FRiDA gymnasiet Vänersborg

2022/2023

The AES encryption algorithm

En undersökning av The Advanced Encryption Standard (AES)

Klass:
NA20

Författare:
Gabriel Lindeblad

Handledare:
Rickard Janveden

Program:
Naturvetenskapsprogrammet

August 30, 2022

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut lacinia ex eget sagittis congue. Nullam cursus egestas dolor, suscipit gravida magna ultrices sit amet. Nullam placerat dui eu arcu pharetra, sit amet tempor dolor convallis. Aenean sodales condimentum turpis, commodo maximus augue. Aenean vel nibh dui. Pellentesque ex libero, lacinia nec mauris vel, convallis consectetur felis. Maecenas ut nibh sed magna maximus imperdiet at id purus. In vel consequat metus. Donec non tincidunt nunc. Sed pulvinar odio ut sapien vestibulum, quis mollis arcu tempor. Maecenas ut sem leo. Sed leo risus, mollis eu ex vitae, feugiat consequat metus. Aenean interdum volutpat urna, nec tempor mi accumsan quis. Morbi blandit maximus urna non aliquet aes.

Inehållsförteckning

Acronymer

AES Advanced Encryption Standard

CBC Cipher Block Chaining mode

ECB Electronic Code Book mode

OFB Output Feedback mode

1 Introduktion

Dator, mobiltelefon och till och med bil är några uta av dom saker som idag alla är uppkopplade till internet. Information om allt från position och uppdateringar till kockslag och väder skickas från enhet till enhet runt om oss. Utav detta så är mycket vad vi kallar privat information som vi helst inte vill att vem som helst ska kunna se. På grund av just denna anledning så används något som kallas kryptering för att dölja informationen från nyfikna mellanhänder.

I mordentid så är det absolut vanligast att Advanced Encryption Standard (AES) används för att kryptera våran information.

1.1 Syfte

Syftet med denna undersökning är att undersöka krypterings algoritmen AES, för att utveckla en förståelse för mer avancerad krypterings algoritmer. Samt att bygga en uppfattning om hur man på olika sätt kan implementera krypterings algoritmer och vad de får för betydelse för deras säkerhet och hastighet.

1.2 Frågeställningar

- Hur påverkas tiden de tar att kryptera något mellan de olika nyckel längderna 128-bit, 192-bit och 256-bit nyckel?
- Hur påverkas algoritmen av de olika körlägen och vilken betydelse får de för den resultatet?
- Hur förändras tiden de tar att kryptera något beroende på ifall algoritmen körs i ECB, CBC eller OFB samt vilken betydelse ur ett användnings perspektiv de får?

1.3 Avgränsning

Denna rapport är inte en komplett utvärdering av AES och dess användning utan fokuserar enbart på hur nyckellängd och körläge påverkar krypteringstiden. Detta samt hur den resulterande chiffer texten påverkas av vissa körlägen och hur detta då i sin tur kan påverka säkerheten.

Denna analys av algoritmens säkerhet är alltså inte en komplett säkerhets utvärdering och tar inte hänsyn till faktorer så som möjliga attacker där ibland exempelvis Brute-Force[1] & Side-Channel[2] attacker. Undersökningen är även begränsad till en mjukvaruimplementering och tar inte hänsyn till möjliga skillnader som kan uppstå när algoritmen implementeras på en hårdvarunivå.

[1] Neeraj Kumar. "Investigations in brute force attack on cellular security based on des and aes". In: *IJCEM International Journal of Computational Engineering & Management* 14 (2011), pp. 50–52.

[2] Mathieu Renauld, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. "Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA". in: *Cryptographic Hardware and Embedded Systems - CHES 2009*. Ed. by Christophe Clavier and Kris Gaj. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 97–111. ISBN: 978-3-642-04138-9.

2 Bakgrund

2.1 Kryptografi

Ifall man nu vänder sig mot de möjliga felkällorna som finns kan man exempelvis ta upp de faktum att kaliumpermanganatlösningens (KMnO4) koncentration kan ha påverkats av ljuset i rummet. Bland annat skulle detta kunna ske från de att lösningen hällts ut ur sina mörka flaskor och i byretten som till skillnad från flaskorna är klart genomskinlig och stoppar inget ljus. Detta skulle i och med detta kunna vara en möjlig systematisk felkälla som kan ligga till grunden till varför många av värden blev alldeles för stora och till och med översteg 100% vilket är ett helt orimligt resultat. En liknande systematisk felkälla skulle även kunna vara att exaktheten av koncentrationen på kaliumpermanganatlösningen (KMnO4) kan ha varierat mellan behållare, vilket då kan vara en av anledningarna till de mönster så syns bland resultat värdena. Detta då vissa av resultaten på ett sätt ser ut att gruppera sig i grupper där värden inte varierar hur mycket som helst mellan varandra. Bland annat så kan man se detta väldigt tydligt bland de rödmarkerade värdena som är över 100% där dom mellan sig skiljer sig som mest med ca 20 procentenheter. Detta medans det minsta värdet av de rödmarkerade skiljer sig med ca 20 procentenheter till de högsta grön markerade värdet. Samtidigt som skillnaden bland de grön markerade värdena maximalt ligger på ca 20 procentenheter. Ytterligare en felkälla skulle kunna vara avläsningen av volymen kaliumpermanganatlösning (KMnO4) konsumerad vid titreringen. Avläsningen är en sak som bygger på en fysisk observation av en person som får avgöra vad volymen blir utifrån skalan på byretten och vätskenivån. Detta introducerar då en slumpmässig felkälla som påverkar resultatets säkerhet negativt. Något som även ytterligare ökar påverkan från denna felkälla är det faktum att avläsningen ytterligare försvårades på grund av kaliumpermanganatlösningens (KMnO4) mörka färg som gjorde de svårt att avläsa skalan på byretten. Denna felkälla får även en ännu större betydelse ifall man även var tvungen att fylla på byretten en extra gång under titrerings processen, detta då man exempelvis får två värden som de kan uppkomma ett visst fel på samtidigt som de även introducerar ett tredje värde med en viss osäkerhet då man möjligen inte riktigt lyckas fylla byretten till ett exakt sträck på skalan. Ännu en felkälla skulle även kunna vara bestämmelsen av när man nått ekvivalens punkten då man enligt metoden når ekvivalens punkten när den titrerade lösningen blir rosalila i minst 30 sek efter en droppe. Detta innebär att även ifall man använder ett tidtagarur för att ta tiden på färgomslaget så introduceras ytterligare en osäkerhet. Bland annat beror de på att man kan uppfatta vad som är rätt färg för när ekvivalens punkten är nådd olika från person till persons, vilket då skapar en viss subjektivitet då lösningen inte helt i vissa fall blir en helt exakt klar färg av rosalila direkt. I och med detta så skulle de kunna ha en påverkan på resultatet och på så vis även de slutliga resultatets säkerhet. Denna felkälla får även en ännu större betydelse ifall man även var tvungen att fylla på byretten en extra gång under titrerings processen, detta då man exempelvis får två värden som de kan uppkomma ett visst fel på samtidigt som de även introducerar ett tredje värde med en viss osäkerhet då man möjligen inte riktigt lyckas fylla byretten till ett exakt sträck på skalan. Ännu en felkälla skulle även kunna vara bestämmelsen av när man nått ekvivalens punkten då man enligt metoden når ekvivalens punkten när den titrerade lösningen blir rosalila i minst 30 sek efter en droppe. Detta innebär att även ifall man använder ett tidtagarur för att ta tiden på färgomslaget så introduceras ytterligare en osäkerhet. Bland annat beror de på att man kan uppfatta vad som är rätt färg för när ekvivalens punkten är nådd olika från person till persons, vilket då skapar en viss subjektivitet då lösningen inte helt i vissa fall blir en helt exakt klar färg av rosalila direkt. I och med detta så skulle de kunna ha en påverkan på resultatet och på så vis även de

slutliga resultatets säkerhet.

2.1.1 Uppkomst

abstract

2.1.2 Användning

abstract

3 Teori

3.1 Kryptering

abstract

3.2

3.3 section 3

4 Metod & Genomförande

4.1 Implementering

abstract

4.2 Test Uppsättning

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut lacinia ex eget sagittis congue. Nullam cursus egestas dolor, suscipit gravida magna ultrices sit amet. Nullam placerat dui eu arcu pharetra, sit amet tempor dolor convallis. Aenean sodales condimentum turpis, commodo maximus augue. Aenean vel nibh dui. Pellentesque ex libero, lacinia nec mauris vel, convallis consectetur

4.3 Genomförande

5 Resultat

5.1 section 1

abstract

5.2 section 2

5.3 section 3

6 Diskussion

6.1 section 1

abstract

6.2 section 2

fotnotes are here aes and agian aes

6.3 section 3

Källförteckning

Kumar, Neeraj. “Investigations in brute force attack on cellular security based on des and aes”. In: *IJCEM International Journal of Computational Engineering & Management* 14 (2011), pp. 50–52.

Renauld, Mathieu, François-Xavier Standaert, and Nicolas Veyrat-Charvillon. “Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA”. In: *Cryptographic Hardware and Embedded Systems - CHES 2009*. Ed. by Christophe Clavier and Kris Gaj. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 97–111. ISBN: 978-3-642-04138-9.

Figurer