Projektna Mapa

Načrt Projektne naloge pri informatiki

Ljubljana, šolsko leto 2018/19 Avtor: Luka Orlić

# Osnovni podatki o projektni nalogi:

|  |  |
| --- | --- |
| Naslov naloge: | Moderna Kriptografija |
| Avtor: | Luka Orlić |
| Elektronski naslov: | luka@orlic.si |
| Mentorica: | Prof. Marina Trost |

# Predstavitev zamisli naloge:

Tema projektne naloge je moderna kriptografija oziroma kriptografija s pomočjo algoritmov digitalnih računalnikov. V teoretičnem delu projektne naloge bom opisal uporabo kriptografije, ter površinsko pokril razliko med kriptografijo in stenografijo, v drugem delu bom naredil delitev kripotgrafije (Zgoščevalna funkcija, digitalni podpis, simetrične algoritme, asimetrične algoritme) in vse razložil, poglobil se bom v simetrične in zgoščevalne funcije, asimetrične algoritme bom pokril le v osnovi, saj bo sošolec to področje pokril v svoji projektni nalogi vse to je v dogovoru z mentorico Prof. Marino Trost (glej [točko 4](#_Konzultacija_z_mentorico)). V praktičnem delu bom naredil program z enkripcijo in dekripcijo, ki uporblja vsaj tri algoritme, ti algoritmi so: XOR chiper, Triple DES, Vigenere cipher

Cilji so:

1. Splošna razlaga namena kriptografije in razlike od stenografije.
2. Osnovna razlaga vsakega dela kriptografije.
3. Poglobljena razlaga simetričnih algoritmov in zgoščevalnih funkcij
4. Uresničitev praktičnega dela (3 algoritmi)

Način dela:

Del ob potekalo razdeljeno v treh delih. Prvi in drugi del bosta pokrila teoretični del projektne naloge, dokler bo tretji del pokrival praktični del projektne naloge. V prvem oziroma raziskovalnem delu, bom zbral in raziskal vsa potrebna znanja in informacije glede projektne naloge, v drugem delu oz. pisnem delu, bom napisal ter oblikoval projektno nalogo in s tem izpolnil prve tri cilje (i., ii. in iii.). Nalogo bom zaključil s tretjim oz. praktičnim delom tako, da bom napisal program, ki bo uporabljal vsaj 3 algoritme. Tako bo izpolnjen tudi zadnji cilj (iv.).

# 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.

# Konzultacija z mentorico

24.10.2018 – Pogovor glede projektne naloge sošolca, katerega naloga delno pokriva lastno projektno nalogo – Sklep: Da se sam s sošolcem dogovorim, kdo bo kaj opisal.

Ker sošolčeva naloga (Anže Hočevar - RSA Enkripcija in deljenje datotek prek TCP protokola) v večjem delu nanaša na področje asimetrične enkripcije oziroma kriptografije kot moja naloga, sva sklenila da bo on to tudi prevzel za opis.

5.11.2018 – Dogovor glede praktičnega dela ter ponovna obnova prejšnih dogovorov.

Dogovorili smo se, da praktični del, ki bo vseboval vsaj tri algoritme (XOR Cypher, Vigenère Cipher, Triple DES) narejen tako, da XOR Cypher in Vigenère cipher bosta ročno napisana oziroma sprogramirana dokler pa bo Triple DES naložen z “knjižnice”.

# Seznam opravil, nalog, problemov

|  |  |
| --- | --- |
| Kaj že vem? | Česa še ne vem?/naloge |
| Delitev kriptografije | Kako izprogramirati XOR in Vigenère algoritem |
| Simetrični algoritmi | Programski jezik za praktični del |
| Osnove A-simetričnih algoritmov | V kateri meri omeniti stenografijo? |
|  | Poskušati implimentacije stenografije v program? |
|  | Zakaj natančneje se uporablja kriptografija |
|  | Zgoščevalne funkcije |
|  | Najbolj varni algoritem |
| Ali post-kvanta enkripcija spade v moderno kriptografijo |

# Ovrednotenje projektne naloge: