

# The AES encryption algorithm

En undersökning av The Advanced Encryption Standard (AES)

Klass:

**NA20**

Handledare:

**Jimmy Nylén**

Författare:

**Gabriel Lindeblad**

Program:

**Naturvetenskapsprogrammet**

# 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

<b>Ordlista</b>	<b>4</b>
<b>Akronymer</b>	<b>5</b>
<b>1 Inledning</b>	<b>6</b>
1.1 Syfte . . . . .	6
1.2 Frågeställningar . . . . .	6
1.3 Avgränsning . . . . .	6
<b>2 Bakgrund</b>	<b>7</b>
2.1 Kryptografi . . . . .	7
2.1.1 Uppkomst . . . . .	7
2.1.2 Utveckling . . . . .	7
2.2 AES Uppkomst . . . . .	7
<b>3 Teori</b>	<b>8</b>
3.1 Kryptering . . . . .	8
3.2 Blockchiffer . . . . .	8
3.2.1 Körlägen . . . . .	8
3.2.1.1 ECB . . . . .	8
3.2.1.2 CBC . . . . .	8
3.2.1.3 OFB . . . . .	8
3.3 Symetrisk & Asymmetrisk Kryptering . . . . .	8
3.3.1 Symetrisk Kryptering . . . . .	8
3.3.2 Asymmetrisk Kryptering . . . . .	8
3.4 AES . . . . .	8
3.4.1 Finite Fields . . . . .	8
3.4.2 Struktur . . . . .	8
3.4.2.1 SubBytes operation . . . . .	8
3.4.2.2 ShiftRows operation . . . . .	8
3.4.2.3 MixColumns operation . . . . .	8
3.4.2.4 AddRoundKey operation . . . . .	8
3.4.3 Nyckel utökning . . . . .	8
3.4.3.1 RotWord . . . . .	8
3.4.3.2 SubWord . . . . .	8
3.4.3.3 Rcon . . . . .	8
3.4.4 AES-128bit . . . . .	8
3.4.5 AES-192bit . . . . .	8
3.4.6 AES-256bit . . . . .	8
<b>4 Metod &amp; Genomförande</b>	<b>9</b>
4.1 Implementering . . . . .	9
4.2 Test Uppsättning . . . . .	9
4.3 Genomförande . . . . .	9
<b>5 Resultat</b>	<b>10</b>
5.1 Nyckellängds Test . . . . .	10

## *INNEHÅLL*

---

5.2 Körläges Test . . . . .	10
<b>6 Diskussion &amp; Slutord</b>	<b>11</b>
6.1 Felkällor . . . . .	11
6.2 Förbättringar . . . . .	11
6.3 Slutsats . . . . .	11
6.4 Slutord . . . . .	11
<b>Källförteckning</b>	<b>12</b>
<b>Figurer</b>	<b>13</b>

# Ordlista

<b>Caesarchiffer</b>	Caesarchiffer är ett substitutions chiffer, vilket helt enkelt bygger på att man byter ut varje bokstav i medelandet med en annan. Ersättningens bokstaven bestäms genom att man hoppar ett visst antal hopp i alfabetet som exempelvis 3 hopp, vilket då innebär att om man har bokstaven a då skulle den bli ett d istället.[ <a href="#">Wik21</a> ]
<b>Python</b>	Python är ett högnivå programmerings språk byggt på programmerings språket C. De är skapat av Guido van Rossum och släpptes i Februari 1991.[ <a href="#">Pyt22</a> ]
<b>XOR</b>	Ett logisk operation inom datorvetenskap som fungerar ungefär som + uttrycket, med den enda skillnaden att $1 \text{ xor } 1 = 0$ . Detta samt att xor är en binär operation, vilket innebär att termerna bara kan vara 0 eller 1 och resultatet det samma.[ <a href="#">LEW12</a> ]

# 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

Kryptering, en bärande grundsten i dagens digitaliserade samhälle. De är väggen mellan oss och resten av världen, ett läs runt våra liv. Kryptering bygger på ett simpelt koncept, att dölja informationen från all förutom den menade mottagaren. Ett koncept som exempelvis fanns redan för 2000 år sedan när Julius Caesar använde de vi idag kallar Caesarchiffer för att skicka hemliga meddelanden.<sup>1</sup> Sedan dess har kryptografi självklart utvecklats enormt och vi har gått från de på ett sätt simpla men även eleganta Caesarchiffer som användes då till moderna algoritmer så som Advanced Encryption Standard och Data Encryption Standard. Dessa algoritmer har samma syfte som Caesarchiffer men har utvecklats under en tid där datorer står som de dominerande informationshanteringsverktyget, vilket även är vad som används i denna rapport för att undersöka just en av dessa algoritmer.

## 1.1 Syfte

Syftet med denna undersökning är att undersöka krypterings algoritmen AES, för att utveckla en förståelse för mer avancerade 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 skifftertexten av de olika körlägen och vilken betydelse får de för den resultatet?
- Hur förändras tiden det tar att kryptera något beroende på ifall algoritmen körs i ECB, CBC eller OFB samt vilken betydelse det får ur ett tillämpningsperspektiv?

## 1.3 Avgränsning

Denna rapport är en avgränsad utvärdering av AES och dess användning som fokuserar på hur nyckellängd och körläge påverkar krypteringstiden. Detta samt hur den resulterande skifftertexten påverkas av vissa körlägen och hur detta i sin tur kan påverka säkerheten.

Denna analys av algoritmens säkerhet utelämnar faktorer så som möjliga attacker där ibland exempelvis Brute-Force<sup>2</sup> & Side-Channel<sup>3</sup> attacker. Undersökningen är även begränsad till en mjukvaruimplementering och tar inte hänsyn till möjliga skillnader som kan uppstå när algoritmen implementeras på en hårdvarunivå.

---

<sup>1</sup>Dennis Luciano och Gordon Prichett. “Cryptology: From Caesar ciphers to public-key cryptosystems”. I: *The College Mathematics Journal* 18.1 (1987), s. 2–17.

<sup>2</sup>Neeraj Kumar. “Investigations in brute force attack on cellular security based on des and aes”. I: *IJCCEM International Journal of Computational Engineering & Management* 14 (2011), s. 50–52.

<sup>3</sup>“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

Ordet kryptografi härstammar från de två grekiska orden kryptos som betyder gömd och grafein som betyder skrift.<sup>4</sup> I sin simplaste form handlar kryptografi alltså om att gömma information. Detta är något som har visat sig på många olika sätt genom historien från något så simpelt som att skriva ett medelande i text då många i början inte kunde läsa till att idag istället använda komplexa algoritmer.<sup>5</sup> Begreppet kryptografi har dock också fått en utökade betydelse med tiden då det idag även inkluderar olika metoder för att säkerställa autenticiteten av informationen och avsändaren.<sup>6</sup>

### 2.1.1 Uppkomst

Kryptografins historia kan man nästan säga börjar vid den tidigaste formen av skrift, vilket grundar sig i de faktum att de flesta inte kunde läsa. Detta är ju såklart något som förändrats på senare tid och i takt med de så har även kryptografin utvecklats. Exempel på utvecklingen går att se så tidigt som 1900 f.Kr då vissa egyptiska skribenter använde sig utav hieroglyfer på ett avvikande sätt, vilket troligen då gjordes i syfte att dölja informationen från dom som inte visste vad det skulle betyda.

Den tidiga kryptografin är även något som kan observeras hos romarna där man använde Caesarchiffer och hos grekerna. Där grekernas metod byggde på att man virade en tejpbil runt någon form av ett cylinderformat objekt och sedan skrev medelandet på tejpen. När tejpen sedan togs av så är texten oläslig och mottagaren behövde vira upp tejpen på ett cylinderformat objekt med samma diameter för att läsa det.<sup>7</sup>

### 2.1.2 Utveckling

## 2.2 AES Uppkomst

---

<sup>4</sup>Wikipedia. *Kryptografi*. 2020. URL: <https://sv.wikipedia.org/w/index.php?title=Kryptografi&oldid=48532107> (hämtad 2022-09-07).

<sup>5</sup>Tony M Damico. “A brief history of cryptography”. I: *Inquiries Journal* 1.11 (2009).

<sup>6</sup>Nationalencyklopedin. *kryptografi*. 2022. URL: <http://www.ne.se/uppslagsverk/encyklopedi/1%C3%A5ng/kryptografi> (hämtad 2022-09-07).

<sup>7</sup>Dam09.

# **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 Finite Fields**

### **3.4.2 Struktur**

**3.4.2.1 SubBytes operation**

**3.4.2.2 ShiftRows operation**

**3.4.2.3 MixColumns operation**

**3.4.2.4 AddRoundKey operation**

### **3.4.3 Nyckel utökning**

**3.4.3.1 RotWord**

**3.4.3.2 SubWord**

**3.4.3.3 Rcon**

### **3.4.4 AES-128bit**

### **3.4.5 AES-192bit**

### **3.4.6 AES-256bit**

# **4 Metod & Genomförande**

Metoden för 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 används 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**

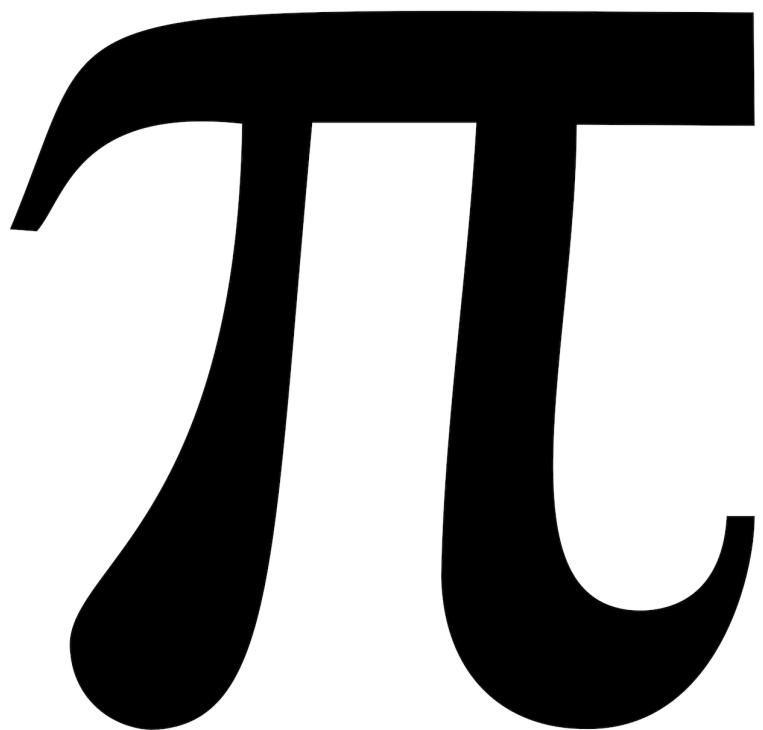
XOR

# Källförteckning

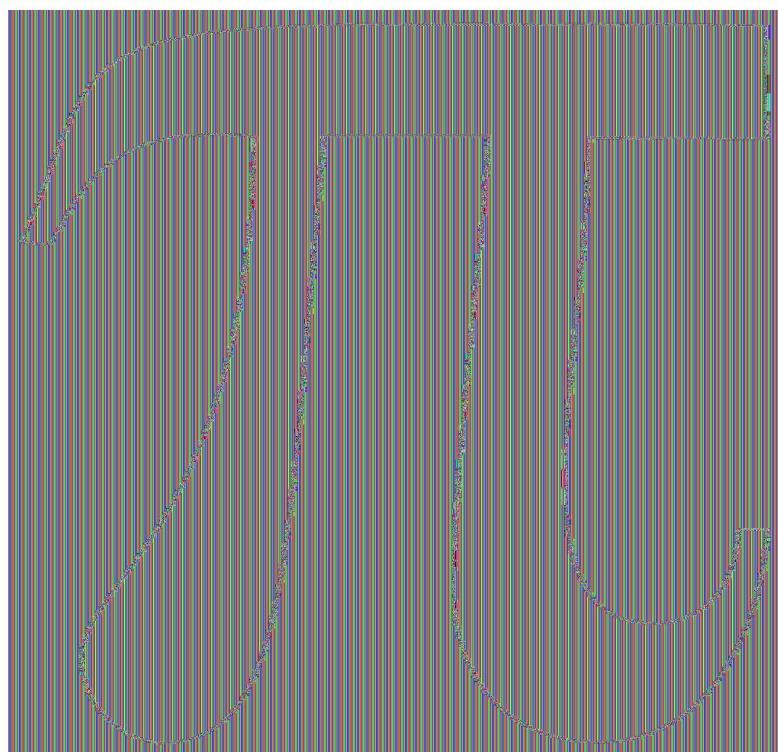
- [CG09] “Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA”. I: *Cryptographic Hardware and Embedded Systems - CHES 2009*. Utg. av Christophe Clavier och Kris Gaj. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, s. 97–111. ISBN: 978-3-642-04138-9.
- [Dam09] Tony M Damico. “A brief history of cryptography”. I: *Inquiries Journal* 1.11 (2009).
- [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.
- [LEW12] FEATURE MICHAEL LEWIN. “All about XOR”. I: *For details of ACCU, our publications and activities, visit the ACCU website: www. accu. org* (2012), s. 14.
- [LP87] Dennis Luciano och Gordon Prichett. “Cryptology: From Caesar ciphers to public-key cryptosystems”. I: *The College Mathematics Journal* 18.1 (1987), s. 2–17.
- [Nat22] Nationalencyklopedin. *kryptografi*. 2022. URL: <http://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/kryptografi> (hämtad 2022-09-07).
- [Pyt22] Python Software Foundation. *What is Python?* 2022. URL: <https://docs.python.org/3/faq/general.html#what-is-python> (hämtad 2022-09-01).
- [Wik20] Wikipedia. *Kryptografi*. 2020. URL: <https://sv.wikipedia.org/w/index.php?title=Kryptografi&oldid=48532107> (hämtad 2022-09-07).
- [Wik21] Wikipedia, the free encyclopedia. *Caesarchiffer*. 2021. URL: <https://sv.wikipedia.org/w/index.php?title=Caesarchiffer&oldid=48885737> (hämtad 2022-09-23).
- [Wik99] Wikipedia, the free encyclopedia. *Advanced Encryption Standard*. 1999. URL: [https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard#/media/File:AES\\_\(Rijndael\)\\_Round\\_Function.png](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#/media/File:AES_(Rijndael)_Round_Function.png) (hämtad 2022-09-02).

# Figurer

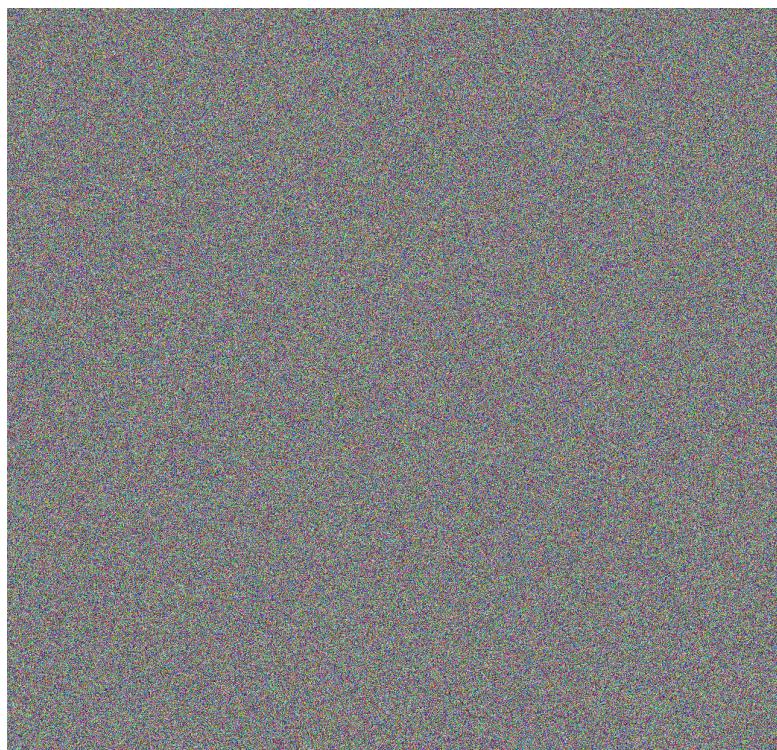
8.1	Före Kryptering . . . . .	14
8.2	Efter ECB Kryptering . . . . .	14
8.3	Efter CBC Kryptering . . . . .	15
8.4	Efter OFB Kryptering . . . . .	15
8.5	Uppställning av vanliga rundor . . . . .	16



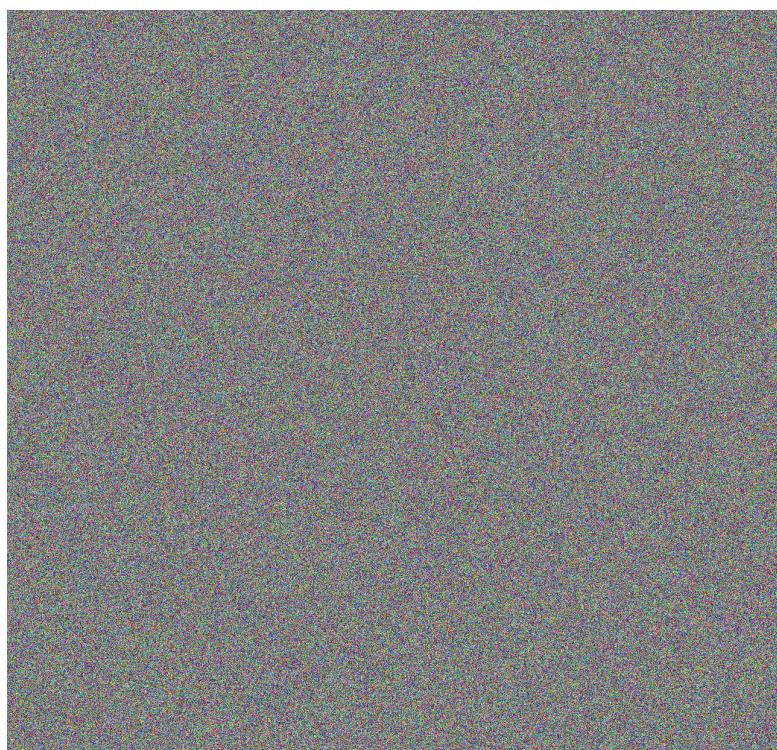
Figur 8.1: Före Kryptering



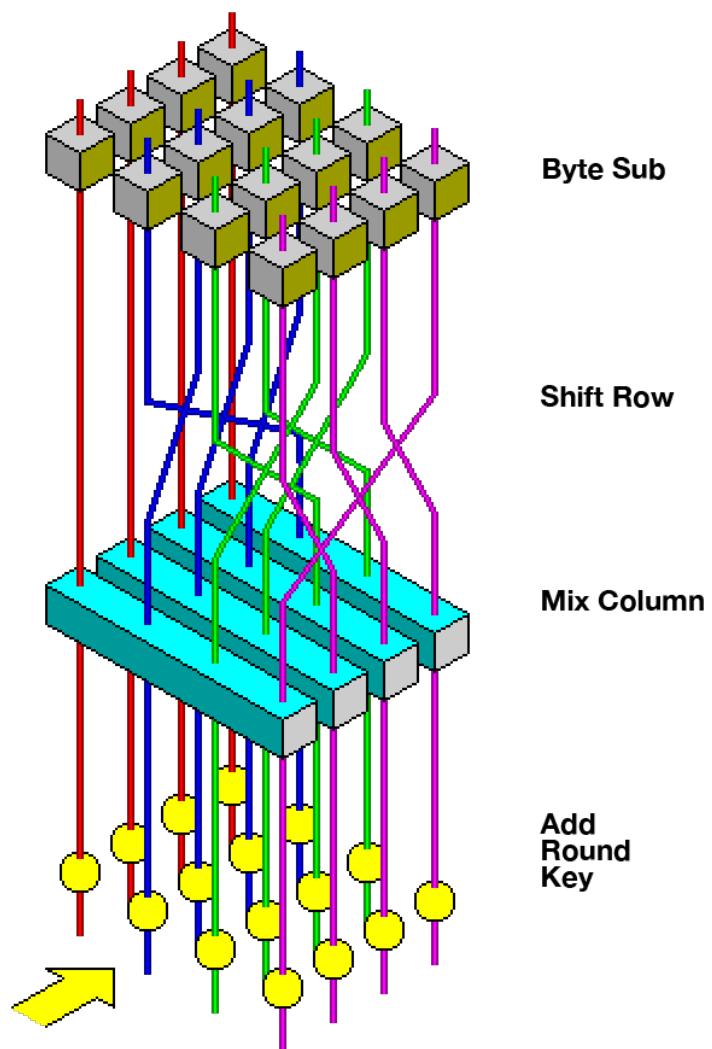
Figur 8.2: Efter ECB Kryptering



Figur 8.3: Efter CBC Kryptering



Figur 8.4: Efter OFB Kryptering



Figur 8.5: Uppställning av vanliga runder

Källa: Wikipedia, the free encyclopedia. *Advanced Encryption Standard*. 1999. URL: [https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard#/media/File:AES\\_\(Rijndael\)\\_Round\\_Function.png](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#/media/File:AES_(Rijndael)_Round_Function.png) (hämtad 2022-09-02)