Informačné vzdelávanie

**Bezpečnosť - šifrovanie**

**Meno autora** : Emma Macháčová

**Dátum vytvorenia** : 15.11.2019

**Obsah**

[Abstrakt 0](#_Toc25006012)

[1. Úvod 1](#_Toc25006013)

[2. Počítačová bezpečnosť 2](#_Toc25006014)

[2.1 Čo je to počítačová bezpečnosť 2](#_Toc25006015)

[2.2 Všeobecné bezpečnostné ciele 3](#_Toc25006016)

[3. Ako zabezpečiť počítačovú bezpečnosť 4](#_Toc25006017)

[3.1 Zraniteľné miesta počítačových systémov 4](#_Toc25006018)

[3.2 Hrozby pre počítačovú bezpečnosť 4](#_Toc25006019)

[3.2.1 Fyzické útoky 5](#_Toc25006020)

[3.2.2 Výskumné útoky 5](#_Toc25006021)

[3.2.3 Sieťové odpočúvanie 5](#_Toc25006022)

[3.2.4 Útoky na symetrickú schému šifrovania 5](#_Toc25006023)

[3.3 Bezpečnostné aplikácie a opatrenia 5](#_Toc25006024)

[4. Šifrovanie 6](#_Toc25006025)

[4.1 Princíp šifrovania 6](#_Toc25006026)

[4.2 Symetrické šifrovanie 7](#_Toc25006027)

[4.1.1 Šifrovacie kľúče 7](#_Toc25006028)

[4.1.2 Typy šifrovacích kľúčov 8](#_Toc25006029)

[4.2 Druhy šifrovania 8](#_Toc25006030)

[5. Dešifrovanie 9](#_Toc25006031)

[5.1 Princíp dešifrovania 9](#_Toc25006032)

[6. Záver 10](#_Toc25006033)

[7. Zoznam použitej literatúry 13](#_Toc25006034)

[8. Zoznam obrázkov 12](#_Toc25006035)

# **Abstrakt**

# **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#!) 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. Prírodné hrozby, ako sú zemetrasenia, hurikány, povodne a požiar, môžu spôsobiť vážne poškodenie počítačových systémov. Proti prírodným katastrofám je možné zaviesť len málo záruk a nikto im nemôže zabrániť v tom, aby sa stali. Ľudské hrozby sú také, ktoré 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), ktoré sa snažia poškodiť a narušiť systém. Ľudské hrozby sa delia na: [[8]](#endnote-8)

* Neštruktúrované hrozby, pozostávajúce väčšinou z neskúsených jednotlivcov, ktorí používajú ľahko dostupné nástroje na hackovanie.
* Štruktúrované hrozby, keď ľudia poznajú slabé miesta systému a dokážu porozumieť, rozvíjať a využívať kódy a skripty. [[9]](#endnote-9)

Samotný útok môže mať mnoho podôb, vrátane aktívnych sieťových útokov na sledovanie nešifrovaného prenosu pri hľadaní citlivých informácií, alebo pasívne útoky, ako napríklad monitorovanie nechránenej sieťovej komunikácie a dešifrovanie slabo šifrovaného prenosu, a následné získanie autentifikačných informácií atď. Bežné typy počítačových útokov sú: [[10]](#endnote-10)

### **3.2.1 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**

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

### **3.2.3 Sieťové odpočúvanie**

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

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

Vo všeobecnosti existujú dva všeobecné prístupy k útoku na symetrickú schému šifrovania. Prvý útok 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. Tento typ útoku využíva charakteristiky algoritmu, aby sa pokúsil odvodiť konkrétny otvorený text alebo odvodiť použitý kľúč. Ak sa útoku podarí zistiť kľúč, účinok je katastrofický: všetky budúce a minulé správy šifrované týmto kľúčom sú kompromitované.

Druhá metóda, známa ako útok hrubou silou, je vyskúšať každý možný kľúč na dešifrovanie šifrovaného textu, až pokiaľ sa nezíska zrozumiteľný preklad do otvoreného textu. [[14]](#endnote-14)

## **3.3 Bezpečnostné aplikácie a opatrenia**

- ake bezpecnostne aplikacie existuju?

- ake opatrenia su mozne na lepsie zabezpecenie?

- co su to certifikaty, ako sluzia, kto ich poskytuje?

- "cyber security" AND "tools"

- <https://www.sciencedirect.com/science/article/pii/S0167404810000775>

- Information security enforcement

- "cyber security applications"

- <https://link.springer.com/chapter/10.1007/978-3-319-16549-3_5>

- Intrusion Detection

# **4. Šifrovanie**

Vývoj presných definícií bezpečnosti šifrovania, ako aj podrobné pochopenie vzťahu šifrovania a bezpečnosti, bol hlavnou oblasťou výskumu v modernej kryptografii. [[15]](#endnote-15)

Šifrovanie chráni pred pasívnym útokom (odpočúvanie). Iná požiadavka je ochrana pred aktívnym útokom (falšovanie údajov a transakcií). Ochrana proti takýmto útokom je známa ako autentizácia správ alebo údajov. [[16]](#endnote-16)

Správa, súbor, dokument alebo iný súbor údajov sa považuje za autentický keď je pravý a pochádza z jeho udaného zdroja. Autentizácia správ alebo údajov je procedúra, ktorá umožňuje komunikujúcim stranám verifikovať, či sú prijaté alebo uložené správy autentické.[[17]](#endnote-17)

- co to znamena v ramci informacnych technologii?

- ake je vyuzitie sifrovania?

## **4.1 Princíp šifrovania**

- ako to funguje?

## **4.2 Symetrické šifrovanie**

Symetrické šifrovanie je univerzálnou technikou na zabezpečenie dôvernosti prenášaných alebo uložených údajov. [[18]](#endnote-18)

Táto časť predstavuje základný koncept symetrického šifrovania. Nasleduje prehľad dvoch najdôležitejších symetrických šifrovacích algoritmov: štandard šifrovania údajov DES (Data Encryption Standard) a pokročilý šifrovací štandard AES (Advanced Encryption Standard), ktoré sú algoritmy blokového šifrovania. Nakoniec, táto časť zavádza koncept algoritmov prúdového symetrického šifrovania. [[19]](#endnote-19)

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. [[20]](#endnote-20)

Existujú dve požiadavky na bezpečné používanie symetrického šifrovania:

1. 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. [[21]](#endnote-21)

2. Odosielateľ 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.[[22]](#endnote-22)

### **4.1.1 Šifrovacie kľúče**

- popis, princip prace :

- ako su v sifrovani vyuzivane sifrovacie kluce?

- ako funguju sifrovacie kluce? ako vznikaju?

- ako ich (sif. kluce) realne vyuzivaju uzivatenia?

### **4.1.2 Typy šifrovacích kľúčov**

- typy sifrovacich klucov (public key..)

- "encryption key"

- https://patents.google.com/patent/US9002018B2/en

- "key encryption"

- https://link.springer.com/chapter/10.1007/3-540-39200-9\_16

- Bilinear Diffie-Hellman, Forward security, Key exposure

## **4.2 Druhy šifrovania**

- ake su druhy sifrovania?

- aky je rozdiel medzi symetrickym a asymetrickym sifrovanim?

# **5. Dešifrovanie**

- co to je?

## **5.1 Princíp dešifrovania**

- ako funguje?

- ako sa to lisi od sifrovania?

- co je to cyberspace?

- SSL/TLS?

- cloud copmuting - co to je, na co to sluzi:

- "security" AND "data encryption"

- https://patents.google.com/patent/US5999629A/en

# **6. Záver**

# **7. Zoznam obrázkov**

# **8. Zoznam použitej literatúry**

1. Dictionary. *Dictionary by Merriam-Webster* [online]. [miesto vydania neznáme], © 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]. [miesto vydania neznáme], 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]. [miesto vydania neznáme], 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]. [miesto vydania neznáme], 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]. [miesto vydania neznáme], 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]. [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-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]. [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-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. 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-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. 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-17)
18. 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-18)
19. 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-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. 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-22)