KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Počítačová biometria

(Bio)kryptografia

J. Majerník, L. Urbanská, A. Kačmariková

V-AR-24-25

KCKB UPJS CSIRT UPJS

Kryptografia v biometrii

- skutočné vzorky (obrázky) alebo záznamy) fyzických alebo behaviorálnych charakteristík (znakov) nie sú to, čo je v skutočnosti uložené v databáze biometrického systému pre následné porovnanie
- prevedú sa na matematické súbory, napríklad binárne matematické súbory (napríklad v prípade rozpoznávania odtlačkov prstov, geometrie ruky alebo rozpoznávania žilových vzorov), alebo nejaký druh štatistického profilu (široko používaný s biometrickými behaviorálnym charakteristikami, napríklad rozpoznávanie stlačení klávesov alebo rozpoznávanie podpisu)

- **častá otázka:**
  Ak by takéto biometrické šablóny boli ukradnuté alebo zneužité, dalo by sa s nimi urobiť niečo škodlivé?

Kryptografia v biometrii

- **odpoveď:**
  teoreticky nie, kybernetický útočník teoreticky nemôže nič urobiť
- niekoľko dôvodov:
  - každý dodávateľ biometrických systémov/aplikácií má vlastnú sadu proprietárnych matematických algoritmov na vytváranie šablón pre registráciu (*enrollment*) aj overenie (*verification*)
  - väčšina biometrických systémov vyžaduje, aby bola charakteristika (obrázok alebo záznam) odobratá v reálnom čase od skutočnej osoby
  - skutočný kompozitný obraz alebo záznam nemožno rekonštruovať spätným inžinierstvom ani v prípade šablóny pre registráciu, a ani pre overovanie

Kryptografia v biometrii

- **avšak:**
  - z technického hľadiska, biometrický systém a jeho zodpovedajúce šablóny pre registráciu a overovanie sú len technologické prvky
  - majú teda svoje obmedzenia, čo sa týka toho, čo dokážu a čo nemôžu robiť, ako aj svoju náchylnosť na kybernetické útoky (potrebné uvažovať aj s teoretickou možnosťou, že zložený obraz sa dá sfalšovať)
- z tohto dôvodu samotná biometrická šablóna potrebuje ďalšiu vrstvu ochrany, ktorú získava využitím princípov a nástrojov kryptografie
- keďže na posilnenie biometrických šablón sa používajú práve kryptografické koncepty používame aj označenie biokryptografia
- aj preto je v oblasti biometrie veľmi dôležité poznať a aplikovať základné princípy kryptografie

Podstata kryptografie

- kryptografia je veda, ktorej história siaha hlboko do minulosti (min. až do čias Júliusa Caesara)
- najjednoduchší pohľad na kryptografiu **mylne** hovorí, že je to **iba** kódovanie a dekódovanie textu alebo písomných správ medzi dvoma stranami (odosielateľ a prijímateľ)
- v bežnej každodennej komunikácii veríme, že prijímateľ textovú alebo písomnú správu dostane, bez akýchkoľvek problémov
- v dnešnej digitálnej dobe však existujú riziká, že prijímateľ správu nedostane, alebo že môže byť zachytená treťou stranou a zneužitá
- vždy existuje možnosť, že tretia strana by mohla tajne odpočúvať a použiť dôverné informácie na účely osobného zisku alebo krádež identity

Podstata kryptografie

- nemôžeme skutočne zaručiť žiadny druh bezpečnosti, najmä pokiaľ ide o elektronickú komunikáciu, ako je napríklad e-mail, ktorý sa prenáša po celom svete a v rámci internetu
- vieme ale zabezpečiť, že ak by akýkoľvek typ správy zachytila tretia strana, správa by sa stala nepoužiteľnou
- text alebo písomná správa je odosielateľom zakódovaná a zostáva zakódovaná počas prenosu, až kým prijímajúca strana nedostane text alebo písomnú správu a dekóduje ju

Napríklad:

I LOVE YOU. >> zakódované >> **UYO I VEOL.**

- **kódovanie**: ak poznáme prevodový mechanizmus (tabuľku) vieme dekódovať – bez tajomstva

Podstata kryptografie

- **kryptografia**: využíva procesy a techniky, ktoré utajujú správy šifrovaním a odtajujú dešifrovaním, pre bezpečnú komunikáciu v prítomnosti tretích strán
- vo všeobecnosti ide o konštrukciu a analýzu, ktoré prekonávajú vplyv protivníkov (tretích strán, útočníkov), a ktoré súvisia s rôznymi aspektmi dôvernosti údajov, integrity údajov, autentifikácie a odmietnutia

- **šifrovaná správa** – má byť teda utajená, t. j. písomná správa je maskovaná takým spôsobom, že je úplne bezvýznamná, resp. nerozlúštiteľná

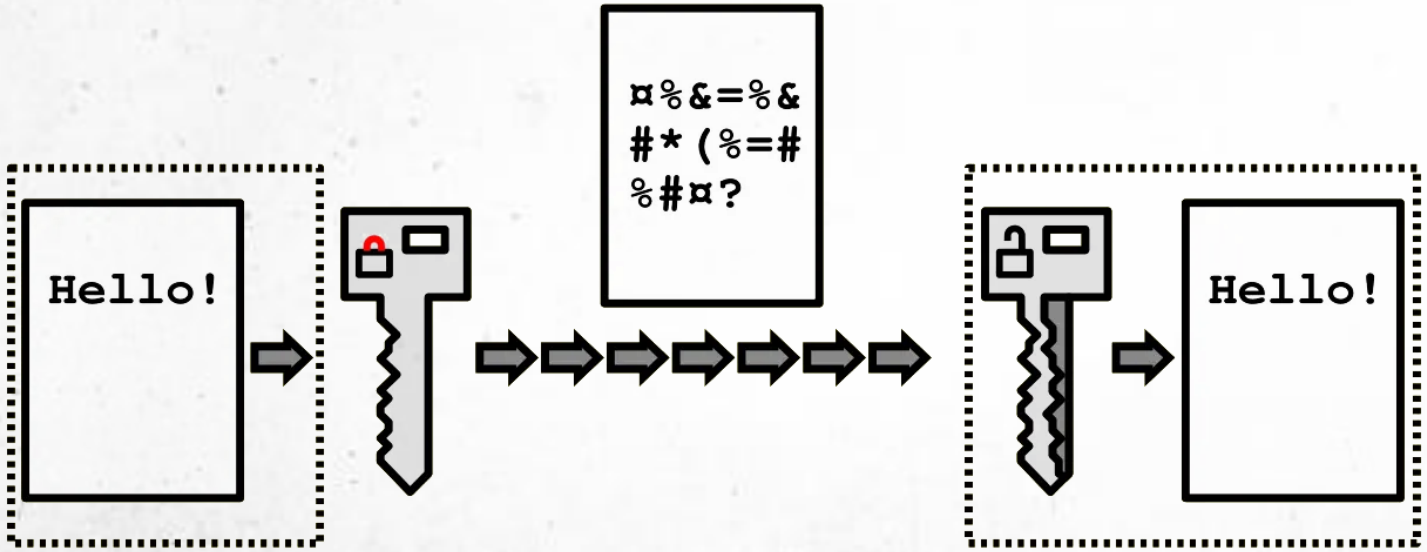
  (šifrovanie je možné definovať a opísať ako **konverziu** informácií z čitateľného stavu do zdanlivého nezmyslu)

Podstata kryptografie

Ako odosielajúca strana šifruje správu?

Ako prijímajúca strana šifrovanú správu dešifruje?

- šifrovanie zjednodušene znamená, že na text alebo písomnú správu je aplikovaný špeciálny matematický vzorec, ktorý označujeme ako šifrovací algoritmus



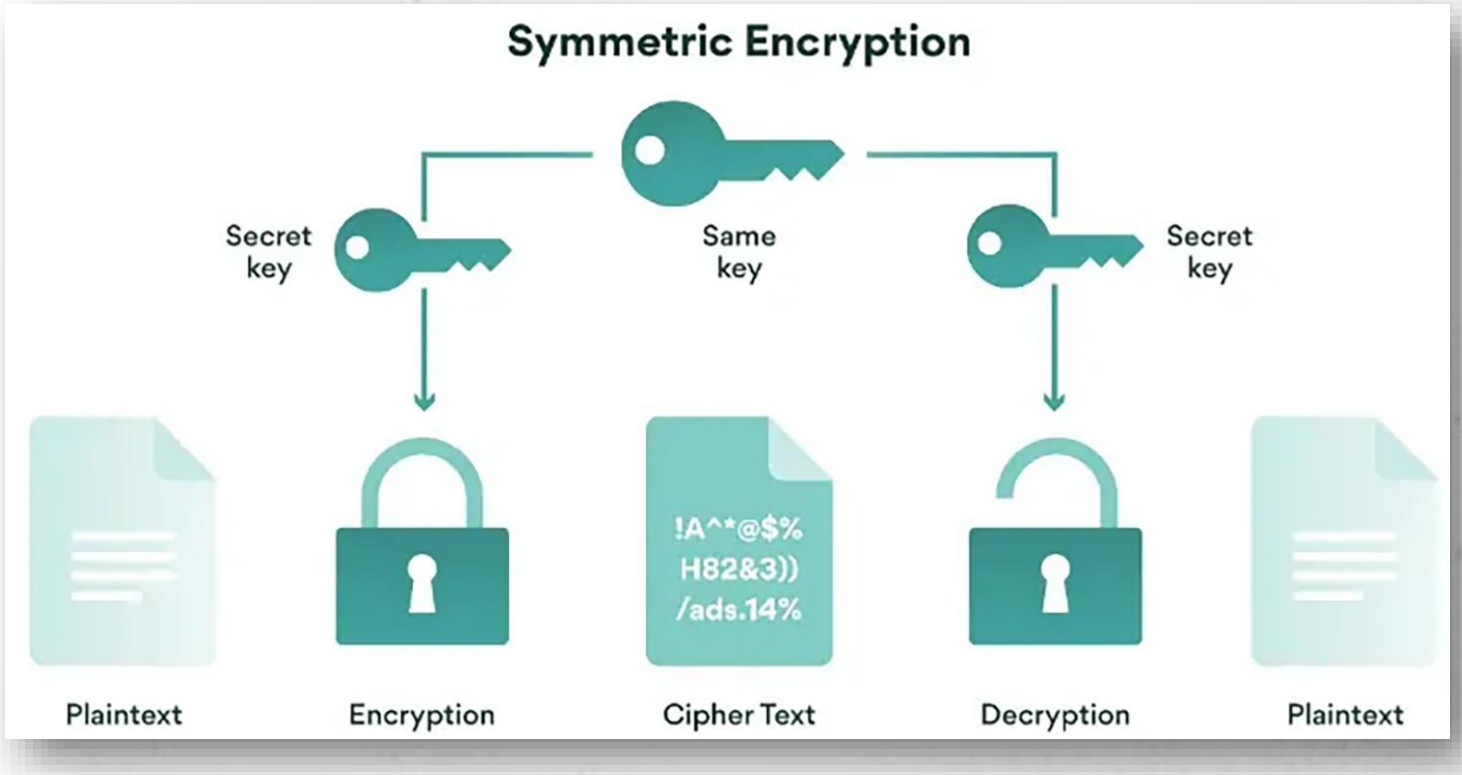
- na dešifrovanie sa používa sa kľúč, ktorý pozná iba odosielajúca a prijímajúca strana
  (v kryptografii sa tento kľúč nazýva aj **šifra**, zvyčajne ide o krátky reťazec znakov, ktorý je potrebný na prelomenie šifrovaného textu)

Šifrovanie

- šifrovací algoritmus môže byť v skutočnosti verejne známy a dostupný pre každého
- kľúč musí zostať tajomstvom medzi odosielajúcou a prijímajúcou stranou
- na odoslanie šifrovaného textu medzi odosielajúcou a prijímajúcou stranou a na zdieľanie kľúča potrebného na šifrovanie a dešifrovanie šifrovaného textu sú potrebné špecifické kryptografické systémy
- v súčasnosti existujú dva takéto typy kryptografických systémov:
  - systémy so symetrickým kľúčom
    (šifrovanie **privátnym** kľúčom)
  - systémy s asymetrickým kľúčom
    (šifrovanie **verejným** kľúčom)
- mnohé šifrovacie systémy kombinujú oboje

Symetrické šifrovanie

- symetrické šifrovanie na šifrovanie a dešifrovanie používa iba jeden kľúč, ktorý sa nazýva súkromný kľúč šifrovaného textu
- jednou z najjednoduchších metodík v systémoch so symetrickým kľúčom je Caesarova šifra, ktorej história siaha až do čias Júliusa Caesara

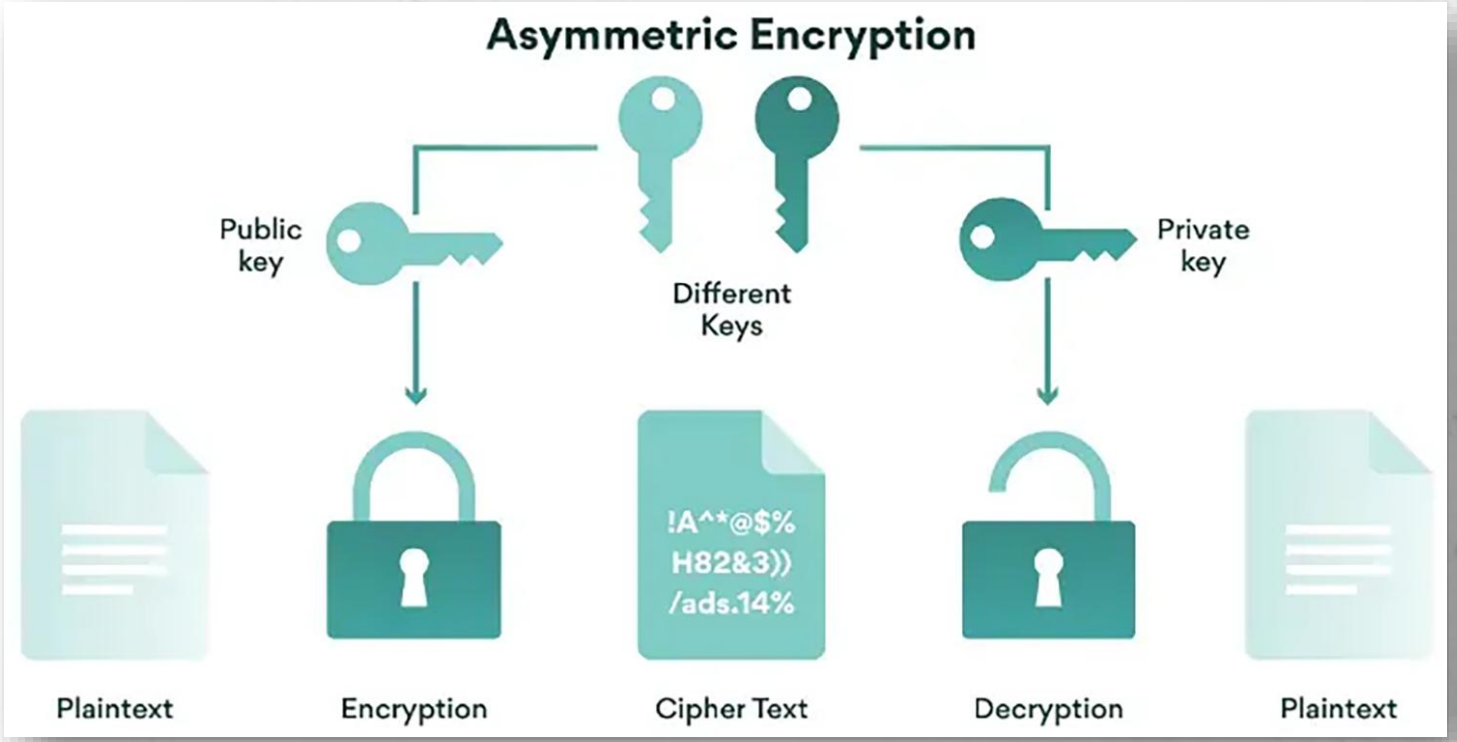


Symetrické šifrovanie

- algoritmus Needham-Schroder - špeciálne navrhnutý, aby sa vysporiadal s odosielajúcimi a prijímajúcimi stranami, ktoré môžu byť po odoslaní správy offline
- algoritmus štandardu digitálneho šifrovania (DES) - výkonný algoritmus, kde šifrovaný text je podrobený 16 iteráciám, aby bolo zabezpečené úplné šifrovanie
- algoritmus štandardu trojmiestneho šifrovania (3DES) - vylepšenie algoritmu DES, ktoré podrobuje šifrovaný text trikrát väčšiemu počtu iterácií
- medzinárodný algoritmus šifrovania dát (IDEA) - novší rýchlejší algoritmus, neustále mení písmená v šifrovanej správe, kým ho prijímajúca strana nedešifruje
- algoritmus pokročilého šifrovacieho štandardu (AES) - najnovší symetrický kryptografický algoritmus
- ...

Asymetrické šifrovanie

- asymetrické šifrovanie na šifrovanie a dešifrovanie používa dva typy kľúčov, ktoré sa nazývajú verejný kľúč a súkromný kľúč
- odosielajúca strana použije verejný kľúč na zašifrovanie správy
- prijímajúca strana, použije súkromný kľúč, na dešifrovanie zašifrovaného textu
- hlavným cieľom je vyhnúť sa potrebe, osobného stretnutia oboch strán na bezpečnú distribúciu kľúča



Asymetrické šifrovanie

- existujú dva odlišné scenáre:
  - prijímajúca strana môže cielene oznámiť odosielajúcej strane verejný kľúč vo verejnom kanáli, aby sa mohla začať a následne ďalej nadviazať komunikácia
  - odosielajúca strana a prijímajúca strana o sebe vopred nič nevedia
- prijímajúca strana zverejní svoj verejný kľúč globálne, aby každý, kto si želá komunikovať s prijímajúcou stranou, tak mohol urobiť
- verejný kľúč je „doslova“ verejný, čo znamená, že ho môže použiť ktokoľvek, **dokonca aj hackeri**

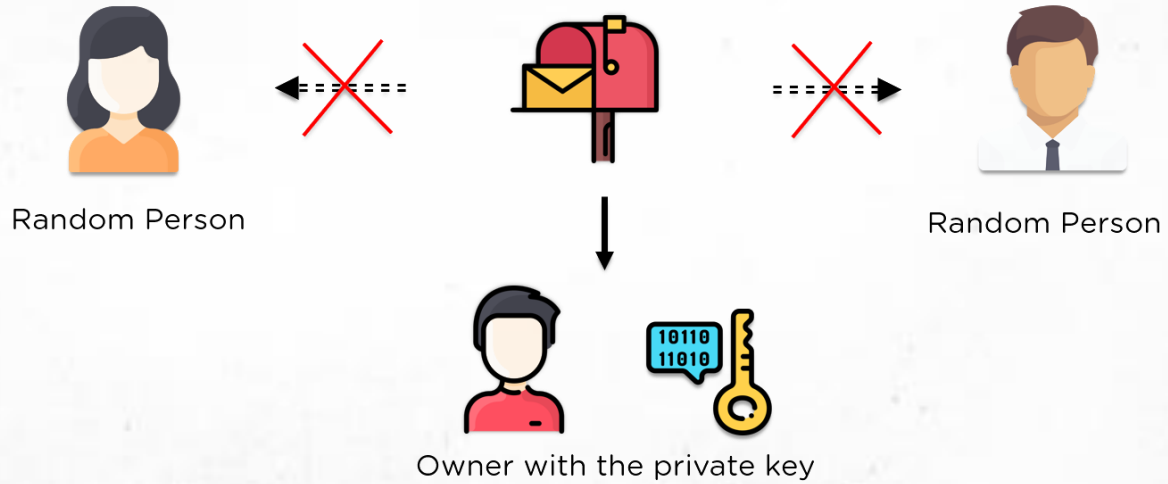
Ako potom zostáva asymetrická kryptografia bezpečná?

Asymetrické šifrovanie

- spolieha sa výlučne na to, že používaný súkromný kľúč je naozaj súkromný – prístupný len jeho vlastníkovi
- ak je vlastníctvo súkromného kľúča akýmkoľvek spôsobom ohrozené, potom je úplne ohrozená aj bezpečnostná schéma asymetrickej kryptografie
- aby sa zabezpečilo, že súkromné kľúče zostanú súkromné, asymetrická kryptografia využíva silu prvočísel
- základnou myšlienkou je vytvoriť veľmi veľké číslo ako súčin dvoch veľmi veľkých prvočísel
- z matematického hľadiska je základným predpokladom časová náročnosť potrebná pre vypočítanie dvoch prvočísel, ktoré sú deliteľmi veľmi veľkého súčinu (niekoľko stoviek celých čísel)

Asymetrické šifrovanie

- známy je len jeden kľúč (verejný) a preto je technika asymetrickej kryptografie používaná odosielajúcou a prijímajúcou stranou zostáva stále neporušená a bezpečná
- hacker teda nemôže spätne analyzovať jeden kľúč, aby sa dostal k druhému kľúču a prelomil šifrovaný text
- v kryptografii asymetrickým kľúčom môže ten istý verejný kľúč použiť na komunikáciu viacero rôznych odosielajúcich strán s jednou prijímajúcou stranou (vzťah 1:N)



Asymetrické šifrovanie

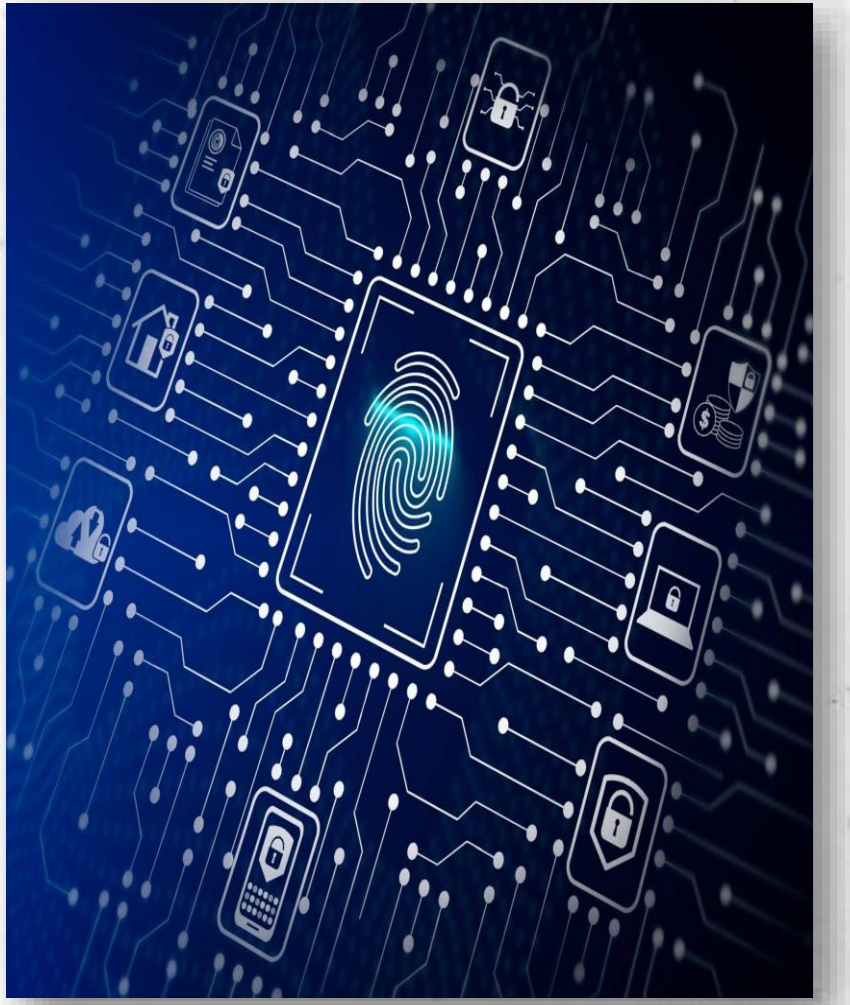
- algoritmus RSA - najznámejší asymetrický kryptografický algoritmus (vytvorili Ron **R**ivest, Adi **S**hamir a Leonard **A**delman). Využíva silu prvočísel na vytvorenie verejného aj súkromného kľúča. Šifrovanie sa vykonáva symetrickými algoritmami a potom sa súkromný kľúč ďalej šifruje verejným kľúčom prijímajúcej strany. Na prijímajúcej strane sa súkromný kľúč vygenerovaný symetrickým kryptografickým algoritmom dešifruje a verejný kľúč vygenerovaný asymetrickou kryptografiou sa potom použije na dešifrovanie zvyšku šifrovaného textu.
- Diffie-Hellmanov algoritmus – známy aj ako algoritmus DH (vytvorili Whit **D**iffie a Martin **H**ellman). Nepoužíva sa na šifrovanie textu, ale jeho hlavným cieľom je vyriešiť problém odosielania kľúča cez zabezpečený kanál.
- Algoritmus teórie eliptických vĺn – novší typ, používaný na šifrovanie veľmi veľkého množstva údajov, je veľmi rýchly a nevyžaduje veľa výpočtového výkonu ani času.
- ...

Symetrické a asymetrické šifrovanie

	Symetrické	Asymetrické
Počet kľúčov	Oboma stranami je používaný jeden identický kľúč.	Hlavná strana generuje dva kľúče, t. j. verejný a súkromný.
Rýchlosť	Veľmi rýchly šifrovací proces.	Pomalší šifrovací proces.
Efektivita	Používané na rýchle šifrovanie veľkého množstva dát.	Častejšie používané na šifrovanie menších objemov dát.
Bezpečnosť	Bezpečné, ale poskytuje iba dôvernosť.	Bezpečnejšie ako symetrické šifrovanie, pričom poskytuje dôvernosť, autentickosť a nepopierateľnosť.
Dĺžka kľúča	128-256 bitov	2048 a viac
Príklady	DES, 3DES, RC4, AES	RSA, DSA, ECC

Biokryptografia

- poskytuje prostriedky na ďalšie zabezpečenie biometrických šablón (vzorov)
- koncepty zašifrovania a dekódovania sú teda aplikované na biometriu
- biometrické šablóny sú chránené šifrovacími a dešifrovacími kľúčmi, kým sú uložené v databáze alebo sa prenášajú cez sieť



Biokryptografia

- ak je šablóna (vzor) biometrickej charakteristiky zašifrovaná, možno ju považovať za šifrovanú biometrickú šablónu, a keď je dešifrovaná, možno ju opäť považovať za nešifrovanú biometrickú šablónu
- aby bola biokryptografia skutočne účinná, musí poskytovať aj nasledujúce funkcie:
  - autenticita - príjemca biometrickej šablóny by mal byť schopný na 100% overiť jej pôvod
  - integrita - biometrická šablóna by nemala byť počas prenosu žiadnym spôsobom ani formou upravená
  - nepopierateľnosť - odosielateľ biometrickej šablóny by nemal falošne popierať, že danú šablónu pôvodne odoslal

Biokryptografia

- hlavným komponentom biokryptografie sú kľúče, používané na šifrovanie alebo dešifrovanie biometrickej šablóny
- samotný kľúč je sériou matematických hodnôt - čím väčšia je hodnota, tým ťažšie je ju počas prenosu prelomiť
- rozsah možných matematických hodnôt je priestorom kľúčov
  (napríklad podpisové kľúče, autentifikačné kľúče, kľúče na šifrovanie údajov, kľúče relácií a pod.)
- na ďalšie posilnenie silných stránok infraštruktúry verejného kľúča založenej na biokryptografii sa na ochranu integrity biometrickej šablóny používajú matematické hašovacie funkcie (pridávané k šifrovanej biometrickej šablóne)
- ak sa hodnoty hašovacej funkcie nezmenili po jej výpočte prijímajúcou stranou, potom si príjemca môže byť istý, že biometrická šablóna nebola nijako zmenená ani upravená
- hašovacie funkcie je možno vypočítať iba v jednom smere

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť

jaroslav.majernik@upjs.sk
lenka.urbanska@upjs.sk
andrea.kacmarikova@upjs.sk