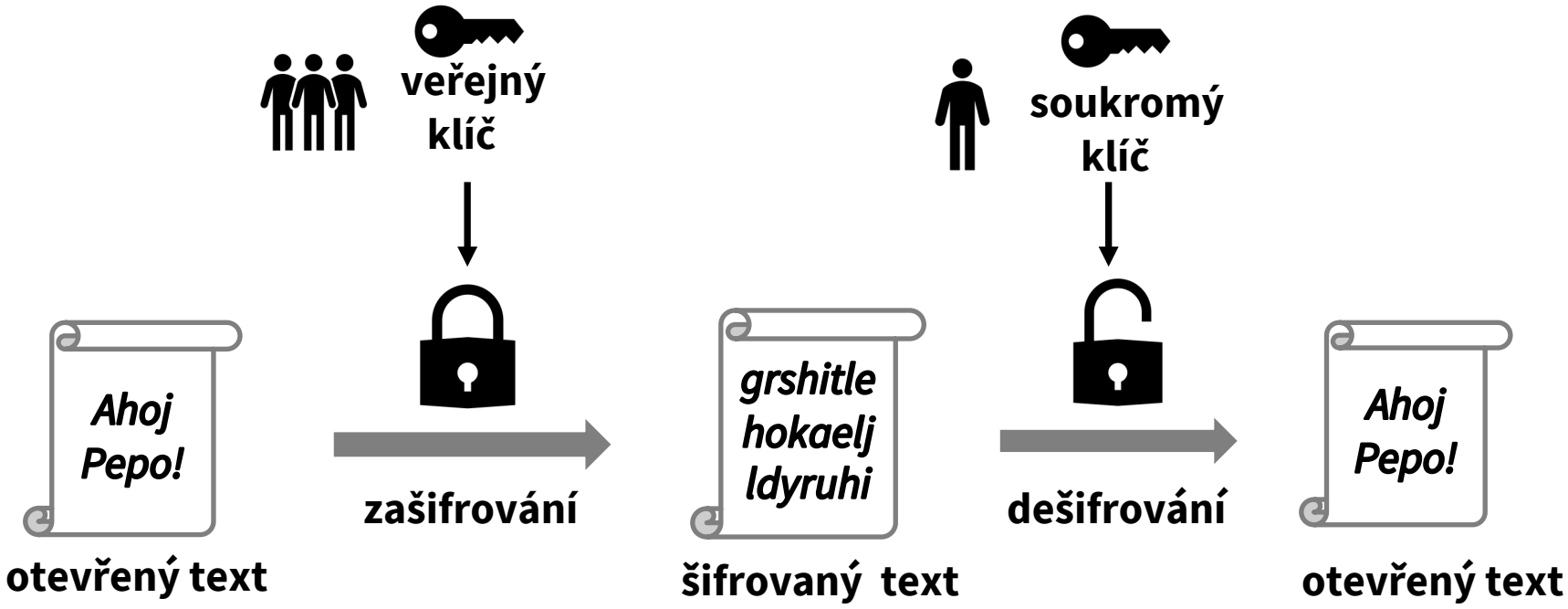
Symetrická kryptografie: Výhody a nevýhody

- **Výhody:**
  - Jednoduchost šifrovacího a dešifrovacího algoritmu.
  - Rychlé algebraické/binární operace často opakované v iteracích.
  - Rychlost (stovky i více Mbit/s).

- **Nevýhody:**
  - Nutnost sdílení/přenosu klíče předem nebo při inicializaci komunikace jiným zabezpečeným kanálem (sms, osobní domluva, jiné algoritmy a workflow).
  - Při komunikaci s více účastníky, nutnost velkého množství klíčů - dáno krypto pravidly.

2. Asymetrická kryptografie

Schéma asym. kryptografie



- Moderní alternativa k symetrickým systémům (použitelná v mnoha moderních aplikacích).
- Využití asymetrického klíčového páru.

Asymetrická kryptografie: Výhody a nevýhody

- **Výhody**
  - Odpadá nutnost přenosu/sdílení klíče před inicializací komunikace.
  - Pro více uživatelů není potřeba tolik klíčů – v tomto případě stačí jeden klíčový pár.

- **Nevýhody**
  - Velmi vysoké výpočetní nároky (komplikovaný matematický vztah mezi klíči a zejména pak šifrovací a dešifrovací funkce pracující s umocněním a mod funkcí pro velmi velké čísla.
  - Nízká rychlost a nepraktičnost pro datové přenosy (cca 100x pomalejší než symetrická).
  - Nutnost dobře zabezpečit a kontrolovat veřejný klíč - od toho máme certifikáty a digitální podpisy (jednoduchý útok - výměna veřejného klíče).

3. Hybridní kryptografie

Hybridní šifrování - princip

- Asymetrické šifrování má jednu velkou nevýhodu. Je velmi náročné na matematické operace, tedy i na výkon počítače. V praxi se proto používá kombinace symetrického a asymetrického šifrování.

- Využijeme výhod obou: rychlost symetrického šifrování a „použitelnost" asymetrického šifrování.

Hybridní šifrování - princip

- Kombinace výhod z obou symetrických a asymetrických systémů
  - “Hlavní” data (velká velikost) jsou šifrovány rychlou symetrickou šifrou
  - Klíč k symetrické šifře (symetrický či konvenční klíč) je pak zašifrován asymetrickou šifrou
  - Obě části (zašifrovaná data a zašifrovaný symetrický klíč) jsou spojeny do jednoho balíku a odeslány
- Naprosto běžný standard HTTPS, FTPS, SSH, SSL protokolů
- Prvním nejrozšířenějším systémem byl PGP (Open PGP) - *Pretty Good Privacy*

PGP - princip

- *Pretty Good Privacy* („velmi dobré soukromí“)
- Jeden z nejznámějších a nejbezpečnějších šifrovacích algoritmů
- Vznik 1991, autor Phil R. Zimmermann
- *Zajímavost: Po vzniku platil zákaz vyvážení programu mimo hranice USA z důvodu jeho kvalit a byl řazen do podobné kategorie jako například zbraně.*

PGP: Postup šifrování

- Úplně nejdříve je původní text (plaintext) zkomprimován. Pro kompresi je vyžita FREEWARE rutina PKZIP verze 2.x

- Při každém šifrování jakéhokoli dokumentu je prvně náhodně vygenerován konvenční (symetrický) klíč.
- Tímto klíčem je zašifrovaný zkomprimovaný vlastní dokument (symetrická šifru, proces je velmi rychlý). PGP využívá tři druhy symetrických algoritmů. Všechny tři pracují s 64-bitovými bloky. Jedná se o CAST, Triple-DES a IDEA. Tyto byly vytvořeny mimo PGP a do PGP pouze přidány. CAST a IDEA používají 128-bitové klíče, Triple-DES používá 168-bitový klíč [1].

PGP: Postup šifrování

- Dalším krokem je zašifrování symetrického klíče klíčem veřejným. Zde se již jedná o pomalejší proces, ale jelikož je délka symetrického klíče relativně malá, jde to velmi rychle.

- Obě tyto části jsou spojeny do jednoho souboru, a teprve potom se jedná o PGP zašifrovaná data.

PGP: schéma šifrování

*Samozřejmě zašifrováno ne zakódování

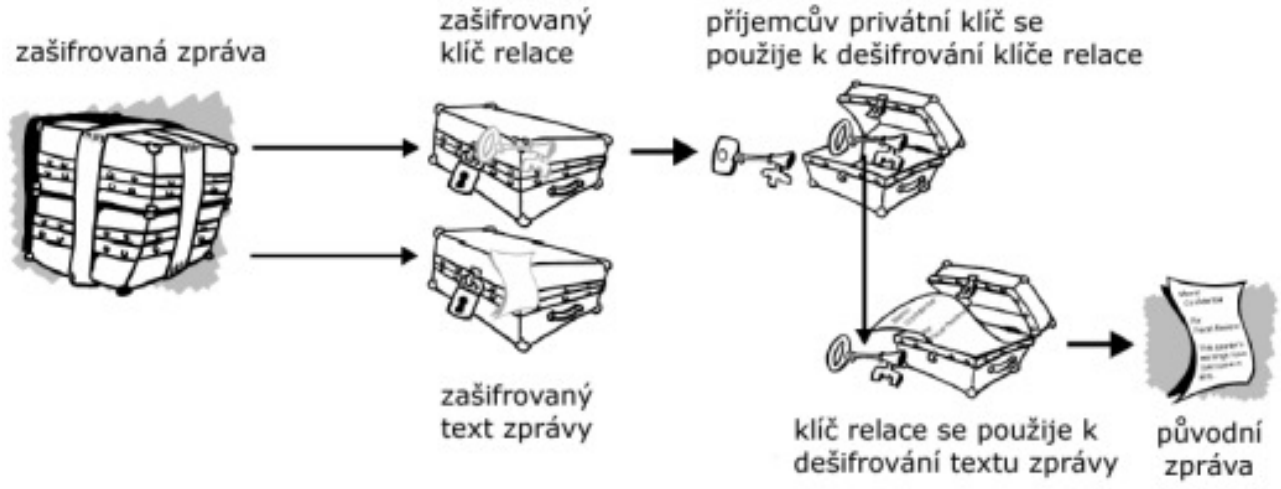
Zdroj: [2]

PGP: Postup dešifrování

Dešifrování probíhá inverzně k již popsanému procesu zašifrování.

- Prvně je balík rozdělen na zašifrovaný text a zašifrovaný konvenční klíč.
- Konvenční klíč je „odšifrován“ privátním klíčem.
- Konvenční klíč je pak použit k dešifrování textu.
- Text/data je nakonec dekomprimován a konečně čitelný.

Schéma dešifrování



Zdroj: [2]

Další příklady hybridních systémů - TLS

Transport Layer Security (TLS) je základní kryptografický protokol zajišťující zabezpečenou komunikaci na internetu. Zahrnuje tři základní fáze [3]:

1. Dohodu účastníků na podporovaných algoritmech

2. Výměnu klíčů založenou na šifrování s veřejným klíčem a autentizaci vycházející z certifikátů

3. Šifrování provozu symetrickou šifrou

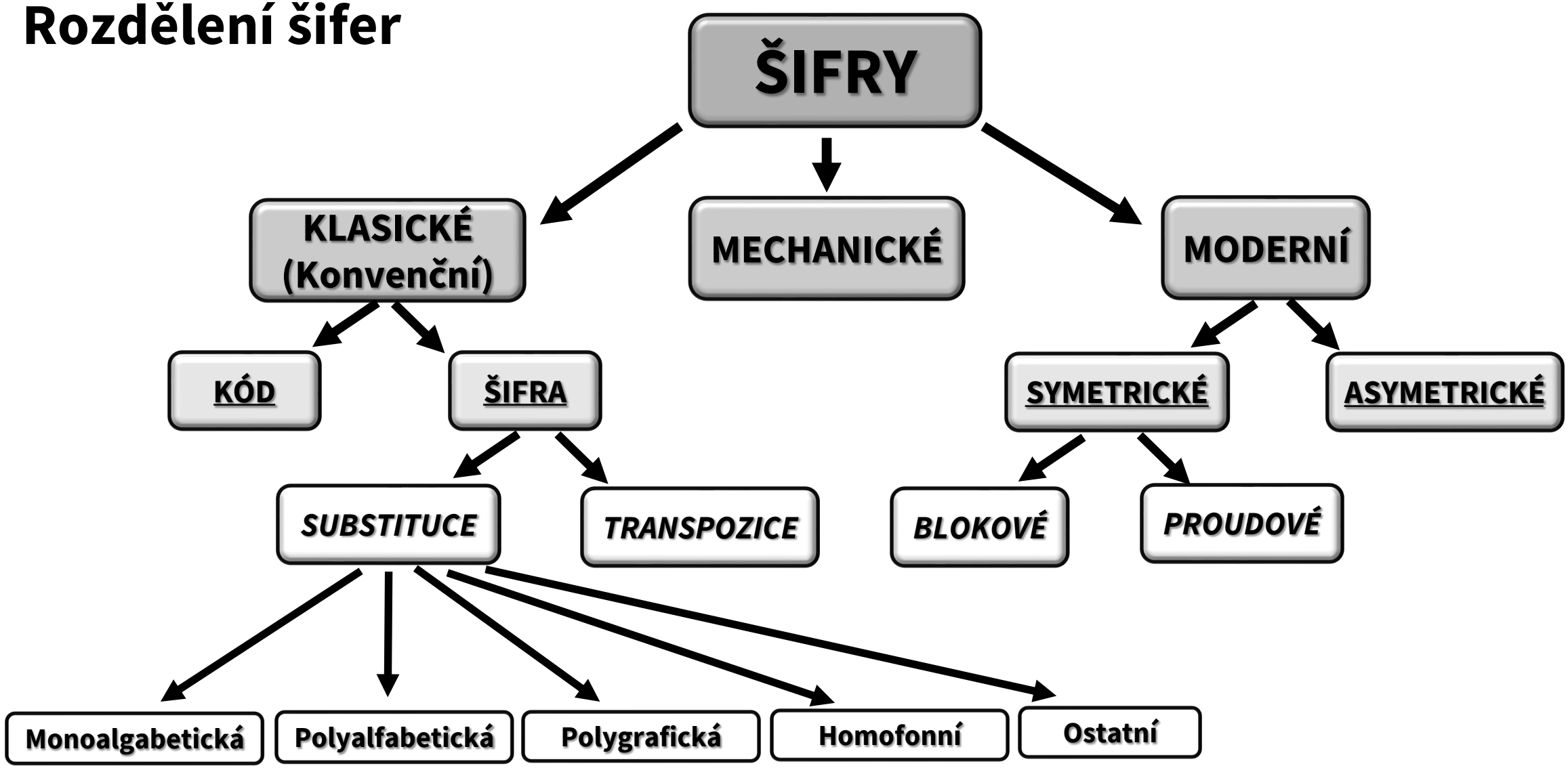
Další příklady hybridních systémů - TLS

Během první fáze se klient a server dohodnou na používaných kryptografických algoritmech. Současné implementace podporují následující možnosti:

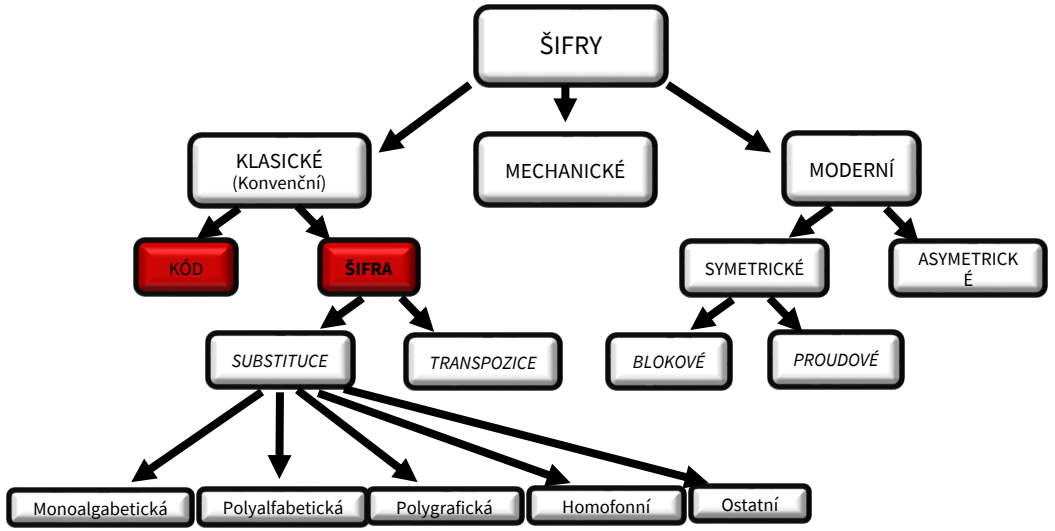
- pro kryptografii s veřejným klíčem: RSA, Diffie- Hellman, DSA
- pro symetrické šifrování: RC2, RC4, IDEA, DES, Triple DES, AES, Camellia
- pro jednosměrné hešování: Message-Digest algorithm (MD2, MD4, MD5), Secure Hash Algorithm (SHA-1, SHA-2)

4. Rozdělení šifer

Rozdělení šifer



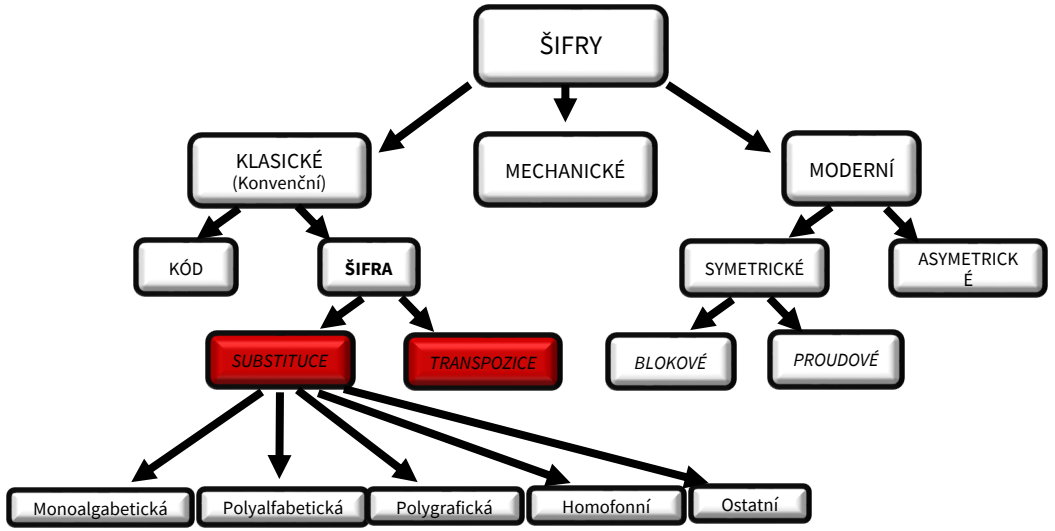
Rozdělení šifer



- **KÓD**
  - Jedná se o jednoduchý systém „bez algoritmu“
  - Příkladem je např. kódová kniha = slovník, která se často měnila.
  - Např. *AB28* znamenalo: je třeba zaútočit dnes v 20:00 večer.

- **ŠIFRA**
  - Zde se již jedná o systémy s jednoznačnou algoritmickou strukturou a logikou

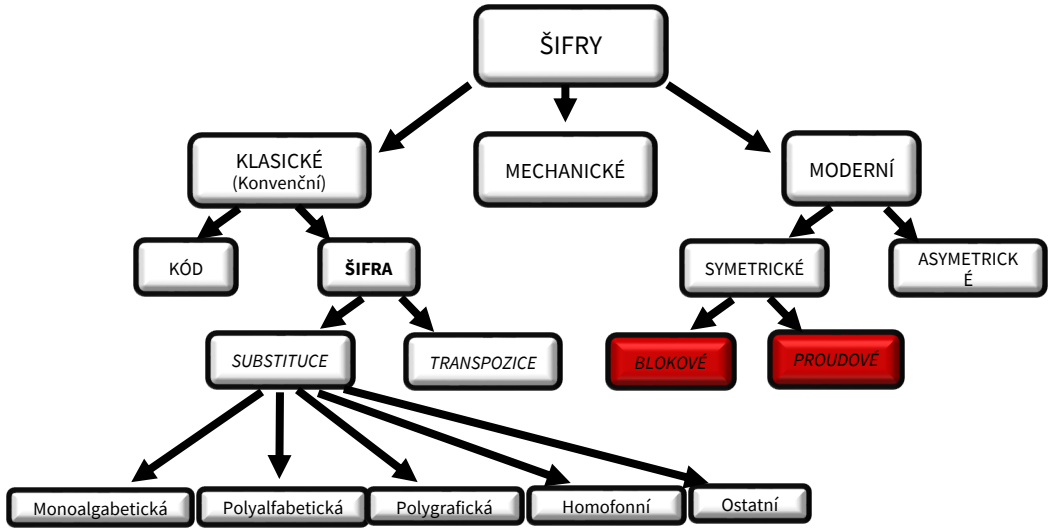
Rozdělení šifer



- **SUBSTITUCE**
  - Z matematické „substituce“ = nahrazení.
  - Systémy, kde je abeceda OT substituována za jinou (jednu nebo více) abeced ŠT.
  - Pořadí znaků ovšem zůstane zachováno. Tj. znak, který je na prvním místě v OT je na prvním místě i v ŠT.

- **TRANSPOZICE**
  - Jedná se o „prosté“ přeskupení znaků (někdy označováno jako permutace, nebo reshuffling).
  - Abeceda OT i ŠT zůstává neměnná.

Rozdělení šifer



- **BLOKOVÉ**
  - Moderní symetrické systémy pro šifrování datových souborů.
  - Data jsou rozdělena do bloků konstantní délky a následně zpracována.

- **PROUDOVÉ**
  - Symetrické systémy, které využívají filozofie šifrování tzv. bit po bitu.
  - Aplikace pro přenos telekomunikací/datastreamů.

Seznam odkazů

[1] How PGP works. [online]. Dostupné z: https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html#p10

[2] Moderní metody šifrování. [online]. Dostupné z: https://pctuning.tyden.cz/software/ochrana-soukromi/4711-moderni_metody_sifrovani

[3] Transport Layer Security. [online]. Dostupné z: https://cs.wikipedia.org/wiki/Transport_Layer_Security

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204