Onderzoeksidee

Constantin Blach, s4329872

1 Onderwerp

Mijn onderzoek gaat over een mogelijke additie aan het Rijndael ecryptie algoritme, wat ondertussen beter onder Advanced Encryption Standard (AES) bekend is. AES is inmiddels al rond tien jaar het grondprincipe van encrypties online. Het algoritme is een symmetrische algoritme, en- en decryptie werkt dus met dezelfde sleutel.

2 Probleemstelling

AES gebruikt merdere (afhankelijk van de lengte van de sleutel) encryptie ronden, waar elke ronde drie stappen bevat. Bij deze stappen worden functies gebruikt, die in een specific getallen field werken. Voor alle berekeningen wordt een binary Galois-Field(2^n) gebruikt. Meestal wordt hier van GF(2^8) (bevat getallen van 0 t/m 255) gebruik gemaakt.

Mijn hoofdvraag is dan, of het van voordeel kan zijn, om een ander getallenfield te gebruiken. Vooral kan het handig zijn, om GF(p) (p is prime) te kiezen. Daardoor kan het gekozen field misschien rare characteristics opwijzen, waardoor het voor een aanvaller moeilijk kan zijn, om de sleutel uit te vinden.

Ik moet dus zelf eigen functies bedenken, die in een GF(p) berekeningen uitvoeren, waardoor het moeilijke wordt om het te achtervolgen.

Een mogelijke deelvraag/fallback kan zijn, om de data, die we willen versleutelen, eerst in het goede formaat in GF(p) te krijgen, wat we dan met ons algoritme kunnen versleutelen. Natuurlijk moet aan het eind, na de decryptie weer dezelfde data tevoorschijn komen.

3 Verantwoording

AES zoals het nu is, is al relatief zeker. Een mogelijk aanvaller zou rond 2^126 berekeningen moeten doen, om de makkelijkste versie van AES te kunnen breken. Dit aantal is misschien nu nog ok, maar in de toekomst, met nog betere rekeningskracht, zou het vast te makkelijk zijn, om aan de gezochte key te komen.

Daarom zou het handig zijn, om het op dit moment meest gebruikte encryptie algoritme uit te breiden en wat zekerder te maken, om al tegen mogelijke aanvallen beveiligd te zijn.

4 Theoretisch kader

Het meest belangrijke concept voor dit werk is natuurlijk hoe AES in elkaar zit, hoe het werkt en wat de mogelijke problemen zijn. Hier is veel informatie over te vinden, bijvoorbeeld bij een Dozent van de RU, Joan Daemen, die AES mee heeft bedacht.

In het begin zijn vooral informatie over algoritme belangrijk, zodat ik misschien een mogelijke verbetering of problemen kan vinden. Hier zijn vooral boeken, maar ook papers over geschreven. (1,2)

Bovendien is AES het meest gebruikte algoritme in het internet. Daarom is er ook al veel onderzoek na gedaan, omdat het erg belangrijk is, dat AES betrouwbaar is.

Er zjn ook recente papers, die al met de beveiliging van AES te maken hebben. Er worden al een aantal problemen met AES gevonden, die tot nu toe nog niet gevaarlijk zijn, omdat we nog te weinig rekenkracht hebben om het te breken. (3)

5 Methode

AES gebruikt drie functies per encryptie ronde. Om te kunnen testen, hoe goed mijn bedachte functies werken, moet ik ze dus met de huidige implementatie van AES vergelijken.

Misschien zou ik ook mijn resultaten aan crypto experten kunen geven, om te kijken, of ze leaking informatie daaruit kunnen halen. (Blijft het dan nog mijn werk?)

6 Literatuur

1. Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners, 1st edn. Springer Publishing Company, Incorporated (2009)

2. M.Pitchaiah, Philemon Daniel, Praveen: Implementation of Advanced Encryption Standard Algorithm (2012)

3. Joni Moenttinen: The Security of Advanced Encryption Standard (2015)