FRiDA gymnasiet Vänersborg

2022/2023

The AES encryption algorithm

En undersökning av The Advanced Encryption Standard (AES)

Klass:
NA20

Handledare:
Jimmy Nylén

Författare:
Gabriel Lindeblad

Program:
Naturvetenskapsprogrammet

1 september 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.

Innehåll

Ordlista

Python Python är ett högnivå programmerings språk byggt på programmerings språket C. De är skapat av Guido van Rossum och släpptes i Februari 1991.[2]

XOR ...

Akronymer

AES Advanced Encryption Standard

CBC Cipher Block Chaining mode

DES Data Encryption Standard

ECB Electronic Code Book mode

OFB Output Feedback mode

1 Inledning

I takt med att vårat samhälle i allt större utsträckning digitaliserats så har behovet utav att kunna hålla information privat också ökat. För att lösa detta så använder vi något kallat kryptering i syfte att dölja och skydda vår information. Kryptering är något som idag används nästan överallt i form av olika standarder så som AES och DES. Vad vi en gör så påverkas vi på något sätt av den när den skyddar våran information. På grund av detta så kan man förstå hur vikten av en grundläggande förståelse kan vara något viktigt

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". I: *IJCEM International Journal of Computational Engineering & Management* 14 (2011), s. 50–52.

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

2 Bakgrund

2.1 Kryptografi

2.1.1 Uppkomst

2.1.2 Utveckling

2.2 AES Uppkomst

3 Teori

3.1 Kryptering

3.2 Blockchiffer

3.2.1 Körlägen

3.2.1.1 ECB

3.2.1.2 CBC

3.2.1.3 OFB

3.3 Symetrisk & Asymmetrisk Kryptering

3.3.1 Symetrisk Kryptering

3.3.2 Asymmetrisk Kryptering

3.4 AES

3.4.1 AES-128bit

3.4.2 AES-192bit

3.4.3 AES-256bit

4 Metod & Genomförande

Metoden for denna undersökning bygger på en implementering av AES i programmeringsspråket Python. Detta tillsammans med ett antal konstruerade tester även dom implementerade i Python är vad som använts för undersökningen.

4.1 Implementering

4.2 Test Uppsättning

4.3 Genomförande

5 Resultat

5.1 Nyckellängds Test

5.2 Körläges Test

6 Diskussion & Slutord

6.1 Felkällor

6.2 Förbättringar

6.3 Slutsats

6.4 Slutord

XOR

Källförteckning

[Kum11] Neeraj Kumar. "Investigations in brute force attack on cellular security based on des and aes". I: *IJCEM International Journal of Computational Engineering & Management* 14 (2011), s. 50–52.

[Pyt22] Python Software Foundation. *What is Python?* 2022. URL: https://docs.python.org/3/faq/general.html#what-is-python (hämtad 2022-09-01).

[RSV09] Mathieu Renauld, François-Xavier Standaert och Nicolas Veyrat-Charvillon. "Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA". I: *Cryptographic Hardware and Embedded Systems - CHES 2009*. Utg. av Christophe Clavier och Kris Gaj. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, s. 97–111. ISBN: 978-3-642-04138-9.

Figurer