**BI-SPOL-6 Asymetrické kryptosystémy (šifra RSA, Diffie-Hellman, RSA digitální podpis), hešovací funkce (SHA-2, HMAC)**

BI-BEZ

### Asymetrické kryptosystémy

* pro šifrování a dešifrování se používá pár rozdílných klíčů
* **veřejný klíč**: veřejný, kdokoliv může zašifrovat zprávu a odeslat ji
  + distribuce za účelem vytváření šifrovaných zpráv a ověření digitálního podpisu
* **soukromý klíč**: nesdílený, pouze s tímto klíčem lze zprávu dešifrovat
  + skrytý za účelem dešifrování přijatých zpráv a vytváření digitálních podpisů
* šifrujeme pomocí VK a dešifrujeme pomocí SK
* SK se nedá z VK vypočítat v rozumném čase

#### Problém diskrétního algoritmu

* Využívá ho např. Diffie-Hellman

Obsah obrázku text

Popis byl vytvořen automaticky

* Pohybujeme-li se v konečné grupě, která obsahuje prvky nesoudělné s n, jedná se o náročnou operaci (v reálných číslech není výpočet mocniny výrazně jednodušší než výpočet logaritmu)

Obsah obrázku text

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

#### Faktorizace velkých čísel

* Zakládá se na rozložení určitého čísla na součin prvočísel
* NP problém
* Máme-li hodnoty p a q, které neznáme, ale známe jejich součin, je nalezení Φ(n) podobně složité jako faktorizace celého čísla n
* Φ(n) je eulerova funkce – počet přirozených čísel menších než n, která jsou s n nesoudělná

### RSA

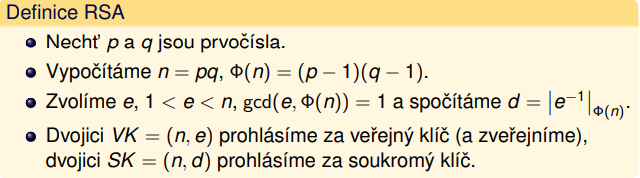
* Zabezpečení utajené komunikace v síti – každá komunikující dvojice musí používat šifrovací klíč
* Pokud je šifrovací klíč známý, je dešifrovací klíč generovatelný s použitím malého počtu operací
* Šifrovací systém veřejného klíče (VK) je řešení problému s přidělováním klíče pro utajenou komunikaci
  + Má VK a SK
  + Vypočítat SK z VK nelze v rozumném čase vypočítat
  + Použitím VK je zřízena utajená komunikace v síti s několika subjekty (Alice má svůj VK a SK, všichni mohou Alici posílat zašifrované zprávy pomocí VK, ale jen ona si je může přečíst, protože jen ona má svůj SK)
  + Seznam klíčů VK1, VK2, … VKn je veřejný

**Princip RSA šifrovacího systému**

* RSA je šifrovací systém VK založený na modulárním umocňování
* **Dvojice (e, n) je VK**; e – exponent, n – modul
* **Dvojice (d, n) je SK**; d – exponent, n – modul
* n – je **součin dvou prvočísel** p a q, tj. n = p\*q a gcd (e, Φ(n)) = 1
* Φ(n) = Φ(p\*q) = (p - 1)\*(q - 1)
  + Když neznáme p a q, tak je toto těžké vypočítat, podobně jako faktorizace

Obsah obrázku text, osoba, snímek obrazovky

Popis byl vytvořen automaticky



**Postup pro generování VK a SK**

**Obsah obrázku text

Popis byl vytvořen automaticky**

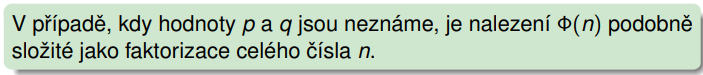
**Obsah obrázku text

Popis byl vytvořen automaticky**

**Bezpečnost RSA**

**Obsah obrázku text

Popis byl vytvořen automaticky**

****

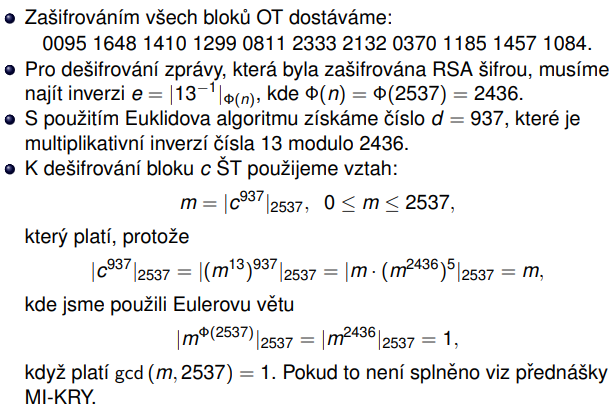
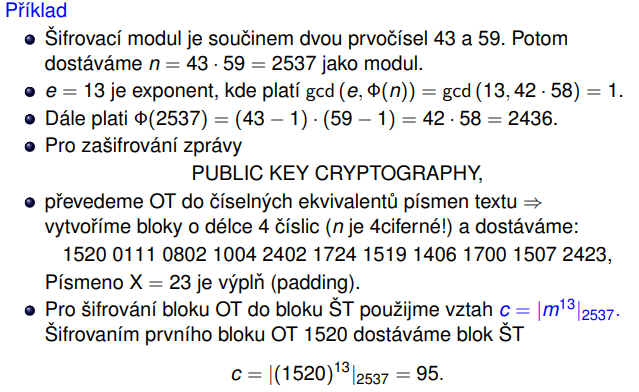
**Problém faktorizace a RSA**

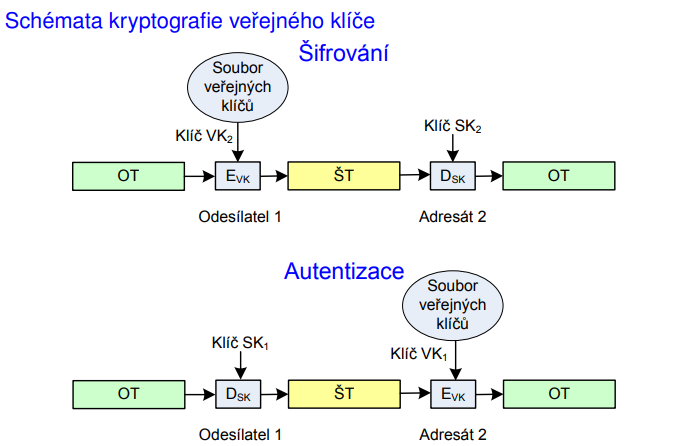
Obsah obrázku text

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

**Příklad RSA**



### Digitální podpis RSA

* RSA lze použít pro podepsání zprávy
* při použití podpisu se příjemce zprávy může ujistit, že zpráva přišla od oprávněného odesílatele, a že tomu tak je na základě nestranného a objektivního testu
* takové ověření je potřebné pro elektronickou poštu, elektronické bankovnictví atd.

**Princip**

**Obsah obrázku text

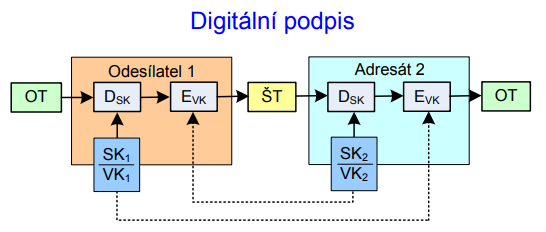
Popis byl vytvořen automaticky**

**Obsah obrázku text

Popis byl vytvořen automaticky**

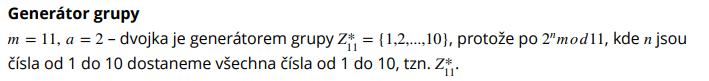
**Obsah obrázku text

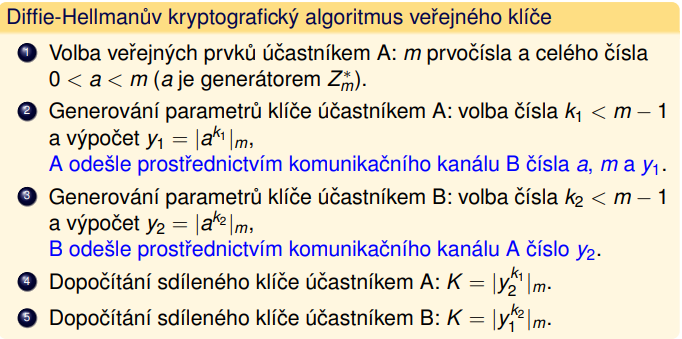
Popis byl vytvořen automaticky**

****

### Diffie-Hellman

* Problém se symetrickými šiframi je, že příjemce musí dostat pravý společný klíč. V otevřené formě se nesmí předávat. DH je jeden ze způsobů zřízení společného klíče
* Založen na problému diskrétního logaritmu



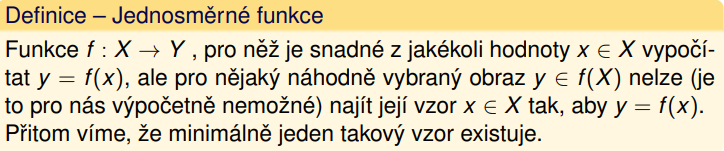


* generátor grupy a musí generovat všechna čísla grupy ve formě *a^n mod m*
* veřejné prvky jsou v tomto případě *m* a *a*

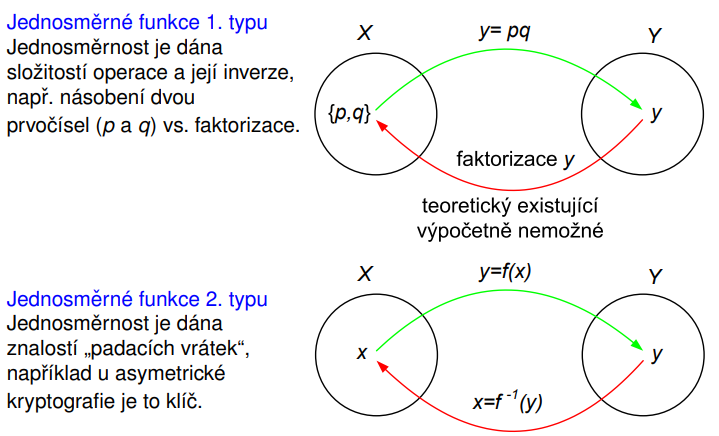
## Hešovací funkce

* využití: digitální podpis, ukládání hesel v DB, přenos dat

#### Jednosměrná funkce



* jednosměrné funkce dělíme na:
  + jednosměrné, pro které je výpočetně nemožné, ale teoreticky proveditelné, najít vzor z obrazu
  + jednosměrné funkce s padacími dvířky, u kterých lze najít vzor z obrazu, ale je za předpokladu znalosti „padacích dvířek“ – klíče



#### Kryptografická hašovací funkce

#### 

* např**. „some data“ → „9b3a5c834f23782024ac19eb2c7fec8537ce8e888c1920b“**

**Vstup a výstup**

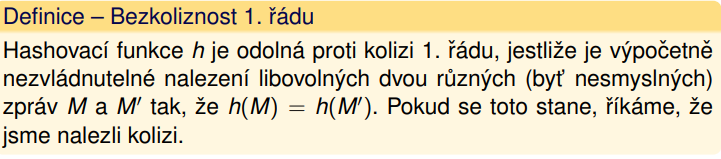
Obsah obrázku text

Popis byl vytvořen automaticky

Obsah obrázku text

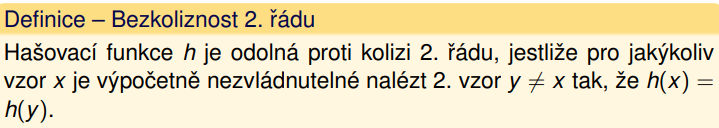
Popis byl vytvořen automaticky

#### Bezkoliznost



Obsah obrázku text

Popis byl vytvořen automaticky



Obsah obrázku text

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

* úloha nalezení kolizí je příliš těžká a výpočetně neproveditelná

#### Konstrukce moderních hašovacích funkcí

Obsah obrázku text

Popis byl vytvořen automaticky

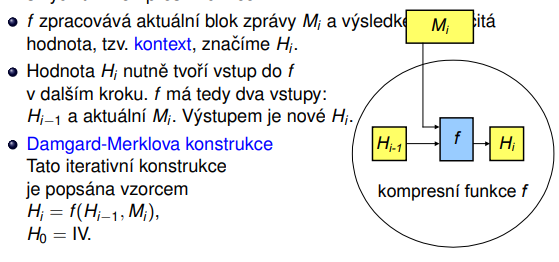
Obsah obrázku text

Popis byl vytvořen automaticky



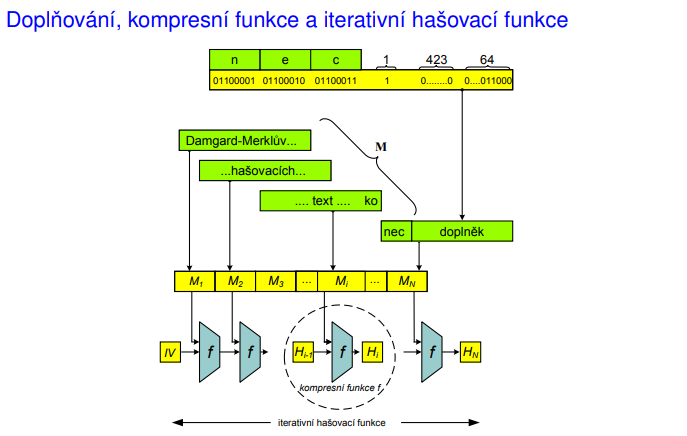
#### Damgard-Merklova konstrukce

* současné hashovací funkce používají Damgard-Merklův (DM) princip iterativní hašovací funkce s využitím kompresní funkce f (např. XOR)



Obsah obrázku text

Popis byl vytvořen automaticky

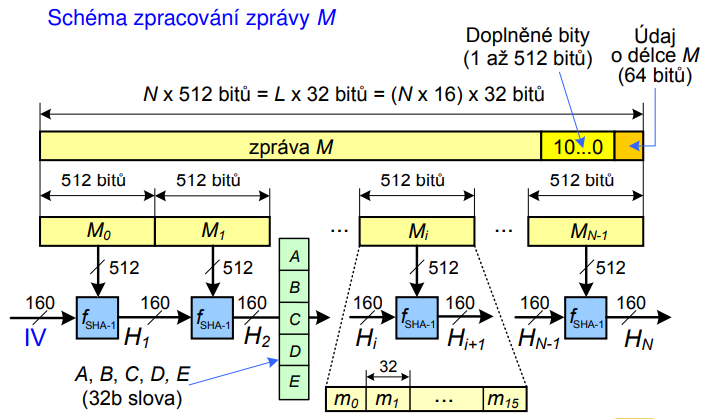


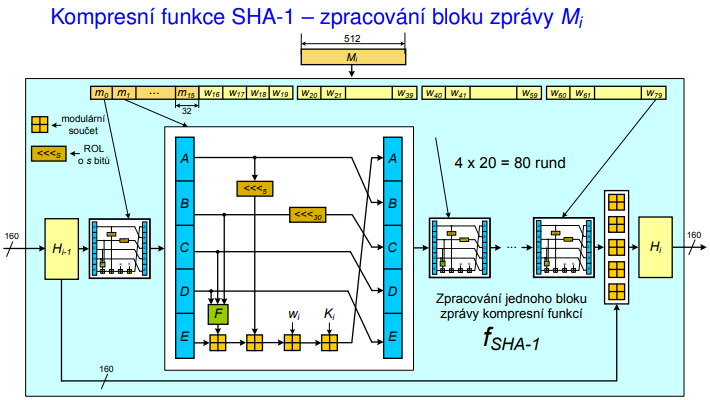
Obsah obrázku text

Popis byl vytvořen automaticky

Konstrukce kompresní funkce viz. přednáška č. 5

### SHA2





Obsah obrázku text

Popis byl vytvořen automaticky

* A,B,C,D,E – vstupně/výstupní 32b registry kompresní funkce
* 160 bitový kontext (začínáme s IV) je postupně „zašifrováván“ 32b slovem mi pro rundy 0, 1, …, 15 a pro rundy 16, 17, …, 79 32b slovem wi, pro které platí:



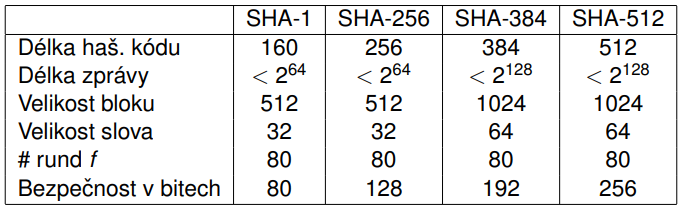
Obsah obrázku stůl

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky

* založené na D-M konstrukci
* skupina SHA-(224/256/348/512), rozdíl je v délce hash kódu (pravděpodobnosti kolize)
* 80 rund (80x zašifrované - může být i různými funkcemi *f, g, h...*)
* Základní vlastnosti hašovacích funkcí SHA-x:



Obsah obrázku text

Popis byl vytvořen automaticky

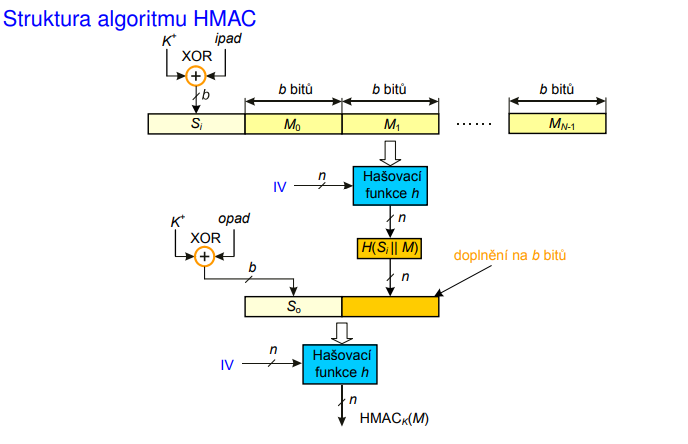
### HMAC

Obsah obrázku text

Popis byl vytvořen automaticky

Obsah obrázku text

Popis byl vytvořen automaticky



Obsah obrázku text

Popis byl vytvořen automaticky