

The AES encryption algorithm

En undersökning av The Advanced Encryption Standard (AES)

Klass:

NA20

Författare:

Gabriel Lindeblad

Handledare:

Rickard Janveden

Program:

Naturvetenskapsprogrammet

August 26, 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

1	Introduktion	3
1.1	Syfte	3
1.2	Frågeställningar	3
2	Bakgrund	4
2.1	section 1	4
2.1.1	section 2	5
2.1.1.1	section 3	5
3	Teori	6
3.1	section 1	6
3.2	section 2	6
3.3	section 3	6
4	Material & utförande	7
4.1	section 1	7
4.2	section 2	7
4.3	section 3	7
5	Resultat	8
5.1	section 1	8
5.2	section 2	8
5.3	section 3	8
6	Diskussion	9
6.1	section 1	9
6.2	section 2	9
6.3	section 3	9
	Källförteckning	10

1 Introduktion

Kryptering, något vi möter varje dag i dagens samhälle men...

När de vi idag kallar internet uppkom och öppnades för allmänheten så var tankarna på hur vår data och information

Hela tiden runt om oss skickas information digitalt från enhet till enhet. Information från höger till väster bara flödar ...

Information, en grundsten i dagens samhälle ...

1.1 Syfte

Syftet med denna undersökning är att undersöka krypterings algoritmen AES (Advanced Encryption Standard), 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 [och något mer], samt vilken betydelse ur ett användnings perspektiv får de?

2 Bakgrund

2.1 section 1

Ifall man nu vänder sig mot de möjliga felkällorna som finns kan man exempelvis ta upp de faktum att kaliumpermanganatlösningens (KMnO_4) koncentration kan ha påverkats av ljuset i rummet. Bland annat skulle detta kunna ske från de att lösningen hållts 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 (KMnO_4) 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 (KMnO_4) 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 (KMnO_4) 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 section 2

abstract

2.1.1.1 section 3

abstract

3 Teori

3.1 section 1

abstract

3.2 section 2

3.3 section 3

4 Material & utförande

4.1 section 1

abstract

4.2 section 2

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 section 3

5 Resultat

5.1 section 1

abstract

5.2 section 2

5.3 section 3

6 Diskussion

6.1 section 1

abstract[1]

6.2 section 2

footnotes are here¹ aes and again aes

6.3 section 3

¹this is the first footnote

Källförteckning

[1] Sverige, Jun 2022. 9