Gimnazija Vič

Tržaška cesta 72

1000 Ljubljana

Projektna Naloga

Moderna kriptografiaj

Mentorica: Marina TROST

Ljubljana, 2019 Avtor: Luka ORLIĆ, 1.a

IZVLEČEK

Moderna kriptografija ima široko uporabo v vsakodnevnem življenju. V nalogi so podana področja uporabe kriptografije v sodobnem svetu s posebnim poudarkom na digitalnih potrdil, zgoščevalnih funkcijah v moderni kriptografiji in metodah simetrične kriptografije. Brez poudarka so pokrite razlike med moderno kriptografijo in steganografijo ter asimetrična kriptografija.

Projektna naloga v teoretičnem delu govori o moderni kriptografiji v sodobnem svetu. V njej so podani podatki kako in kje se kriptografija uporablja v današnjem svetu, razložila bo uporabo digitalnih podpisov in zgoščevalnih funkcij v moderni kriptografiji ter tudi metode simetrične in asimetrične kriptografije. Simetrično podrobneje kakor asimetrično, kot po dogovoru z mentorico projekta. Omenjeni bosta kriptoanaliza in steganografija.

KLJUČNE BESEDE

moderna kriptografija, simetrična kriptografija, asimetrična kriptografija, steganografija, kriptografske zgoščevalne funkcije, digitalna potrdila

ABSTRACT

Modern cryptography has a wide range of uses in everyday life. Within the project, there are given the uses of modern cryptography in the modern world with special emphasis on digital certificate, cryptographic hash functions in modern cryptography and methods of symmetric-key algorithms. Without any special emphasis it will cover asymmetric-key algorithms and also the differences between modern cryptography and steganography.

The project work, within the theoretical part, will talk about modern cryptography within the modern world. Within it, they are given, how and where cryptography is used within the modern world, explain the use of digital certificates and hash functions within modern cryptography and also methods of symmetrical-key algorithms and asymmetrical-key algorithms, as per the agreement with the mentor of the project work. It will also mention cryptanalysis and steganography.

KEY WORDS

Modern cryptography, symmetric-key algorithms, asymmetric-key algorithms, steganography, cryptographic hash functions, digital certificates

Kazalo

[IZVLEČEK 2](#_Toc1929409)

[KLJUČNE BESEDE 2](#_Toc1929410)

[ABSTRACT 2](#_Toc1929411)

[KEY WORDS 3](#_Toc1929412)

[1. UVOD 5](#_Toc1929413)

[2. ZGODOVINA KRIPTOGRAFIJE 5](#_Toc1929414)

[3. SIMETRIČNA KRIPTOGRAFIJA 7](#_Toc1929415)

[4. KRIPTOGRAFSKA ZGOŠČEVALNA FUNKCIJA 8](#_Toc1929416)

[Slika 1: Prikaz monoalfabetske substitucije s nespremenljivim ključem 6](file:///D:\Luka_9gag\PROJEKTNA--INFO\INFO--Projektna%20Naloga.docx#_Toc2506757)

[Slika 2: Prikaz monoalfabetske substitucije s spremenljivim ključem 7](#_Toc2506758)

[Slika 3: Prikaz splošne simetrične kriptografije 8](#_Toc2506759)

[Slika 4: Prikaz asimetrične kriptografije 9](#_Toc2506760)

# UVOD

V današnjem času se s kriptografijo srečujemo na vsakem koraku, čeprav se tega pogosto ne zavedamo. S kriptografijo se srečujemo povsod, v računalnikih, mobitelih, radijski sprejemniki, hladilnikih, urah in avtih ter mnogih drugih napravah. Kriptografija je disciplina katera se ukvarja s proučevanjem metod za pošiljanje sporočil v takšni obliki, da jih lahko preberejo izključno tisti katerim je sporočilo namenjeno. S pomočjo kriptografije si vsakodnevno življenje olajšamo ter zagotavljamo varnost in zasebnost. Pomembno je, da se ljudi zavedajo, kako ta del sveta deluje in vpliva na vsakega posameznika, da se lahko zavedajo in zaščitijo pred vse večjimi težavami zasebnosti in kibernetskega vojskovanja.

# ZGODOVINA KRIPTOGRAFIJE

Različne vrste kriptografije potekajo že od začetka komunikacije. Od nekdaj so želeli sporočila in njihov pomen skriti tako, da ga ne more vsak razumeti. Zato so sporočila pričeli prikrivat. Znana zgodba, ki govori o tem kako generali Histius dal sužnju glavo obriti in nanjo tetoviral skrivno sporočilo ter rekel sužnju, ko pride do prejemnika naj mu le ta obrije glavo in prebere kaj je zapisano. Čeprav je dober način, da se informacije samo skrije, se je hitro pokazalo, da mogoče le ta ni učinkovita, ker se sporočila hitro lahko najdejo, in nato jih lahko kdorkoli prebere in se zaveda kaj sporočilo pravi. Temu pravimo tudi steganografija[[1]](#footnote-1). Zato se dokaj hitro razvijejo načini spreminjanja sporočil po raznih metodah, da četudi je sporočilo najdeno, ga ne more vsak kdo prebrati in razumeti. V srednjem veku se največ kriptografije uporablja ravno v cerkvenih inštitucijah. Primer je ko papež Clement VII., da narediti šifro imenovano *nomenclator*. Na začetku je to spreminjanje sporočil bilo nadomeščanje besed z drugimi, in je veljalo, da ima vsaka beseda ali črka pripisano natanko eno novo črko ali besedo, bodisi izmišljeno bodisi že obstoječo.

|  |
| --- |
| Slika 1: Prikaz monoalfabetske substitucije s nespremenljivim ključem  Slika : Prikaz monoalfabetske substitucije s nespremenljivim ključem |

Ta princip se je hitro pokazal za nepraktičnega, zato ker če je nasprotnik ugotovil sistem, je z lahkoto ugotovil originalno sporočilo. Tak sistem kot je prikazan na sliki 1, imenujemo kriptosistem. Zaradi tega problema se razvije tako imenovano Kerckhoffovo načelo, ki govori, da varnost sporočila ne sme biti odvisna od sistema temveč od gesla oziroma ključa.

|  |
| --- |
| Slika : Prikaz monoalfabetske substitucije s spremenljivim ključem |

Sistemi kot na sliki 2, ki vsebujejo ključe delujejo na še dosti preprost način, namreč imajo dve tabeli, prva s preprostimi črkami in druga z njihovim nadomestkom, ki je lahko ali znak ali nova pripisana črka. Na tej točki se opazi, če se ozremo nazaj na zgodbo o Histuisu, da dokler je on uporabljal metode steganografije oziroma prikrivanja sporočila z nepomembnimi objekti oziroma informacijami in kasnejšimi metodami kriptografije, ki se nato razvijejo še globje in se delijo na razne vrste.

# SIMETRIČNA KRIPTOGRAFIJA

Kriptografijo delimo na dva glavna dela, namreč simetrično in asimetrično. Vsa simetrična kriptografija poteka na principu, da obstaja sporočilo, ki se ga zakodira s pomočjo tajnega ključa. To sporočilo pa lahko dekodirajo le osebe, ki poznajo to geslo. Glede na to kako se to sporočilo zakodira, delimo simetrično kriptografijo na še dva poglavitna dela, ta sta tokovne šifre in bločne šifre. Tokovno šifriranje poteka, tako da se vsaka črka posebej zakodira, dokler pri tako imenovanem bločnem šifriranju, pa ta vzame nek odsek podatkov, najpogosteje bloke po 64 bitov, in te bloke zakodira.

|  |
| --- |
| Slika : Prikaz splošne simetrične kriptografije |

V praksi to pomeni, da se določen odsek poda skozi določen algoritem, ki uporabi tajni ključ in pride ven v zakodirani obliki, to zakodirano obliko prejme druga oseba in s pomočjo istega ključa, sporočilo dekodira in prebere. Pri simetrični kriptografiji se pojavljajo standardne slabosti kakor so:

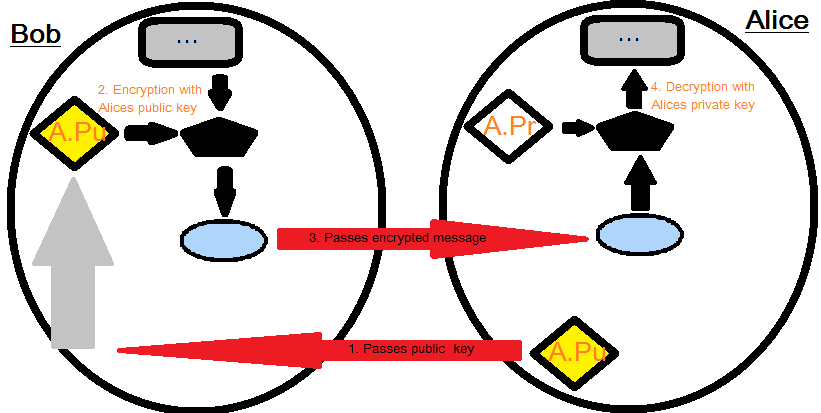
* Šibki ključi
* Nezavarovani prenos ključev
* Hitrost kodiranja
* Prilagodljivost
* Avtentikacija
* Zanesljivost

## KRIPTOGRAFSKA ZGOŠČEVALNA FUNKCIJA

Kriptografske zgoščevalne funkcije, so funkcije ki pretvori poljubno dolg niz v bloke konstantne dolžine ter tako tvori vrsto odtisa le tega niza. Od teh funkcij je pričakovano, da ne obstajata dva različna niza z istim odtisom, to pomeni da če spremenimo niz, posledično se spremeni tudi odtis, ter da se isti niz vedno preslika v isti odtis. Kriptografska zgoščevalna funkcija je tudi enosmerna, kar pomeni da iz odtisa je skoraj nemogoče dobiti originalen niz.

# ASIMETRIČNA KRIPTOGRAFIJA

Asimetrična kriptografija oziroma kriptografija javnega ključa poteka na principu, da ima vsak sistem dva ključa, enega javnega in enega zasebnega. Ta dva ključa sta medsebojno matematično povezana, to pomeni, da z enim lahko sporočilo zakodiramo ampak ga ne moremo tudi dekodirati, da bi to sporočilo dekodirali rabimo drugi ključ. Tako so ene ključ poimenovali zasebni ključ, drugega pa javni ključ. Prednost tega sistema je, da ko hočeš nekomu poslati sporočilo, boš uporabil njegov javni ključ, in četudi nekdo drugi pridobi javni ključ, sporočila ne more več dekodirati, dekodira ga lahko le oseba z zasebnim ključem. To pomeni da varnost kriptografskega sistema ni odvisna od izmenjave klučev, temveč o kvaliteti hranjenja zasebni ključ.



Slika : Prikaz asimetrične kriptografije

Specifično na primeru slike 4, Bob hoče poslati sporočilo Alice. Zato Bob prosi Alice za njen javni ključ. Ko Alice pošlje svoj javni ključ, ga lahko kdorkoli vidi njen ključ, vidi ga tudi Bob, ki ga nato uporabi da sporočilo zakodira. Sedaj ko je sporočilo zakodirano, ga z javnim ključem ni mogoče dekodirati, kar pomeni, da tudi Bob ne more dekodirati sporočila. Sporočilo pošlje Alice, takrat ga lahko kdorkoli vidi, ampak ker ga ne more z javnim ključem dekodirati, mu ta ni v uporabo. Alice prejme sporočilo in ga lahko dekodira le ona, ker ima zasebni ključ.

## DIGITALNA POTRDILA

Digitalna potrdilo je elektronski dokument, ki se uporablja za dokaz javnega ključa, zato se imenuje tudi potrdilo javnega ključa, dokazuje da tisti ki se predstavlja je resnično ta oseba. Digitalno potrdilo vsebuje podatke o ključu, informacije o lastniku in digitalni podpis. Deluje na zelo podobnem principu kakor asimetrična kriptografija, in tudi uporablja iste javne in zasebne ključe. Razlika je, da tokrat to sporočilo oseba zakodira s svojim zasebnim ključem, ter nato lahko kdorkoli to dekodira in preveri z javnim ključem te osebe.

# VIRI IN LITERATURA

Kolak, A. (online). (Univerza v Ljubljani Fakulteta za družbene vede): Pomen in vloga kriptografije in kriptoanalize na področju zagotavljanja nacionalne varnosti. (citirano 4.11.2018). Dostopno na naslovu: <<http://dk.fdv.uni-lj.si/dela/Kolak-Anja.PDF>>.

Wikipedija. (online). (<https://wikimediafoundation.org/>): Kriptografija. (citirano 4.11.2018). Dostopno na naslovu: <<https://sl.wikipedia.org/wiki/Kriptografija>>.

Apple Inc. (online). (Apple Inc.): Cryptography Concepts In Depth. (citirano 4.11.2018). Dostopno na naslovu: <<https://developer.apple.com/library/archive/documentation/Security/Conceptual/cryptoservices/CryptographyConcepts/CryptographyConcepts.html>>.

Blockgeeks. (online). (Blockgeeks): Cryptographic hash functions. (citirano 4.11.2018). Dostopno na naslovu: <<https://blockgeeks.com/guides/cryptographic-hash-functions/>>.

Preneel, B.; The State of Cryptographic Hash Functions. V: Lectures on data security : modern cryptology in theory and practice / Ivan Damgård (ed.), Lecture notes in computer science, Vol. 1561, Berlin [etc.] : Springer, 1999, str. 158-183.

Salvail, L.; The Search for the Holy Grail in Quantum Cryptography. V: Lectures on data security : modern cryptology in theory and practice / Ivan Damgård (ed.), Lecture notes in computer science, Vol. 1561, Berlin [etc.] : Springer, 1999, str. 183-217.

Wolf, S.; Unconditional Security in Cryptography. V: Lectures on data security : modern cryptology in theory and practice / Ivan Damgård (ed.), Lecture notes in computer science, Vol. 1561, Berlin [etc.] : Springer, 1999, str. 217-249.

DUJELLA, Andrej, in MARETIĆ, Marcel. 2007. Kriptografija. Zagreb: Element. ISBN 978-953-197-565-0.

BORUT, Pogačnik. 2006. Teorija kriptologije: Seminar pri predmetu Porazdeljeni informacijski sistemi in celovitost podatkov [online]. [Datum zadnjega popravljanja; 9. Sep. 2006; 11:10:23], [Citirano 25. Feb. 2019; 19:32:03]. Dostopno na spletnem naslovu: <<http://www.lait.fe.uni-lj.si/Seminarji/b_pogacnik.pdf>>.

Mansoor, Ebrahim et al. 2013. Symmetric Algorithm Survey: A Comparative Analysis. International Journal of Computer Applications, vol. 61, str. 12 – str. 19. ISSN 0975 –8887.

1. Steganografija – Je del kriptologije, ki se ukvarja s prenašanjem sporočil na prikrite oziroma zakrite načine. [↑](#footnote-ref-1)