Mooie voorpagina in de maak. Even geduld a.u.b

Inhoudsopgave

Hier een mooie inhoudsopgave maken, misschien met een licht show?

1. Voorwoord
2. De geschiedenis van Cryptografie
3. De modernisering van Cryptografie
4. De huidige versleuteling van banken
5. One time Pad encryptie
6. Problemen van de praktische opdracht
7. De code van de praktische opdracht uitgelegd
8. bronnenlijst

Voorwoord

Ik heb besloten om mijn profielwerkstuk te doen over cryptografie. Cryptografie is een soort geheimschrift dat wordt gebruikt om in het geheim berichten te versturen. Met het versleutelen van berichten kan je dus voorkomen dat een derde persoon bijvoorbeeld meekijkt, die kan het bericht dan wel lezen maar het niet snappen.

Bij dit profielwerkstuk zal ook een praktisch deel zitten, namelijk het schrijven van een werkende app of applicatie die een bepaalde tekst voor je versleuteld, en weer ontsleuteld. Hoe ik dit ga doen weet ik nog niet helemaal, als het een app wordt dan schrijf ik het in Java. Als ik Java ga gebruiken dan gebruik ik Eclipse of Android Studio van Google, omdat die enorm gebruiksvriendelijk is. Het algoritme dat ik nodig heb moet ik van het internet ‘stelen’ en zodanig aanpassen dat het precies is wat ik nodig heb.

De geschiedenis van cryptografie

Vroeger werd cryptografie alleen gebruikt om er voor te zorgen dat een leesbaar bericht onleesbaar werd gemaakt, en bij de ontvanger weer leesbaar werd gemaakt zodat mensen die mee willen lezen een bericht voor zich krijgen wat onleesbaar is. Cryptografie werd gebruikt om de veiligheid van spionnen, diplomaten en andere belangrijke mensen waarvan het belangrijk is dat hun identiteit of positie geheim blijft te handhaven. Tegenwoordig wordt cryprografie gebruikt voor het checken van de integriteit van een bericht, identiteit authenticatie, digitale handtekeningen en vele andere dingen.

De vroegste vormen van ‘geheimschrift’ was niet meer dan het normaal opschrijven van het bericht omdat toen heel veel mensen niet konden lezen en schrijven. Toen er steeds meer mensen konden lezen en schrijven moest er een echte vorm van cryptografie uitgevonden worden. De klassieke cijfers (cipher) die er zijn zijn het substitutiecijfer dat op een systematische manier een letter of een groep letters de waarde van een andere letter, of groep letters, geeft. Zo wordt de zin “Ik ben Kees” bijvoorbeeld: "Gf whj Fhhn”, wat compleet onleesbaar is als je de goede code niet hebt. Het Caesar cijfer, afstammend van de Roeminse tijd. In deze cijfer werd elke letter van het alfabet een andere vaste waarde gegeven verder in het alfabet, of juist minder ver. Julius Casear gebruikte een ‘shift’ van drie om te communiceren met zijn generaals, de letter c kan dan een a worden of een f, en dit ging zo met het hele alfabet. De zwakheid van deze manier van cryptografie is dat je kan kijken naar hoevaak een bepaalde letter gebruikt wordt, en kijkt naar hoe vaak een letter normaal gesproken gebruikt wordt, op deze manier kan je een tekst die met de substitutiecijfer versleuteld is ontsleutelen.