Emma Macháčová

**Bezpečnosť a šifrovanie**

Informačné vzdelávanie

Študijný program: **FIIT B-INFO4 den**

Vyučujúca: **Mgr. Barbora Bieliková**

december 2019

**Obsah**

[Abstrakt 2](#_Toc27602237)

[1. Úvod 3](#_Toc27602238)

[2. Počítačová bezpečnosť 4](#_Toc27602239)

[**2.1 Čo je to počítačová bezpečnosť** 4](#_Toc27602240)

[**2.2 Všeobecné bezpečnostné ciele** 5](#_Toc27602241)

[3. Ako zabezpečiť počítačovú bezpečnosť 6](#_Toc27602242)

[**3.1 Zraniteľné miesta počítačových systémov** 6](#_Toc27602243)

[**3.2 Hrozby pre počítačovú bezpečnosť** 6](#_Toc27602244)

[**3.2.1 Fyzické útoky** 7](#_Toc27602245)

[**3.2.2 Výskumné útoky** 7](#_Toc27602246)

[**3.2.3 Sieťové odpočúvanie** 7](#_Toc27602247)

[**3.2.4 Útoky na symetrickú schému šifrovania** 7](#_Toc27602248)

[**3.3 Bezpečnostné opatrenia** 8](#_Toc27602249)

[**3.3.1 Kerberos** 8](#_Toc27602250)

[4. Šifrovanie 10](#_Toc27602251)

[**4.1 Symetrické šifrovanie** 10](#_Toc27602252)

[**4.2 Asymetrické šifrovanie** 11](#_Toc27602253)

[5. Záver 12](#_Toc27602254)

[7. Zoznam použitej literatúry 13](#_Toc27602255)

# **Abstrakt**

**Kľúčové slová**

počítačová bezpečnosť, šifrovanie dát, šifrovacie kľúče, symetrické šifrovanie, asymetrické šifrovanie, kybernetické útoky, bezpečnostné hrozby, bezpečnostné opatrenia

# **1 Úvod**

Šifrovanie nie je nová technológia, ale v súčasnej dobe so stále narastajúcim rozmachom informačných technológií a so stále rastúcou kyber-kriminalitou, využitie a potreba šifrovania uložených údajov nadobúda novú dimenziu. Cieľom tejto práce je priblížiť šifrovanie v informačných technológiách ako také, jeho význam, princípy a myšlienku, ale taktiež so zameraním sa na šifrovanie vo vzťahu k hrozbám ktorým dnešný používateľ internetu čelí, a tak poukázať na podstatu a využiteľnosť šifrovania.

# **2 Počítačová bezpečnosť**

## **2.1 Čo je to počítačová bezpečnosť**

Pre napísanie seminárnej práce na tému bezpečnosť a šifrovanie je potrebné, aby sme si najskôr objasnili hlavné termíny. Základný termín, od ktorého sa odvodzuje náplň práce, je bezpečnosť. Nás, samozrejme, nezaujíma bezpečnosť ako taká, ale bezpečnosť v sfére informačných technológií. Viaceré vedecké články sa na bezpečnosť pozerajú z rôznych uhlov. Vo väčšine literatúry sa počítačová, alebo kybernetická bezpečnosť používa ako všeobecný pojem. Napríklad pozrime sa, akým spôsobom je definovaná kybernetická bezpečnosť v slovníku Merriam Webster:

*„Kybernetická bezpečnosť sú opatrenia prijaté na ochranu počítača alebo počítačového systému (na internete) pred neoprávneným prístupom alebo útokom“. [[1]](#endnote-1)*

Ďalej sa nám ponúka spracovanie definície pocítačová bezpečnosť autormi [Rossouw von Solms](https://www.sciencedirect.com/science/article/pii/S0167404813000801" \l "!) a [Johan van Niekerk](https://www.sciencedirect.com/science/article/pii/S0167404813000801" \l "!) v článku z časopisu „Computers & Security“, v ktorom sa odkazujú na Medzinárodnú telekomunikačnú úniu (ITU), ktorá nám poskytuje túto definíciu:

*„Kybernetická bezpečnosť je súbor nástrojov, politík, bezpečnostných konceptov, bezpečnostných záruk, usmernení, prístupov k riadeniu rizika, akcií, školení, osvedčených postupov, uistenia a technológií, ktoré možno použiť na ochranu počítačového prostredia a majetku organizácie a používateľa. Medzi aktíva organizácie a používateľa patria pripojené počítačové zariadenia, personál, infraštruktúra, aplikácie, služby, telekomunikačné systémy a celkový počet prenášaných a / alebo uložených informácií v kybernetickom prostredí. Kybernetická bezpečnosť sa snaží zabezpečiť dosiahnutie a udržiavanie bezpečnostných vlastností organizácie a majetku používateľa proti relevantným bezpečnostným rizikám v kybernetickom prostredí.“ [[2]](#endnote-2)*

Pre ešte lepšiu komplexitu predstavy o tom, čo informačná bezpečnosť znamená, je pre nás relevantná aj definícia autorov Whitman a Mattord v ich knihe „Principles of Information Security“ kde definujú bezpečnosť informácií nasledovným spôsobom:

*„Bezpečnosť informácií je ochrana informácií a ich kritických prvkov, vrátane systémov a hardvéru, ktoré tieto informácie používajú, ukladajú a prenášajú“. [[3]](#endnote-3)*

## **2.2 Všeobecné bezpečnostné ciele**

*„Cieľom informačnej bezpečnosti je zabezpečiť kontinuitu podnikania a minimalizovať obchodné škody obmedzením dopadu bezpečnostných incidentov“. [[4]](#endnote-4)*

Je potrebné chrániť informácie pred odcudzením, zneužitím alebo napadnutím. Kybernetickú bezpečnosť je možné merať aspoň jedným z troch cieľov takzvanej „CIA triády“: [[5]](#endnote-5)

1. chrániť dôvernosť údajov
2. zachovať integritu údajov
3. podporovať dostupnosť údajov pre oprávnených používateľov

CIA triáda je bezpečnostný model, ktorý je navrhnutý tak, aby usmerňoval zásady informačnej bezpečnosti vo firme, organizácií alebo spoločnosti. Tento model sa zvykne označovať taktiež AIC (Availability, Integrity, and Confidentiality), aby sa predišlo zámene s ústrednou spravodajskou službou. Prvky triády sa považujú za tri najdôležitejšie komponenty informačnej bezpečnosti. [[6]](#endnote-6)

# **3 Ako zabezpečiť počítačovú bezpečnosť**

Aby sme lepšie chápali princípy zabezpečenia počítačovej bezpečnosti, musíme najskôr stanoviť akým hrozbám čelí a z akého dôvodu. Treba teda venovať pozornosť charakteristike zraniteľných miest, ktoré túto skutočnosť spôsobujú.

## **3.1 Zraniteľné miesta počítačových systémov**

Zraniteľné miesta sú slabé stránky systému alebo jeho konštrukcie, ktoré umožňujú narušiteľovi pristupovať k neoprávneným údajom alebo vykonávať príkazy. Môžu to byť najmä nedostatky v hardvéri alebo softvéri systému, nedostatky v procesoch systému alebo aj nedostatky samotných používateľov systému. [[7]](#endnote-7)

## **3.2 Hrozby pre počítačovú bezpečnosť**

*„Hrozba je akcia, ktorá využíva slabé miesta v systéme a má naň negatívny vplyv. Hrozby môžu pochádzať z dvoch primárnych zdrojov: človeka a prírody.“* [[8]](#endnote-8)

Prírodné hrozby môžu spôsobiť vážne poškodenie počítačových systémov. Je proti nim možné zaviesť len málo záruk a nikto nemôže zabrániť aby sa stali. Ľudské hrozby spôsobujú ľudia. Môže ísť o útoky z vnútra (niekto s oprávneným prístupom do systému) alebo z útokov z vonka (jednotlivec alebo organizácia pracujúca mimo siete). Ľudské hrozby sa delia na neštruktúrované hrozby, pozostávajúce väčšinou z neskúsených jednotlivcov, ktorí používajú ľahko dostupné nástroje na hackovanie a štruktúrované hrozby, keď ľudia poznajú slabé miesta systému a dokážu porozumieť, rozvíjať a využívať kódy a skripty. Samotný útok môže mať mnoho podôb, vrátane aktívnych sieťových útokov na sledovanie nešifrovaného prenosu, alebo pasívne útoky, ako napríklad monitorovanie nechránenej sieťovej komunikácie a dešifrovanie slabo šifrovaného prenosu, a následné získanie autentifikačných informácií atď. [[9]](#endnote-9)

*„V priebehu času sa útoky na internet a systémy pripojené k internetu stali sofistikovanejšími, zatiaľ čo množstvo zručností a znalostí potrebných na vyvolanie útoku sa znížilo - útoky sa stali automatizovanejšími a môžu spôsobiť väčšie škody.“ [[10]](#endnote-10)*

Nakoľko sme si už ujasnili čo sú to hrozby pre počítačovú bezpečnosť, priblížme si ďalej niektoré konkrétne hrozby a problémy, ktoré so sebou tieto hrozby individuálne prinášajú.

### **3.2.1 Fyzické útoky**

Prvý druh útokov ktoré si charakterizujeme sú fyzické útoky. *„Tento druh útokov sa sústredí na hardvérové ​​komponenty. Vzhľadom na bez obslužnú a distribuovanú povahu internetu vecí, väčšina zariadení zvyčajne pracuje vo vonkajších prostrediach, ktoré sú veľmi náchylné na fyzické útoky.“* [[11]](#endnote-11)

### **3.2.2 Výskumné útoky**

Ďalší typ útokov sú výskumné útoky. „Je to neoprávnené zisťovanie a mapovanie systémov, služieb alebo zraniteľností.“ [[12]](#endnote-12) Príkladom prieskumných útokov je skenovanie sieťových portov, „sniffery“ paketov, analýza prenosu a odosielanie otázok o informáciách o IP adresách.

### **3.2.3 Sieťové odpočúvanie**

Sieťové odpočúvanie (alebo eavesdropping) je útok na sieťovej vrstve, ktorý sa zameriava na odchytenie paketov zo siete priamo pri ich prenášaní inými počítačmi, a na čítanie dátového obsahu informácií. Je teda jedným z najúčinnejších typov útokov, pretože „*zneužíva nedostatok šifrovacích služieb*“. [[13]](#endnote-13)

### **3.2.4 Útoky na symetrickú schému šifrovania**

Vo všeobecnosti existujú dva prístupy k útoku na symetrickú schému šifrovania. Prvý z týchto útokov je známy ako kryptanalýza. „*Kryptanalytické útoky sa spoliehajú na povahu algoritmu plus možno aj na niektoré poznatky o všeobecných charakteristikách otvoreného textu alebo dokonca niektorých vzoriek párov otvorený-šifrovaný text*“. [[14]](#endnote-14) Tento typ útoku sa snaží odvodiť konkrétny otvorený text alebo použitý kľúč. „*Ak sa útoku podarí zistiť kľúč, (...) všetky budúce a minulé správy šifrované týmto kľúčom sú kompromitované.“* [[15]](#endnote-15)

Druhá metóda, známa ako útok hrubou silou, je jedna z najznámejších metód – ide o to vyskúšať každý možný kľúč na dešifrovanie šifrovaného textu, až pokiaľ sa daný kľúč netrafí. [[16]](#endnote-16)

„*Užitočný prostriedok klasifikácie bezpečnostných útokov (...) je (rozdelenie na) pasívne útoky a aktívne útoky. Pasívny útok sa pokúša naučiť alebo využiť informácie z internetu ale nemá vplyv na systémové prostriedky. Aktívny útok sa pokúša zmeniť systémové prostriedky alebo ovplyvniť ich fungovanie.“ [[17]](#endnote-17)*

## **3.3 Bezpečnostné opatrenia**

Existuje mnoho spôsobov ako zabezpečiť bezpečnosť údajov a informácií, či už ide o dáta uložené v zariadení, dáta zdieľané medzi rôznymi koncovými bodmi (používateľmi), alebo o dáta priamo spracovávané servermi. Medzi základné metódy a princípy ochrany dát patrí napríklad využívanie kryptografických nástrojov (šifrovanie, autentifikácia správ a hash funkcie, využívanie šifrovacích kľúčov, digitálne podpisy a správa ľúčov..), autentifikácia užívateľov (biometrická autentifikácia, autentifikácia na základe hesla..), kontrola prístupu, využívanie databáz a Cloudovej bezpečnosti (Database Access Controll..) a ďalšie.

Ďalej si povieme niečo o autentifikačných funkciách, ktoré boli vyvinuté na podporu autentifikácie na úrovni aplikácie a digitálnych podpisov. Pozrieme sa teda na jednu z prvých služieb: Kerberos.

### **3.3.1 Kerberos**

Kerberos je autentifikačná služba vyvinutá ako súčasť Project Athena na MIT. Problémy, ktoré rieši Kerberos sú tieto: predpokladajme otvorené distribuované prostredie, v ktorom si želajú používatelia na pracovných staniciach prístup k službám na serveroch distribuovaných v celej sieti. Chceli by sme, aby servery boli schopné obmedziť prístup na oprávnených používateľov a umožniť overenie žiadostí o službu. V tomto prostredí, v ktorom sa nachádza pracovná stanica, sa nedá rátať s tým, že tá-ktorá pracovná stanica správne identifikuje svojich používateľov v sieťových službách. Užívateľ tak môže získať prístup na konkrétnu pracovnú stanicu a predstierať, že jeho identita je identita iného používateľa, ktorý pracuje z tejto pracovnej stanice, alebo používateľ môže odpočúvať sieťovú komunikáciu a použiť opakovaný útok na získanie vstupu na server alebo na narušenie operácie. Namiesto budovania komplikovaných autentifikačných protokolov server Kerberos poskytuje centralizovaný autentifikačný server, ktorého funkciou je autentifikácia používateľov. Na rozdiel od väčšiny ostatných schém autentifikácie, Kerberos spolieha výlučne na symetrické šifrovanie a nevyužíva šifrovanie pomocou verejného kľúča. Bežne sa používajú dve verzie systému Kerberos. Implementácie verzie 4 [MILL88, STEI88] stále existujú. Verzia 5 [KOHL94] opravuje niektoré z bezpečnostných nedostatkov verzie 4 a bola vydaná ako navrhovaný internetový štandard (RFC 1510). [[18]](#endnote-18)

# **4 Šifrovanie**

„*Klasická kryptografia sa snaží zabrániť neautorizovanému (nezamýšľanému) príjemcovi určiť obsah správy*.“ [[19]](#endnote-19)

## **4.1 Symetrické šifrovanie**

*„Symetrické šifrovanie je univerzálnou technikou na zabezpečenie dôvernosti prenášaných alebo uložených údajov.“* [[20]](#endnote-20) Symetrické šifrovanie, tiež označované ako konvenčné šifrovanie alebo šifrovanie s jedným kľúčom, bolo jediným typom šifrovania, ktoré sa používalo pred zavedením šifrovania s verejným kľúčom v neskorých sedemdesiatych rokoch. Symetrické šifrovanie zostáva širšie používaným šifrovaním z uvedených dvoch typov šifrovania. [[21]](#endnote-21) Algorytmy symetrického šifrovania teda používajú rovnaké šifrovacie kľúče pre tak ako šifrovanie holého textu tak aj dešifrovanie zašifrovaného textu.

Tento kľúč je v praxi [zdieľaným tajomstvom](https://en.wikipedia.org/wiki/Shared_secret) medzi stranami a používa sa na udržanie komunikačného spojenia v súkromí. Na šifrovanie správ s plain textom sa použili jednoduché algoritmy využívajúce transpozície alebo mono-abecedné substitúcie .  V prípade Caesarovej posunutia sa každé písmeno v bežnom texte posunie a nahradí sa písmenom určité pevné množstvo pozícií nadol abecedy. [[22]](#endnote-22)

Existujú dve požiadavky na bezpečné používanie symetrického šifrovania: Ako prvé potrebujeme silný šifrovací algoritmus. Prinajmenšom by sme chceli, aby bol algoritmus taký, že útočník, ktorý pozná algoritmus a má prístup k jednému alebo viacerým šifrovaným textom, nebol schopný rozlúštiť šifrovaný text alebo zistiť kľúč. Táto požiadavka sa zvyčajne uvádza v silnejšej forme: Útočník by nemal byť schopný dešifrovať šifrovaný text alebo zistiť kľúč, aj keď má niekoľko šifrovaných textov spolu s odpovedajúcimi otvorenými textami. Druhý podstatný bod je, že dosielateľ a príjemca musia mať kópie tajného kľúča, ktoré dostali bezpečným spôsobom a musia zaistiť bezpečnosť kľúča. Ak niekto získa tajný kľúč a pozná algoritmus, potom všetka komunikácia pomocou tohto kľúča je čitateľná.[[23]](#endnote-23)

## **4.2 Asymetrické šifrovanie**

Myšlienka asymetrického [kryptografického](https://en.wikipedia.org/wiki/Public-key_encryption) systému s [verejným a súkromným kľúčom](https://en.wikipedia.org/wiki/Public-key_encryption) sa pripisuje [Whitfieldovi Diffieovi](https://en.wikipedia.org/wiki/Whitfield_Diffie) a [Martinovi Hellmanovi](https://en.wikipedia.org/wiki/Martin_Hellman) . Ide o kryptografický systém, ktorý používa **páry kľúčov**. **Verejné kľúče,** ktoré môžu byť verejne distribuované, **súkromné ​​kľúče** sú známe iba majiteľovi (a preto sú náležite chránené), to, čo je šifrované verejným kľúčom, je možné dešifrovať iba pomocou pridruženého súkromného kľúča a to, čo je šifrované súkromným kľúčom, je možné dešifrovať iba pomocou priradeného verejného kľúča. [[24]](#endnote-24) Tým pádom, ktokoľvek môže šifrovať správu pomocou verejného kľúča príjemcu a túto šifrovanú správu možno dešifrovať iba pomocou súkromného kľúča príjemcu.

# **5 Záver**

# **7 Zoznam použitej literatúry**

1. Dictionary. *Dictionary by Merriam-Webster* [online]. 2019 [cit. 2019-11-21]. Dostupné na: <https://www.merriam-webster.com/dictionary/cybersecurity> [↑](#endnote-ref-1)
2. VON SOLMS, ROSSOUW a JOHAN VAN NIEKERK. From information security to cyber security. In: *Computers & Security* [online]. 2013, vol. 38, s. 97-102 [cit. 2019-11-21]. ISSN 0167-4048. Dostupné na: <https://doi.org/10.1016/j.cose.2013.04.004> [↑](#endnote-ref-2)
3. WHITMAN, MICHAEL, Herbert Mattord. *Principles of Information Security* [online]. Cengage Learning EMEA, 2009 [cit 2019-11-21]. Tretia edícia. ISBN-10 1-4239-0177-0. Dostupné na: <https://books.google.sk/books/about/Principles_of_Information_Security.html?id=gPonBssSm0kC&redir_esc=y> [↑](#endnote-ref-3)
4. VON SOLMS, ROSSOUW a JOHAN VAN NIEKERK. From information security to cyber security. In: *Computers & Security* [online]. 2013, vol. 38, s. 97-102 [cit. 2019-11-21]. ISSN 0167-4048. Dostupné na: <https://doi.org/10.1016/j.cose.2013.04.004> [↑](#endnote-ref-4)
5. ANWAR, RAJA a KASHIF QURESHI. Security Issues and Attacks in Wireless Sensor Network. In: *World Sciences Journal* [online]. 2014, vol. 30, iss.10, s. 1224-1227 [cit. 2019-11-22]. ISSN 1818-4952. Dostupné na: <https://www.researchgate.net/profile/Raja_Anwar/publication/260744866_Security_Issues_and_Attacks_in_Wireless_Sensor_Network/links/0f3175321a6b61477c000000/Security-Issues-and-Attacks-in-Wireless-Sensor-Network.pdf> [↑](#endnote-ref-5)
6. ANWAR, RAJA a KASHIF QURESHI. Security Issues and Attacks in Wireless Sensor Network. In: *World Sciences Journal* [online]. 2014, vol. 30, iss.10, s. 1224-1227 [cit. 2019-11-22]. ISSN 1818-4952. Dostupné na: <https://www.researchgate.net/profile/Raja_Anwar/publication/260744866_Security_Issues_and_Attacks_in_Wireless_Sensor_Network/links/0f3175321a6b61477c000000/Security-Issues-and-Attacks-in-Wireless-Sensor-Network.pdf> [↑](#endnote-ref-6)
7. ABOMHARA, MOHAMED a GEIR KOIEN. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. In: *Journal of Cyber Security and Mobility* [online]. 2015, vol. 4, iss. 1, s. 65-88 [cit. 2019-11-22]. ISSN 2245-4578. Dostupné na: <https://doi.org/10.13052/jcsm2245-1439.414> [↑](#endnote-ref-7)
8. ABOMHARA, MOHAMED a GEIR KOIEN. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. In: *Journal of Cyber Security and Mobility* [online]. 2015, vol. 4, iss. 1, s. 65-88 [cit. 2019-11-22]. ISSN 2245-4578. Dostupné na: <https://doi.org/10.13052/jcsm2245-1439.414> [↑](#endnote-ref-8)
9. ABOMHARA, MOHAMED a GEIR KOIEN. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. In: *Journal of Cyber Security and Mobility* [online]. [miesto vydania neznáme], 2015, vol. 4, iss. 1, s. 65-88 [cit. 2019-11-22]. ISSN 2245-4578. Dostupné na: <https://doi.org/10.13052/jcsm2245-1439.414> [↑](#endnote-ref-9)
10. STALLINGS, WILLIAM. *Cryptography and Network Security Principles and Practices* [online]. Prentice Hall, 2005 [cit. 2019-12-04]. Štvrtá edícia. ISBN-13: 978-0-13-187319-3. Dostupné na: <http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf> [↑](#endnote-ref-10)
11. ABOMHARA, MOHAMED a GEIR KOIEN. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. In: *Journal of Cyber Security and Mobility* [online]. [miesto vydania neznáme], 2015, vol. 4, iss. 1, s. 65-88 [cit. 2019-11-22]. ISSN 2245-4578. Dostupné na: <https://doi.org/10.13052/jcsm2245-1439.414> [↑](#endnote-ref-11)
12. ABOMHARA, MOHAMED a GEIR KOIEN. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. In: *Journal of Cyber Security and Mobility* [online]. [miesto vydania neznáme], 2015, vol. 4, iss. 1, s. 65-88 [cit. 2019-11-22]. ISSN 2245-4578. Dostupné na: <https://doi.org/10.13052/jcsm2245-1439.414> [↑](#endnote-ref-12)
13. MCGREGOR, P. Animal Communication Networks [online]. Cambridge University Press. Spojené Kráľovstvo: Cambridge University Press. 2005. s 13-15. [cit. 2019-11-23]. ISBN-13 978-0-521-82361-7. Dostupné na: <https://books.google.sk/books?hl=sk&lr=&id=B58DSFCaQpwC&oi=fnd&pg=PA13&dq=eavesdropping&ots=vPTdYlvms7&sig=jQTftLE5I4lfprp-Myp-wonUj5w&redir_esc=y#v=onepage&q=eavesdropping&f=false> [↑](#endnote-ref-13)
14. HUDEC, L. Kryptografické nástroje [prezentácia online]. Fakulta informatiky a informačných technológií Slovenskej technickej univerzity. Bratislava. [cit. 2019-11-23]. Dostupné na: http://www2.fiit.stuba.sk/~lhudec/PIS/2\_tema.ppt [↑](#endnote-ref-14)
15. HUDEC, L. Kryptografické nástroje [prezentácia online]. Fakulta informatiky a informačných technológií Slovenskej technickej univerzity. Bratislava. [cit. 2019-11-23]. Dostupné na: http://www2.fiit.stuba.sk/~lhudec/PIS/2\_tema.ppt [↑](#endnote-ref-15)
16. HUDEC, L. Kryptografické nástroje [prezentácia online]. Fakulta informatiky a informačných technológií Slovenskej technickej univerzity. Bratislava. [cit. 2019-11-23]. Dostupné na: <http://www2.fiit.stuba.sk/~lhudec/PIS/2_tema.ppt> [↑](#endnote-ref-16)
17. STALLINGS, WILLIAM. *Cryptography and Network Security Principles and Practices* [online]. Prentice Hall, 2005. s 13. [cit. 2019-12-04]. Štvrtá edícia. ISBN-13: 978-0-13-187319-3. Dostupné na: <http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf> [↑](#endnote-ref-17)
18. STALLINGS, WILLIAM, Lawrie Brown. *Computer Security: Principles And Practice* [online]. University of New South Wales, Australian Defence Force Academy, 2014 [cit. 2019-12-04]. Tretia edícia. ISBN 978-0-13-377392-7. Dostupné na: <https://vowi.fsinf.at/images/3/3d/TU_Wien-Introduction_to_Security_VU_%28Weippl%29_-_Computer_Security_Principles_and_Practice_%283rd_Edition_-_2015%29.pdf> [↑](#endnote-ref-18)
19. SIMMONS, J. Symmetric and Asymmetric Encryption. In *Computing Surveys* [online]. [New Mexico], vol. 11, no. 4, s. 306-330 [cit. 2019-11-22]. ACM 0010-4892/79/1200-0305 $00 75. Dostupné na: <https://www.princeton.edu/~rblee/ELE572Papers/CSurveys_SymmAsymEncrypt-simmons.pdf> [↑](#endnote-ref-19)
20. HUDEC, L. Kryptografické nástroje [prezentácia online]. Fakulta informatiky a informačných technológií Slovenskej technickej univerzity. Bratislava. [cit. 2019-11-23]. Dostupné na: http://www2.fiit.stuba.sk/~lhudec/PIS/2\_tema.ppt [↑](#endnote-ref-20)
21. HUDEC, L. Kryptografické nástroje [prezentácia online]. Fakulta informatiky a informačných technológií Slovenskej technickej univerzity. Bratislava. [cit. 2019-11-23]. Dostupné na: <http://www2.fiit.stuba.sk/~lhudec/PIS/2_tema.ppt> [↑](#endnote-ref-21)
22. FARZANEH, A., FORLER, CH., LUCKS, S. General classification of the authenticated encryption schemes for the CAESAR competition. In: *Computer Science Review* [online]. 2016, vol. 22, s 13-26. [cit. 2019-12-04]. ISSN: 1574-0137. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S1574013715300290> [↑](#endnote-ref-22)
23. HUDEC, L. Kryptografické nástroje [prezentácia online]. Fakulta informatiky a informačných technológií Slovenskej technickej univerzity. Bratislava. [cit. 2019-11-23]. Dostupné na: <http://www2.fiit.stuba.sk/~lhudec/PIS/2_tema.ppt> [↑](#endnote-ref-23)
24. SIMMONS, J. Symmetric and Asymmetric Encryption. In *Computing Surveys* [online]. [New Mexico], vol. 11, no. 4, s. 306-330 [cit. 2019-11-22]. ACM 0010-4892/79/1200-0305 $00 75. Dostupné na: <https://www.princeton.edu/~rblee/ELE572Papers/CSurveys_SymmAsymEncrypt-simmons.pdf> [↑](#endnote-ref-24)