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

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Kryptologie

Moderní kryptologie: Protokoly výměny klíčů

Základy asymetrické kryptografie

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

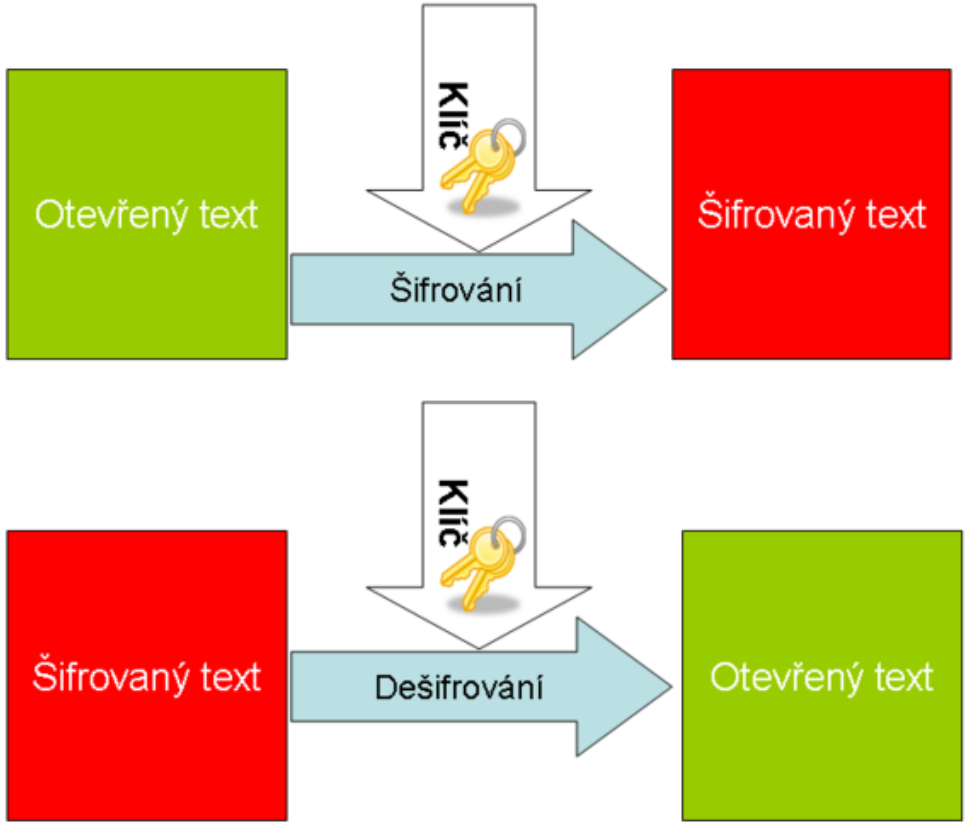
Obsah prezentace

- Úvod do asymetrické kryptografie
- Jednosměrné (jednocestné) funkce
- Protokoly tvorby a výměny klíčů
- Hash funkce

1. Úvod do asymetrické kryptografie

Asymetrická kryptografie: Úvod

Symetrická kryptografie – schéma



Asymetrická kryptografie: Úvod

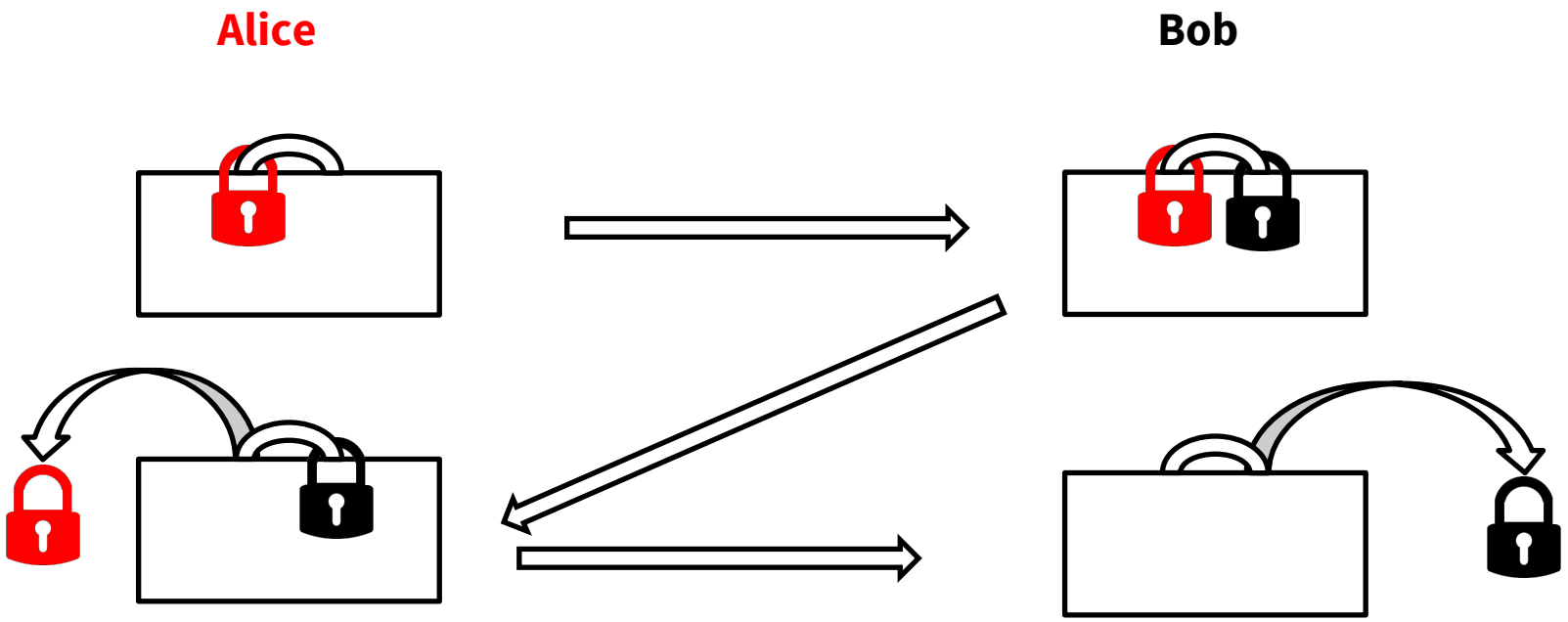
Symetrická kryptografie

- Proč se symetrická kryptografie nazývá symetrická?
- V čem spočívá její symetrie a velká nevýhoda?

Asymetrická kryptografie: Úvod

Myšlenka, která inspirovala asymetrickou kryptografii:

- Alice i Bob potřebují mít jistotu, že po cestě nikdo nepovolaný jejich kufr neotevře.



Asymetrická kryptografie: Úvod

To znamená, že budeme potřebovat 2 různé klíče:

Klíč Alice: 

Klíč Boba: 

Asymetrická kryptografie: Úvod

Asymetrická kryptografie je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají **odlišné klíče**.

- Použití:
  - Utajená komunikace
  - Elektronický podpis (možnost u dat prokázat jejich autora)
  - Bezpečná výměna symetrických klíčů
- Nevhodné pro velké objemy dat.

Asymetrická kryptografie: Úvod

Asymetrické šifrování využívá dvojice klíčů a to **veřejný** a **soukromý**:

- **veřejný**
  - je přístupný všem,
- **soukromý**
  - je dostupný jen tomu, kdo má právo šifrovanou zprávu dešifrovat.

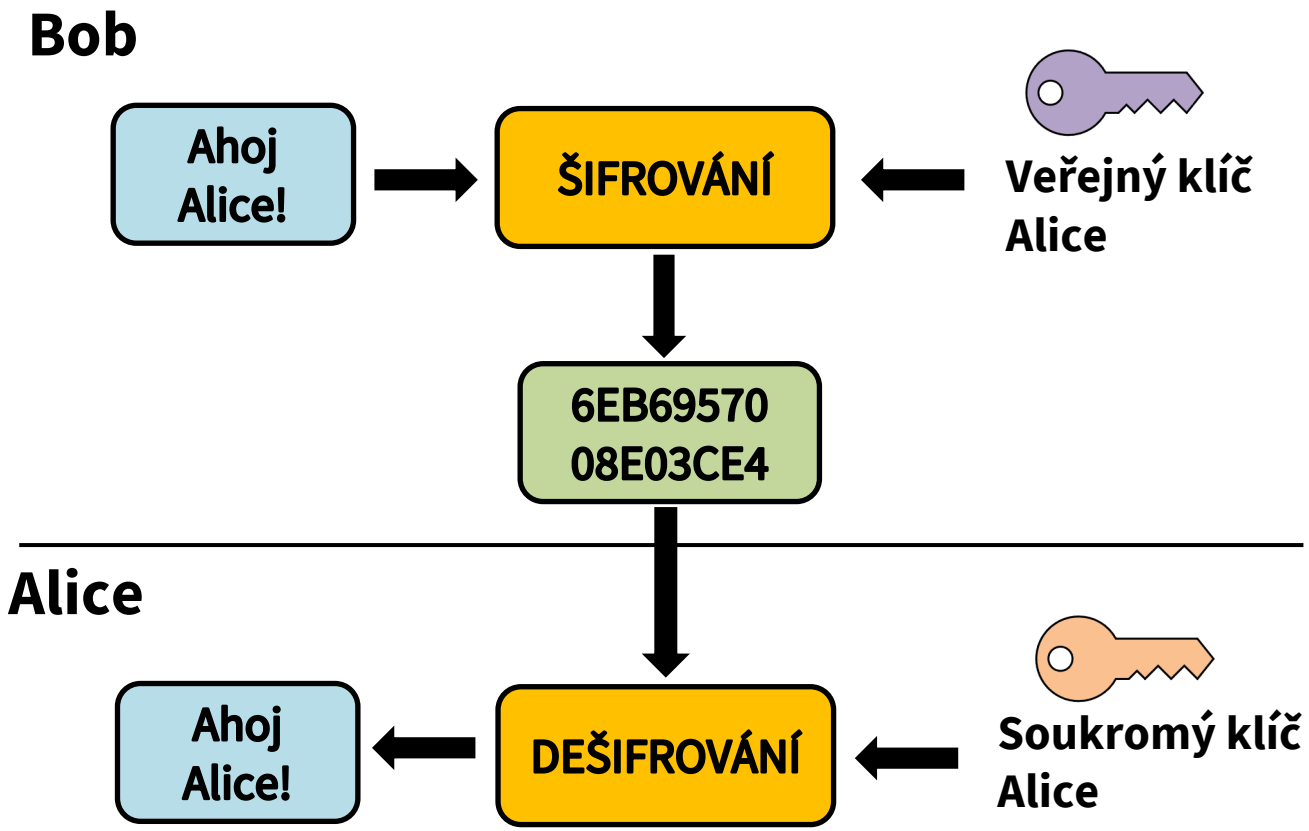
Asymetrická kryptografie: Úvod

- **Veřejný klíč** je umístěn např. na serveru, nebo je zaslán účastníkům e-mailové komunikace.
- **Soukromý klíč** je dostupný pouze majiteli těchto klíčů (soukromý, veřejný).
- Asymetrické šifrování má proti symetrickému jednoduché klíčové hospodářství.

Asymetrická kryptografie: Princip

- Člověk, který hodlá poslat zprávu (šifrovaně) si vyžádá **veřejný** šifrovací klíč příjemce, tímto zprávu zašifruje, a takto zašifrovanou ji odešle.
- Příjemce jakožto **jediný** vlastník svého **soukromého** klíče zprávu dešifrujete.
- Pokud se někdo jiný se svým soukromým klíčem pokusí dopis dešifrovat, vypadne mu po dešifrování holý nesmysl ve formě nespecifikovaného shluku znaků, tzv. „rozsypaný čaj“.

Asymetrická kryptografie: Schéma



Asymetrická kryptografie – mechanismy

Asymetrická kryptografie je založena na tzv. **jednocestných funkcích**, což jsou operace, které lze snadno provést pouze v jednom směru:

- ze vstupu lze snadno spočítat výstup, z výstupu je však velmi obtížné nalézt vstup.

Asymetrická kryptografie

Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče.

- Vznik v roce 1975 (Whitfield Diff a Martin Hellman)

Asymetrická kryptografie

- Využívají principů jednosměrných funkcí - nejběžnějším příkladem je například násobení: je velmi snadné vynásobit dvě i velmi velká čísla, avšak rozklad součinu na činitele (tzv. faktorizace) je velmi obtížný.

- Síla této šifry spočívá v tom, že dosud nebyla objevena metoda, jak rozložit velká čísla na prvočísla - faktorizace. V danou chvíli není ani zcela jisté zda je vůbec možné takovouto metodu objevit. Pokud se tak ovšem stane, bude tato šifra nepoužitelná. Stále tak na poli výzkumu dochází k hledání nástupce.

Asymetrická kryptografie: Algoritmy

- RSA – nejpoužívanější
- ElGamal - Šifrovaná data jsou dvakrát větší než data nešifrovaná. To je důvodem, menšího nasazení. ElGamal spoléhá na problém výpočtu diskrétního logaritmu.
- DSA (Digital Signature Algorithm) - je standard Americké vlády pro digitální podpis. Byl navržen Americkým institutem NIST v roce 1991 pro použití v protokolu DSS (Digital Signature Standard) používaný od roku 1993.
  - Poslední úpravou prošel v roce 2000 a nyní je veden jako jako FIPS 186-2

2. Jednocestné (one-way) funkce

One-way functions - Jednosměrné funkce
Jednoduché aplikace

- Jsou to funkce kterou je snadné spočítat a všeobecně se věří, že je jí těžké invertovat, bez dodatečné informace navíc (vodítko – privátní klíč). Níže jsou uvedené demonstrativní příklady [1]:

- Jednosměrné funkce s padacím zámkem (trapdoor) - příkladem poštovní schránka

- Míchání barev

- Telefonní seznam

3. Protokoly výměny klíčů

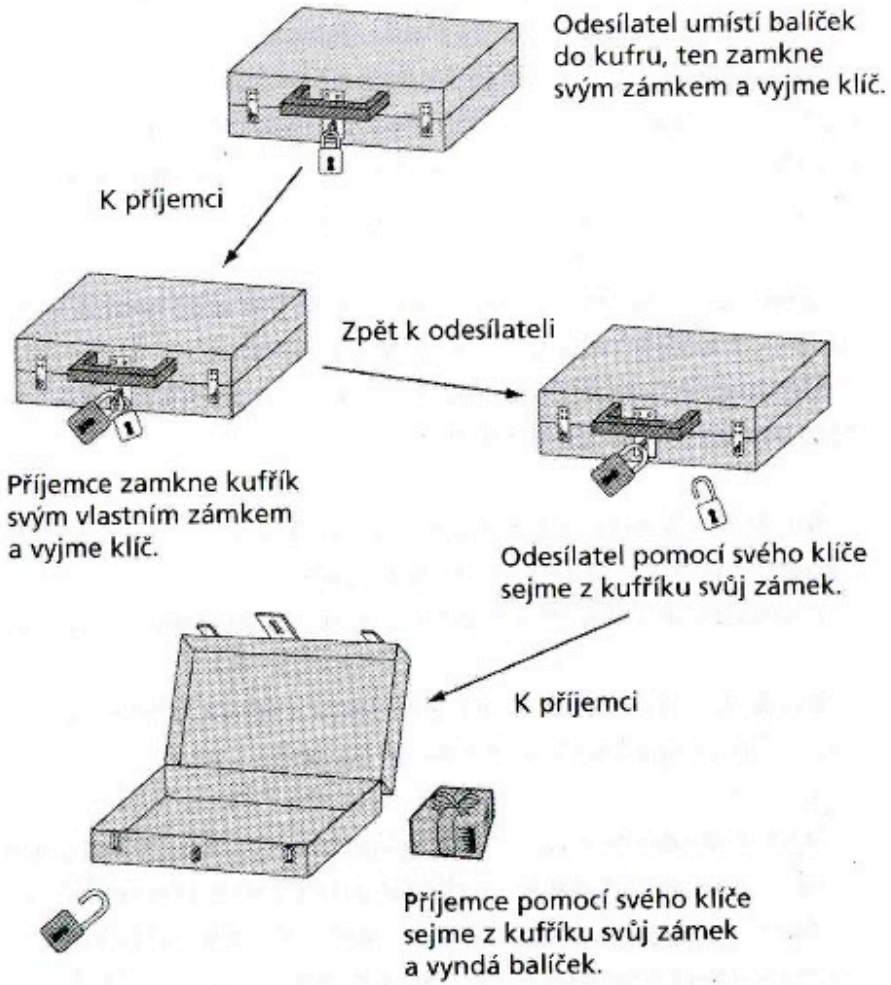
One-way functions – Kryptografické jednosměrné funkce

- Násobení a zpětná faktorizace (velkých) prvočísel
- Problematika Diskrétního logaritmu (DLP)
- Problematika Diskrétního logaritmu eliptických křivek (ECDLP)
- Komplexní Modulární aritmetika

Sdílení klíče - Shamirův Algoritmus

Tzv. kufříkový algoritmus.

Bude fungovat i digitálně?



Zdroj: [1]

Shamirův Three Pass Protocol - Popis

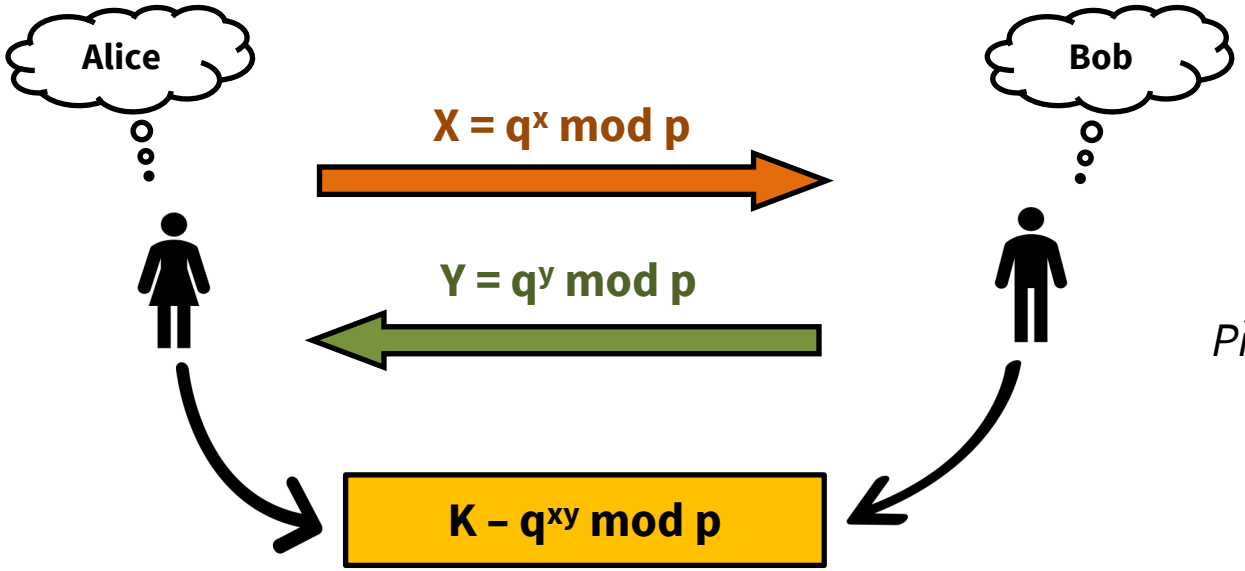
- Bude-li tajná zpráva m, Alicina šifrovací funkce E_A, dešifrovací funkce D_A, Bobova šifrovací funkce E_B a dešifrovací D_B, pak [1]:
  - Krok 1: Alice ➡ Bob $E_A(m)$
  - Krok 2: Bob ➡ Alice $E_B(E_A(m))$
  - Krok 3: Alice ➡ Bob $E_B(m) = D_A(E_B(E_A(m)))$
  - Krok 4: Bob: $m = D_B(E_B(m))$
- Nutná podmínka - použít komutativní funkce.
- Budou takovéto funkce poskytovat dostatečnou ochranu informace?

Diffie - Hellman Protokol

V současné době jeden z nejčastěji využívaných protokolů pro sestavení provozního klíče pro komunikaci na internetu..

- Cílem je sestavit sdílený symetrický klíč pro hlavní datový provoz
- Sestavení probíhá částečně asymetricky.
- Protokol je postaven na jednocestné funkci diskrétní logaritmus
- Pro zamezení útoku na tento protokol (man in the middle) je nutné aplikovat digitální podpisy a certifikáty pro autorizaci sdílených údajů.

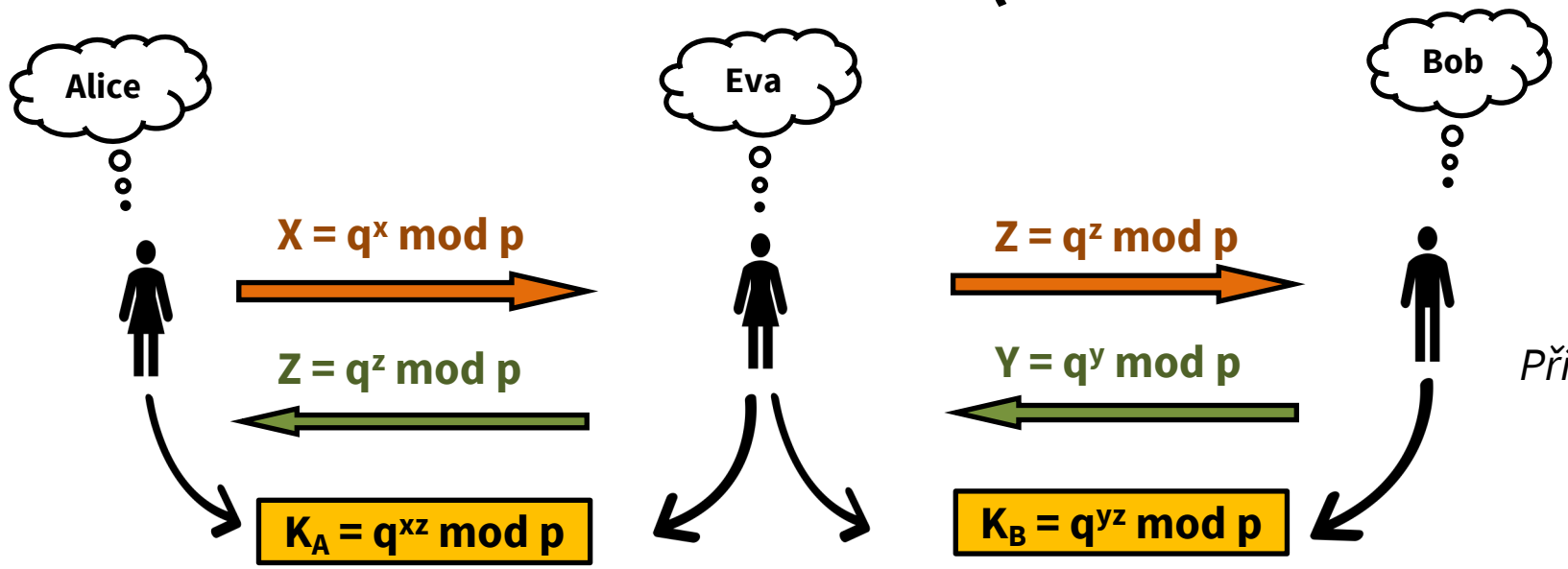
Diffie - Hellman Protokol



Příklad dle: [1]

- Oboustranná dohoda na velkém prvočíslu p a číslu q
  - Alice si zvolí tajné číslo x takové, že 0 < x < p-1 a vypočítá X, pošle Bobovi.
  - Bob si zvolí tajné číslo y takové, že 0 < y < p-1 a vypočítá Y, pošle Alici.
  - Alice vypočítá Yx mod p a Bob vypočítá Xy mod p a mají společný klíč

Útok na Diffie - Hellman Protokol (man in the middle)



Příklad dle: [1]

- Odchycení oboustranné dohody na p a q
- Zvolení vlastního čísla z
- Odchycení výpočtů X a Y
- “Podstrčení” falešného výpočtu s použitím z Bobovi i Alici
- Zachytávání a překryptovávání obousměrné komunikace

4. Hash funkce

Hash Algoritmy

- Vedle šifrování symetrickým a asymetrickým klíčem existuje ještě jedna oblast kryptografie, kde potřebujeme informaci pouze zahashovat, ale už nikdy dostat zpět.

- Příkladem je uložení hesel systému a kontroly integrity.

- Uživatel zadá např. heslo „pepa01“, toto heslo se zahashuje na něco nečitelného, například „t6x/Onm“, které se uloží do systému.

- Jelikož procedura hashování je stejná a neměnitelná, stejné heslo se vždy zahashuje na stejný výsledek. Tímto postupem docílíme toho, že systém nemusí znát heslo uživatele, stačí znát zahashovanou hodnotu.

Hash Algoritmy: Grafický princip

Zdroj: [2]

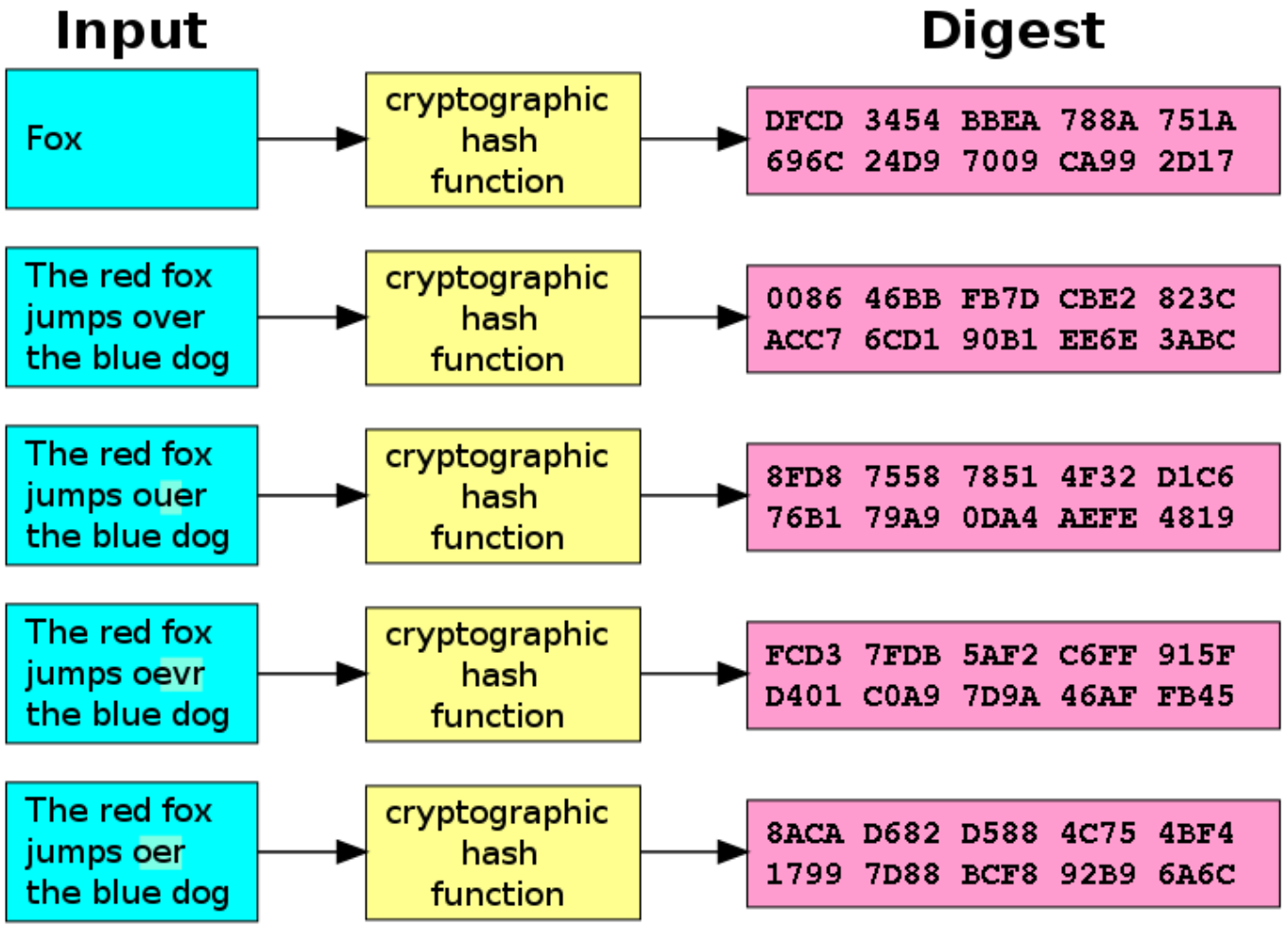
Kryptografické Hash Algoritmy

- Pro potřeby kryptografie musí být algoritmus hashování jednosměrný.
- Pozor neplést si to s jednocestou funkcí pro Asymetrickou kryptografii.
- Známe-li hodnotu hashe (a máme li rovněž původní dokument, ze kterého byla vypočítána), mělo by být velmi obtížné vytvořit jiný dokument se stejnou hashovací hodnotou.
- Pro útoky na HASH záznamy se používají tzv. Rainbow tabulky [3], [4].

Kryptografické Hash Algoritmy

- Doporučeným standardem pro délku hash funkce 160 bitů (a více), která se používá i pro digitální podpisy.
- Hash algoritmy umíme otestovat integritu textu, tj. máme informaci o tom, že daný text je původní.
- Hash je miniaturní otisk obsahu dokumentu. Při změně jen jednoho bitu zprávy se musí hodnota hashe změnit.

Kryptografické Hash Algoritmy - ukázka



Zdroj: [5]

Požadavky na Hash Algoritmy

- Na vstupu libovolná délka textu, na výstupu pevná délka.
- Jednosměrnost - nesmí být možné z Hashe odvodit původní zprávu.
- Bezkoliznost – nesmí být možné dostat na dvě různé výchozí zprávy stejnou hodnotu Hash.
  - Funkce je slabě bezkolizní, pokud k danému textu není výpočetně možné vymyslet jiný text, který bude mít stejný otisk.
  - Funkce je silně bezkolizní, pokud není výpočetně možné najít dva různé texty se stejným otiskem.

Požadavky na Hash Algoritmy

Mezi dnes běžně používané algoritmy patří SHA-2, SHA-256 a dříve populární MD5

- **MD5** – kontrola integrity souborů – rychlé otestování, jestli jsou dva soubory bez nutnosti porovnávat celé soubory (pozor - již byl prolomen!!!).

- **SHA** – nástupce MD5, navrhla jej organizace NSA (Národní bezpečnostní agentura v USA).
  - SHA-1, SHA-2, SHA-3

DSS – standard digitálního podpisu

- DSS - Digital Signature Standard, založen na DSA Digital Signature Algorithm (vznik 1991)
- Odesílatel před odesláním zprávy spočítá otisk této zprávy.
- Tento vypočítaný otisk zašifruje svým privátním klíčem a spolu s vlastní zprávou pošle příjemci.

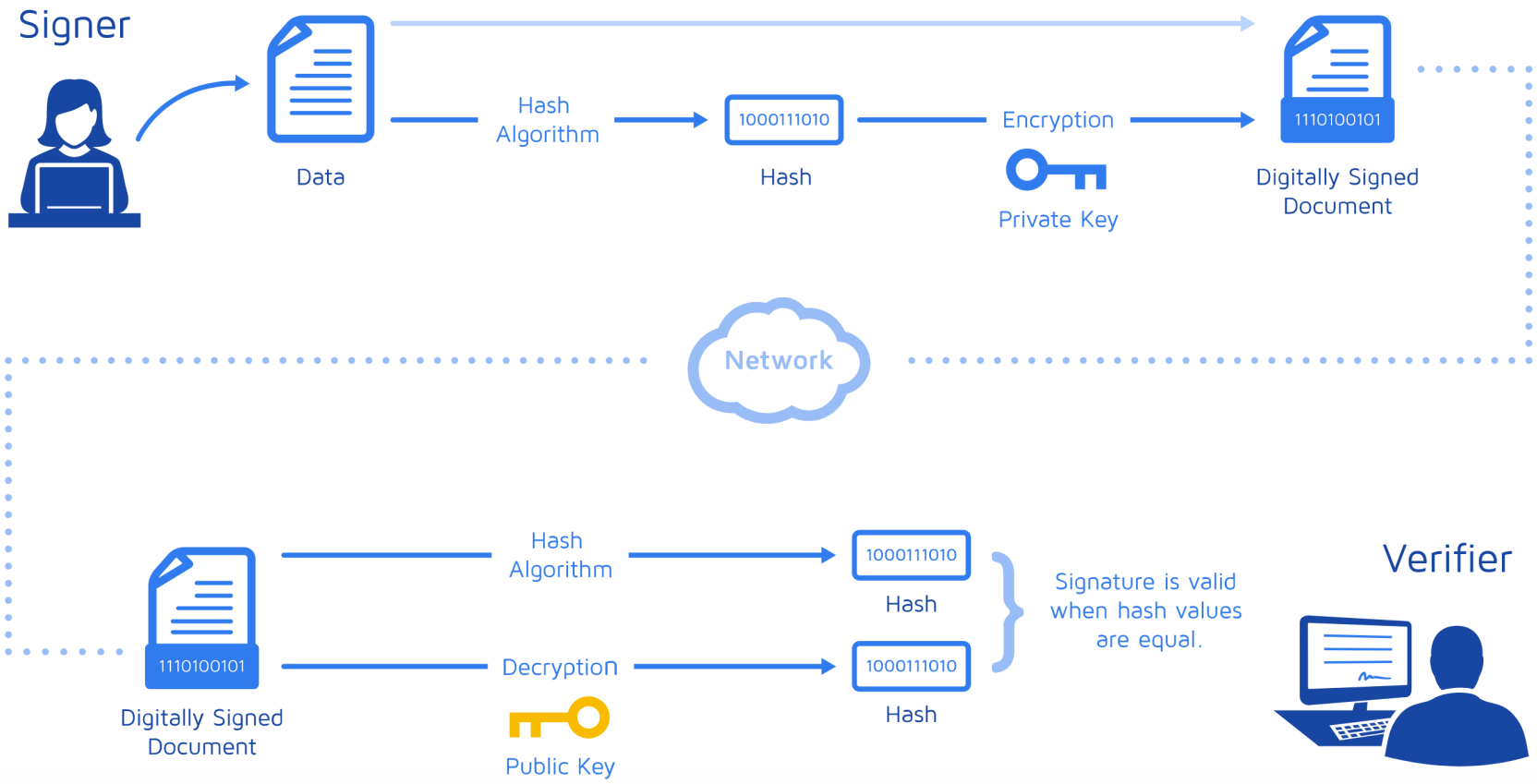
DSS - digitální podpis

- Příjemce vypočítá veřejným klíčem vysílače také otisk přijaté zprávy a porovná vypočítaný otisk s otiskem, který získal od příjemce.

- Pokud jsou oba otisky totožné, je tedy přijatá zpráva v takovém tvaru, v jakém ji vysílač skutečně poslal.

DSS - digitální podpis

- Standard digitálního podpisu



Zdroj: [6]

Seznam odkazů

[1] PIPER, F. C. a Sean MURPHY. Kryptografie. Praha: Dokořán, 2006. Průvodce pro každého. ISBN 80-7363-074-5.

[2] Základy moderní kryptologie – Symetrická kryptografie I. Vlastimil Klíma. [online]. Dostupné z: http:// crypto-world.info/klima/mffuk/Symetricka_kryptografie_I_2005.pdf

[3] Rainbow Tables. [online]. Dostupné z: https://en.wikipedia.org/wiki/Rainbow_table

[4] Rainbow tables tajemství zbavené. [online]. Dostupné z: https://www.soom.cz/clanky/1165--Rainbow-tables-tajemstvi-zbavene

[5] Cryptographic HASH functions. [online]. Dostupné z: https://commons.wikimedia.org/wiki/File:Cryptographic_Hash_Function.svg

[6] What are digital signatures, how it works. [online]. Dostupné z: https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq

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