Navn:

Fødselsdato:

Skole:

Fag:

bekend,)

Dato for prøveaflæggelse:

Middelfart Gymnasium & HF

Studieretningsprojekt 2020

Fag:	Vejleder:
Matematik A	
Engelsk A	

Opgaveformulering:

Der ønskes en analyse og fortolkning af Mark Haddons *The Curious Incident of the Dog in the Night-time* (2003) med særligt fokus på skrivestil og genre.

Gør matematisk rede for primtal og for relevante dele af den matematiske teori, der ligger til grund for RSA kryptosystemet. Beskriv på baggrund heraf kryptosystemets virkemåde, og vis som eksempel hvordan teksten "ANNA" krypteres og dekrypteres med den offentlige nøgle n = 2059 og selvvalgt e.

Inddrag overvejelser om afkodning i kryptosystemer i en diskussion af "afkodning" som metafor for hovedkarakteren Christophers adfærd, tanker og omverdensrelationer.

Forventet omfang: 15-20 sider á 2400 anslag med mellemrum, inklusiv fodnoter, men eksklusiv forside, resume, indholdsfortegnelse, litteraturliste og bilag.

Med aflevering i Netprøver erklærer jeg mig enig i, at opgavebesvarelsen er udarbejdet af mig. Jeg har ikke anvendt tidligere bedømt arbejde uden henvisning hertil, og opgavebesvarelsen er udfærdiget uden anvendelse af uretmæssig hjælp og uden brug af hjælpemidler, der ikke har været tilladt under prøven.

Resume

Opgaven redegør for RSA-kryptering og den bagvedliggende talteori som primtalsfaktorisering, Euklids algoritme og Bezouts identitet. Opgaven analyserer Mark Haddons roman ”The Curious Incident of the Dog in the Night-Time”, hvor der er et særligt fokus på personkarakteristik af hovedpersonen og det forhold, han har til andre. Derudover er der også fokus på skrivestil, genre og matematikkens betydning for romanens hovedperson Christopher. Til slut diskuteres det, hvilken sammenhæng RSA-kryptosystemets opbygning har til Christophers måde at begå sig i verden, og hvordan det kan forstås som en metafor for hans egen og andres kommunikation og forståelse. Resultatet af analysen viser, at matematikken og særlige karakteristika ved at leve med Aspergers syndrom har en stor betydning for, hvordan Christopher ser og afkoder verden på. Det ses gennem skrivestilen i romanen, hvor fortælleren er Christopher selv. Derudover konkluderer opgaven, at Christopher kan forstås som romanens største mysterium, fordi det også for læseren kan være svært at dekryptere Christophers tankegang.

Indholdsfortegnelse

Indledning **4**

1. Talteori **4**

1.1 Primtal 4

1.2 Primtalsfaktorisering 5

1.3 Euklids algoritme og Bezouts identitet 6

2. RSA-kryptering **7**

2.1 Dannelsen af nøgler 8

2.2 Enkryptering og dekryptering 9

3. Eksempel med RSA-kryptering **10**

3.1 Kryptering 11

3.2 Dekryptering 12

4. Bevis for RSA-kryptering **12**

5. Verden gennem Christophers øjne **15**

5.1 Skrivestilen 17

5.2 En aspergers søgen efter uafhængighed 18

6. Mere end en kriminalroman? **19**

6.1 En bog til børn eller voksne? 20

7. En aspergers afkodning af verden **21**

7.1 En særlig evne 23

Konklusion **24**

Litteraturliste **25**

Bøger 25

Hjemmesider 25

Bilag **27**

Bilag A: Eratosthenes' si 27

Indledning

En person, der lider af Aspergers syndrom, vil ofte blive beskrevet som dysfunktionel på bestemte områder, bl.a. i sociale relationer og i kommunikationen med andre. Derudover ses oftest et særligt talent hos folk med Aspergers syndrom indenfor bestemte områder. Personer, der lider af Aspergers syndrom, oplever ofte at blive misforstået i sociale sammenhænge. De har svært ved at udtrykke sig på en måde, som bliver forstået rigtigt af modtageren. Netop disse træk ved Aspergers syndrom ses hos hovedpersonen i romanen "The Curious Incident of the Dog in the Night-Time" af Mark Haddon fra 2004. I opgaven vil der blive redegjort for primtal og den generelle talteori bag RSA-kryptering. I forbindelse med dette vil kryptosystemets virkemåde blive beskrevet, og der opstilles et eksempel med dette. Derudover vil der fremgå en analyse og fortolkning af Mark Haddons "The Curious Incident of the Dog in the Night-Time", hvor der er særligt fokus på romanens skrivestil og genre. Endvidere diskuteres afkodningen i kryptosystemer i relation til hovedpersonens adfærd, tanker og omverdensrelationer.

1. Talteori

I dette afsnit gennemgås talteorien bag RSA-kryptering. Her kigges altså nærmere på egenskaberne ved primtal. Talteorien afgrænses ud fra en vurdering af, hvad der er relevant for opgaven, og derfor gennemgås kun de mest basale definitioner, sætninger og beviser.

1.1 Primtal

Definition 1 (Primtal)[1]*:*
Primtal er tal, der ikke har andre divisorer end 1 og tallet selv.

Ud fra definition 1, vil det vil altså sige, at de første 15 primtal er:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

[1] Riber, Peter (2008): *Kryptering*, s. 24.

Dog er der uendeligt mange primtal og for at finde antallet af primtal under et bestemt tal *n*, kan Eratosthenes' si anvendes. Denne metode anvender Christopher i bogen "The Curious Incident of the Dog in the Night-Time" af Mark Haddon, hvor han fortæller om, hvordan man finder primtal[2]. Metoden går ud på, at alle de naturlige tal oplistes i en tabel, hvilket vil sige 2, 3, 4, … *n*. Herefter sættes der en streg over alle de tal, som 2 går op i. Derefter markeres alle de tal, som 3 går op i. Dette fortsættes, indtil den mindste af de tilbageværende værdier er større end $\sqrt{n}$. Tilbage står de primtal, der er under n. Illustrationen af dette ses i bilag A.

1.2 Primtalsfaktorisering[3]

Definition 2 (Primtalsfaktorisering):
Man primtalsfaktoriserer et tal ved at omskrive det til et produkt af ikke-trivielle faktorer, der alle selv er primtal.

Eksempel:
Her er det vigtigt at huske, at primtal ikke kan primtalsfaktoriseres, fordi et primtal ikke har andre divisorer end 1 og tallet selv. Derfor vælges tallet 40, som ikke er et primtal. Hvis man vil primtalsfaktorisere tallet 40, kan det ikke opstilles $10 \cdot 4 = 40$. Selvom det er en faktorisering, så er 10 og 4 ikke primtal, og derfor er det ikke en primtalsfaktorisering. I stedet kan det opstilles $2 \cdot 2 \cdot 2 \cdot 5 = 40$. Det kan omskrives til $2^3 \cdot 5 = 40$.

Primtalsfaktorisering er det, som gør RSA-kryptering til et så sikker kryptosystem. Det er nemt at primtalsfaktorisere små tal, men når tallene bliver større, bliver det straks sværere. Et eksempel kunne være, at den hurtigste computer i verden bruger et sekund på at primtalsfaktorisere et tal på 80 decimaler. Hvis der tilføjes flere hundrede decimaler til dette, ville selv en milliard computere ikke kunne primtalsfaktorisere dette i Jordens levetid.

[2] Haddon, Mark (2010): *The Curious Incident of the Dog in the Night-Time*, s. 14.
[3] Riber, Peter (2008), s. 24-25.

1.3 Euklids algoritme og Bezouts identitet[4]

Sætning 2.1 (Euklids algoritme)[5]:

Hvis vi har givet to heltal a og b med $b > 0$, så findes der heltal q og r således, at

$$a = b \cdot q + r \quad \text{for} \quad 0 \leq r < b$$

Heltallet q kaldes her for kvotienten og heltallet r for resten. Der gælder endvidere, at r og q er entydigt fastlagt.

Euklids algoritme bruges til at finde den største fælles divisor af to vilkårlige hele tal *a* og *b*, hvilket vil sige det største hele tal, der går op i både *a* og *b*. Det kan også opstilles $sfd(a, b)$, hvilket står for **s**tørste **f**ælles **d**ivisor. Hvis den største fælles divisor for de to tal er 1, vil det sige, at de er indbyrdes primiske. Når to tal er indbyrdes primiske, er det kun tallet 1, der går op i begge tal. Det kan opstilles $sfd(a, b) = 1$. For at finde største fælles divisor for et tal, skal der foretages division med rester. Algoritmen gennemføres ved, at *a* først divideres med *b*, og derefter divideres med resten, fra forrige division, i det tal der opnåedes i forrige division. Dette fortsættes, indtil resten er 0. Hvis $r_0 = a$ og $r_1 = b$, kan algoritmens første trin opstilles således:

$$r_0 = q_1 \cdot r_1 + r_2 \tag{1}$$

Her er q_1 kvotienten for, hvor mange gange r_1 går op i r_0. Herefter fås en rest på r_2. Hvis resten ikke er 0, skal algoritmen fortsætte. Dette skal opstilles som følgende:

$$r_1 = q_2 \cdot r_2 + r_3$$
$$r_2 = q_3 \cdot r_3 + r_4$$
$$\dots$$
$$r_{n-3} = q_{n-2} \cdot r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_{n-1} \cdot r_{n-1} + r_n$$
$$r_{n-1} = q_n \cdot r_n + 0$$

[4] Hansen, Johan P. & Spalk, Henrik Gadegaard (2002): *Algebra og Talteori*, s. 14
[5] Jankvist, Uffe Thomas (2008): "RSA og den heri anvendte matematiks historie - et undervisningsforløb til gymnasiet", s. 25

Når algoritmen viser $sfd(a,b) = r_n$, så er det den sidste rest forskellig fra 0. Af sidste linje fremgår det, at r_n er divisor i r_{n-1}, hvilket kan skrives som $r_n | r_{n-1}$. Derfor er r_n også divisor i r_{n-2}, altså $r_n | r_{n-2}$. Hvis der fortsættes op gennem algoritmen, vil der kommes frem til, at $r_n | b$ og $r_n | a$. Derfor kan det altså med sikkerhed sige, at den største fælles divisor for a og b er r_n.

I forbindelse med Euklids algoritme, kan der anvendes en sætning kaldet Bezouts identitet.

Sætning 2.2 (Bezouts identitet):
Lad a og b være heltal med $b \geq 0$, da findes der heltal s og t, således at

$$sfd(a,b) = s \cdot a + t \cdot b$$

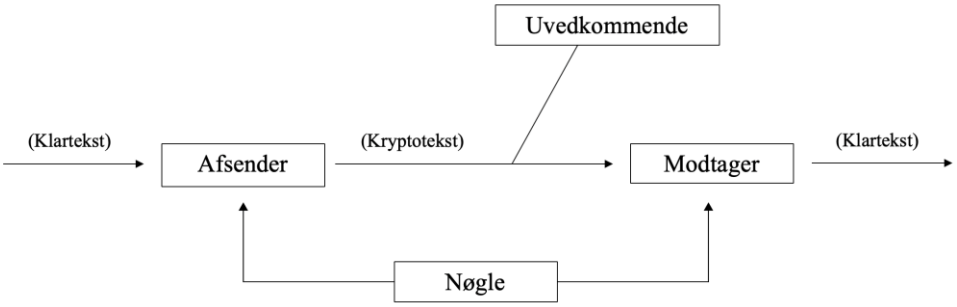
2. RSA-kryptering[6]

Det har i mange tusinde år været vigtigt for mennesker at kunne sende en besked til en anden person uden, at uvedkommende er i stand til at få fat i beskeden. Det har bl.a. været anvendt under krig og i forbindelse med forretninger. Det er her, at kryptologi kommer ind i billedet. Selve ordet kryptologi kommer fra det græske ord kryptos, som betyder hemmelig.[7] En af det meste sikre kryptosystemer er RSA-kryptosystemet, som blev opfundet af de tre matematikere Ronald Rivest, Adi Shamir og Leonard Adleman i 1977. Krypteringssystemets navn er sammensat af det første bogstav i hvert efternavn: RSA. Krypteringssystemet er bygget op om vanskeligheden ved at faktorisere et produkt, der er sammensat af to store primtal. RSA-kryptering er derfor anvendt verden over, fordi det skaber en sikker kommunikationsvej.

For at få et overblik over RSA-kryptering, kan det stilles op som en model. For at kunne kryptere en besked, skal A (afsender) først anmode M (modtager) om en nøgle, der kan bruges til krypteringen. Når M har dannet et nøglepar, sendes kun den ene af nøglerne til A. Denne nøgle er offentlig for alle. Derfor kaldes nøglen for den offentlige nøgle. Den anden nøgle kender kun M, hvilket så er den

[6] Vestergaard, Erik (2007): "RSA-kryptosystemet", s. 3 og 17
[7] Jankvist, Uffe Thomas (2008), s. 1.

hemmelige nøgle. Ved krypteringen sender A ikke klarteksten direkte til M, da det ville være for nemt for en uvedkommende at få fat i beskeden. I stedet krypterer A klarteksten til en kryptotekst med den offentlige nøgle. Herefter kan beskeden sendes, fordi uvedkommende person ikke kan få fat i klarteksten, når den er krypteret. Det kan kun M, fordi M har den hemmelige nøgle, der kan dekryptere kryptoteksten. Når kryptoteksten er blevet dekrypteret, kan M læse klarteksten.[8] Dette er illustreret på figur 1.



Figur 1: Model af RSA kryptosystemet[9]

Denne form for kryptering gør det muligt for alle at sende en dekrypteret besked til M ved blot at anvende den offentlige nøgle. Da det kun er M, der har den hemmelige nøgle, er det kun M, der er i stand til at dekryptere beskeder, der er krypteret med den offentlige nøgle.

2.1 Dannelsen af nøgler

For at kunne komme i gang med krypteringen, er det vigtigt først at kigge på nøglegenerering. Her skal der dannes en offentlig og hemmelig nøgle.

1. Til at starte med vælges to store primtal, p og q, og summen af de to tal beregnes, altså $n = p \cdot q$.
2. Herefter beregnes Eulers phi-funktion, som ser således ud: $\varphi(n) = (p-1)(q-1)$. Resultatet af Eulers phi-funktion fortæller hvor mange tal, der er indbyrdes primiske med n.

[8] Riber, Peter (2008), s. 39-40.
[9] Inspiration fra Landrock, Peter & Nissen, Knud (1997): *Kryptologi - fra viden til videnskab*.

3. Ud fra dette kan den offentlige eksponent, e, beregnes, som vælges ud fra følgende kravene, at $1 < e < \varphi(n)$ og $sfd(e, \varphi(n)) = 1$.
4. Herefter kan den hemmelige eksponent, d, beregnes, som beregnes ud fra $e \cdot d(mod\ \varphi(n)) = 1$.

Dette skaber den offentlige nøgle (også kaldet enkryptionsnøglen), som består af e og n, altså (e, n). Derudover er der også blevet dannet en hemmelig nøgle, d, som bruges til at dekryptere sammen med n. Derfor er tallene p, q og $\varphi(n)$ ikke nødvendige længere, og det bedste er at destruere disse tal, så ingen andre får fat i dem.

2.2 Enkryptering og dekryptering

Enkryptering er den del af RSA-krypteringen, hvor beskeden bliver omdannet til en kryptotekst. Beskeden går altså fra at være forståelig til at være uforståelig. Enkryptering af en tekst sker ved at opløfte *m* til *e*'te potens og derved finde resten modulo *n*. Resultatet for dette kaldes *c*. Udregningen opstilles $m \rightarrow c = m^e (mod\ n)$.

Dekryptering er den del af RSA-kryptering, hvor beskeden bliver omdannet til klarteksten, hvilket er den originale tekst. Beskeden går altså fra at være uforståelig til igen at være forståelig. Dekryptering af en tekst sker ved at opløfte det enkrypterede tal *c* i *d*'te potens og derved finde resten modulo *n*. Resultatet af dette er *m*. Udregningen opstilles $c \rightarrow c^d (mod\ n)$.

Hvis dette opstilles i en samlet udregning, er det tydeligt at se, at det igen ender ved udgangspunktet efter først at have enkrypteret og derefter dekrypteret:

$$c^d\ (mod\ n) = (m^e (mod\ n))^d\ (mod\ n) = (m^e)^d\ (mod\ n) = m^{ed}\ (mod\ n) = m$$

3. Eksempel med RSA-kryptering[10]

1. Der er blevet givet den offentlige nøgle $n = 2059$, og derfor skal der startes med at finde de to faktorer, der tilsammen giver den offentlige nøgle. Det kan gøres ved at anvende kommandoen *ifactor* i Maple (her omskrevet i WordMat):

$$ifactor(2059) = (29)(71)$$

Altså er de to værdier $p = 29$ og $q = 71$.

2. Herefter skal værdien af Eulers φ-funktion i 2059 beregnes:

$$\varphi(n) = (p-1) \cdot (q-1) = \varphi(n) = 1960$$

3. Dernæst skal der vælges et positivt tal e, som er mindre end $\varphi(n)$ og indbyrdes primisk med $\varphi(n)$. Der er mange tal at vælge imellem, så der vælges $e = 3$.

4. Den hemmelige nøgle d skal findes, hvilket gøres med løsningen til $e \cdot d\big(mod\ \varphi(n)\big) = 1$. Da e allerede er kendt, kan det indsættes $3 \cdot d(mod\ 1960) = 1$. Til at finde d anvendes ligning (1) fra Euklids algoritme:

$$1960 = 3 \cdot 653 + 1$$

Da den første ligning allerede har en rest på 1, behøves der ikke flere beregninger. Ligningen skal nu opstilles i Bezouts identitet fra sætning 2.2. For at opstille dette skal 1960 blot ganges med 1:

$$1 \cdot 1960 - 3 \cdot 653 = 1$$

Ud fra dette skal det tal, der er multipliceret med e, bruges, hvilket i dette tilfælde er -653. Det kan skrives op modulo 1960, således:

$$-653\ mod\ 1960 = 1307$$

[10] Vestergaard, Erik (2007): "RSA-kryptosystemet", s. 18-19.

Resultatet af denne beregning er altså $d = 1307$.

Ud fra beregningerne kan det bestemmes, at den offentlige nøgle er $n = 2059$ og $e = 3$, og den hemmelige nøgle er $d = 1307$.

Nu skal klarteksten ANNA enkrypteres og dekrypteres. Hvert bogstav skal oversættes til et tal. Derfor indføres en oversættelsestabel, der består af de 29 danske bogstaver og mellemrumstegn. Her er det vigtigt, at alle bogstaver får et tal med lige mange cifre. I tabellen figur 2, er hvert bogstav blevet givet 2 cifre.

_	A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Figur 2: Oversættelsestabel

Efter dette inddeles klarteksten i blokke af 4 cifre. Dette skyldes, at blokstørrelsen ikke må være større end n.

AN	NA
0114	1401

3.1 Kryptering

Krypteringen opstilles $m \rightarrow m^3 (mod\ 2059)$. Det udregnes for hver blok ovenfor:

$$0114^3 (mod\ 2059) = 1123$$

$$1401^3 (mod\ 2059) = 1164$$

Det vil altså sige, at den krypterede besked kommer til at hedde: 1123 1164

3.2 Dekryptering

Dekrypteringen opstilles $c \rightarrow c^{1307}(mod\ 2059)$. Beregningen er den samme som tidligere, hvor hver blok udregnes hver for sig:

$$1123^{1307}(mod\ 2059) = 114$$

$$1164^{1307}(mod\ 2059) = 1401$$

Den dekrypterede kode er altså: 0114 1401. Hvis tallene oversættes i oversættelsestabellen, findes der frem til den originale tekst ANNA.

4. Bevis for RSA-kryptering

For at være sikker på at den tidligere beregning er rigtig, opstilles et bevis for RSA-kryptering[11]. Der påstås, at der til den offentlige nøgle kan anvendes tallene (n, e), og at der til den hemmelige nøgle kan anvendes tallet d (sammen med e). Det skal altså bevises, at hvis et tal m krypteres til et nyt tal c, og det opstilles som følgende:

$$c = m^e(mod\ n)$$

Og modtageren derefter kan dekryptere c ved at udregne:

$$c^d(mod\ n)$$

Så skulle dette tal gerne være lig med værdien for m. Det skal altså bevises, at

$$m^{ed}(mod\ n) = m$$

Da $e \cdot d \equiv 1\ (mod\ \varphi(n))$, betyder det, at der er et helt tal k. Det opstilles:

$$e \cdot d = k \cdot \varphi(n) + 1 \qquad (2)$$

[11] L&R Uddannelse: "Projekt 0.6 RSA kryptering", s. 17-19.

Derudover er $\varphi(n) = (p-1)(q-1)$, hvilket kan indsættes i ligning (2):

$$e \cdot d = k \cdot \varphi(n) + 1 = k \cdot (p-1) \cdot (q-1) + 1 \quad (3)$$

Når dette er på plads, kan man antage to tilfælde, enten 1) er *m* og *n* primiske, eller 2) er *m* og *n* ikke primiske.

1. Hvis der antages, at *m* og *n* er primiske, skal $m^{ed}(mod\ n)$ omskrives, hvor ligning (2) indsættes:

   $$m^{k\cdot\varphi(n)+1}(mod\ n)$$

   Herefter anvendes potensregler:

   $$(m^{\varphi(n)})^k \cdot m^1(mod\ n)$$

   Så anvendes Eulers sætning:

   $$(1)^k \cdot m^1(mod\ n) \Longrightarrow m(mod\ n)$$

   Dette fører altså tilbage til udgangspunktet igen.

2. Hvis der antages, at *m* og *n* ikke er primiske.

   I dette tilfælde vil der være en fælles divisor, som må være enten p eller q, altså f.eks. $p \mid m$. Derfor må følgende gælde:

   $$m^{ed} - m = h \cdot p \quad (4)$$

   Her må q og p være primiske, fordi ellers ville q gå op i m. Hvis dette var tilfældet, ville $n = p \cdot q$ også gå op i m, men da m er mindre end n, så kan dette ikke lade sig gøre. Da q og p er primiske, opstilles følgende ved hjælp af Fermats lille sætning:

$$m^{q-1} \equiv 1 \; mod \; q$$

Det kan omskrives ved at bruge ligning (3):

$$\begin{aligned} m^{q-1} \equiv 1 \; mod \; q &\Rightarrow (m^{q-1})^{(p-1)} \equiv (1)^{(p-1)} \; mod \; q \\ &\Rightarrow m^{(q-1)(p-1)} \equiv 1 \; mod \; q \\ &\Rightarrow m^{\varphi(n)} \equiv 1 \; mod \; q \\ &\Rightarrow (m^{\varphi(n)})^{k} \equiv 1^{k} \; mod \; q \\ &\Rightarrow m^{k \cdot \varphi(n)} \equiv 1 \; mod \; q \\ &\Rightarrow m^{k \cdot \varphi(n)} \cdot m \equiv 1 \cdot m \; mod \; q \\ &\Rightarrow m^{k \cdot \varphi(n)+1} \equiv m \; mod \; q \\ &\Rightarrow m^{ed} \equiv m \; mod \; q \end{aligned}$$

Ud fra den sidste kongruens ses, at der findes et helt tal l. Derfor kan følgende opstilles:

$$m^{ed} - m = l \cdot q \tag{5}$$

Ud fra ligning (4) og (5) kan følgende opstilles:

$$h \cdot p = l \cdot q$$

Da det antages, at p og q ikke er de samme primtal, så gælder $q \mid h$. Det vil altså sige, at der findes et tal r:

$$h = r \cdot q$$

Hvis dette indsættes i ligning (5), fås følgende:

$$m^{ed} - m = h \cdot p = (r \cdot q) \cdot p = r \cdot q \cdot p = r \cdot n$$

At n går op i $m^{ed} - m$, er det samme som at skrive $m^{ed} \; (mod \; n) = m$. Dette fører altså tilbage til udgangspunktet igen.

Ud fra begge tilfælde virker RSA-kryptering altså.

5. Verden gennem Christophers øjne

Primtal er et emne, der har en stor betydning for hovedpersonen i Mark Haddons roman "The Curious Incident of the Dog in the Night-Time. Bogens hovedperson og fortæller hedder Christopher John Francis Boone. Han nævner, at han godt kan lide primtal, og har derfor også valgt at inddele bogens kapitler efter primtal, i stedet for kardinaltal. Han sammenligner i denne forbindelse primtal med livet, fordi de er logiske men også meget svære at finde regler for[12]. Sådan opfatter han verden, fordi han har svært ved at finde reglerne for, hvordan man begår sig i verden. Christopher er 15 år gammel og bor i Swindon, England med sin far. Allerede i starten af romanen får læseren en fornemmelse af, at der er noget specielt ved Christopher. Da han præsenterer sig selv, nævner han: "I know all the countries of the world and their capital cities and every prime number up to 7,057."[13] Den viden, han præsenterer, er ikke viden enhver person ville have. Dog får man aldrig at vide, at det er Aspergers syndrom, Christopher lider af. Dette antages dog, da det passer meget godt med de typiske personlighedstræk, der oftest ses ved Aspergers syndrom, fordi han netop har svært ved at omgås andre mennesker og fordyber sig særligt meget i bestemte emner[14]. Men han er godt klar over, at han har nogle udfordringer, der ikke er helt normale. Dem laver han en liste over:

> "A. Not talking to people for a long time… E. Not liking being in really small places with other people… H. Not liking yellow things or brown things and refusing to touch yellow things or brown things… O. Hitting other people…"[15]

Han nævner, at tingene på listen gør hans mor og far sure en gang imellem, men at han selv mener, at han er blevet bedre til ikke at have så mange adfærdsproblemer. Det er med til at skabe en form for humor i bogen, fordi læseren ikke har en opfattelse af, at listen er kort. For læseren vil listen netop virke meget lang og krævende. Listen er også med til at understøtte den antagne diagnose, fordi

[12] Haddon, Mark (2010), s. 15.
[13] Ibid, s 2.
[14] James, Ioan: "On Mathematics, Music and Autism", s. 606.
[15] Haddon, Mark (2010), s. 59-60.

personer med Aspergers syndrom ofte har det bedst med at lave lister for at få overblik. Christopher kan generelt godt lide, at der er orden i tingene, og han elsker at lave systemer. Blandt andet laver han et system, der er med til at bestemme, hvor god en dag det vil blive ud fra, hvor mange røde biler han ser på vej til skole[16]. Selvom det for læseren er klart, at dagens gang ikke kan defineres ud fra antallet af røde biler, så giver det Christopher en form for tryghed at vide, hvordan dagen kommer til at forløbe. Han indrømmer også over for Mr. Jeavons, at han er glad for orden, selvom det måske ikke altid er en logisk form for orden. Det viser altså, at han ikke som sådan går op i logikken af hans systemer, men blot ordenen og følelsen af sikkerhed.

Christopher er en meget ærlig person, og læseren bliver ikke inviteret til at være skeptisk over for de ting, som Christopher siger. Han siger flere gange i novellen: ”I always tell the truth.”[17] Det er med til at skabe en tillid til Christopher som fortæller, fordi man er sikker på, at virkeligheden ikke bliver fordrejet eller påvirket af hans egen bias. Dog skal læseren altid ind og tolke hændelser fra romanen, fordi Christopher ikke altid selv opfanger bestemte situationer. Hans ærlighed gør ham også til en meget godtroende person. Når han selv ikke kan lyve, kan han heller ikke opfange, når andre mennesker lyver over for ham. Det ses f.eks., når hans far lyver omkring Christophers mors død. Det falder slet ikke Christopher ind, at faren kunne finde på at lyve, fordi han ikke selv ville kunne finde på det.

Han har derudover svært ved at udtrykke hans følelser og erstatter dem derfor tit med vredesudbrud. Dette ses i stykket: “…and then she laughed. So I tore the original piece of paper up and threw it away.”[18] Han kan ikke finde ud af at fortælle sin lærer, Siobhan, at han bliver ked af det, når hun griner, og derfor reagerer han, som han gør. Det er lidt på samme måde, som et lille barn ville reagere, der endnu ikke kan tale.

[16] Ibid, s. 31.
[17] Ibid, s. 23.
[18] Ibid, s. 3.

5.1 Skrivestilen

Romanen er skrevet i jeg-fortæller. Den bliver fortalt fra Christophers synsvinkel, og derfor får læseren også et særligt indblik i, hvordan han ser verden. Han har en stor sans for detaljer og er derfor meget god til at beskrive sine omgivelser nøje for læseren. Det er med til at gavne hans efterforskning, fordi han indsamler meget relevant viden. F.eks. lægger han med det samme mærke til, at Wellingtons snude stadig er varm, da han finder den død i haven. Dog er der andre ting, som Christopher ikke opfanger, hvilket gør, at læseren selv bliver nødt til at udfylde huller i historien for at få det hele til at hænge sammen. Andre folks reaktioner og følelser bliver udeladt, fordi Christopher ikke opfanger dem. Sproget i bogen er dog ikke det eneste, der adskiller den fra andre romaner. Der inddrages også flere illustrationer, som er med til at skabe en bedre forståelse af situationerne for læseren. F.eks. indleder han romanen med at fortælle om hans problemer med at forstå og afkode andres ansigtsudtryk, hvor han inddrager figur 3.

Figur 3 - Christophers tegning af ansigtsudtryk.[19]

Han nævner, at det er nemmere for ham at forstå andres ansigtsudtryk, når han har skrevet dem ned på papir, for så kan han altid kigge på det, når han bliver i tvivl. I forbindelse med tegningen fortæller Christopher også, at han godt kan lide hunde, fordi de er nemmere at læse. Han nævner, at de kun kan være i fire forskellige slags humør, og at det derfor er nemmere at forstå dem. Derudover nævner han, at de er pålidelige og aldrig ville lyve over for en.

Der ses ikke mange metaforer i bogen. Dette skyldes, at Christopher ikke kan forstå meningen med brugen af metaforer. Han mener, at metaforer burde blive kaldt for løgne, fordi de beskriver noget, som ikke er rigtigt. Det er for ham svært at forestille sig billederne i hovedet, når folk bruger metaforer til at

[19] Ibid, s. 2.

beskrive noget. Dog anvender han flere gange sammenligninger. Han mener, at det er tilladt at bruge sammenligninger, fordi de ikke er løgne[20].

Mark Haddon er god til at beskrive personerne i bogen ved deres sprogbrug. Hvis man f.eks. kigger på brevene fra moren til Christopher, ses der flere stavefejl, som ”defferant”[21] og ”stoped”[22]. Dette giver et indtryk af, at moren ikke er særlig veludannet. Dette understøttes også af det miljø, som Christopher vokser op i, fordi nabolaget ikke virker som det mest trygge sted at befinde sig. Christopher nævner i forbindelse med sin efterforskning på mordet af Wellington, at naboerne tager stoffer, og at han derfor skal holde sig fra deres hus[23]. Det indikerer altså, at han ikke bor i et nabolag med parcelhuse og højtlønnede folk. Christophers syntaktiske niveau er forskelligt, alt efter om han forklarer noget videnskabeligt eller taler om sine egne oplevelser. Dette ses f.eks., når han beskriver Monty Hall problemet: “Supposing that you choose door X, the possibility that you win a car if you then switch your choice is given by the following formula”[24]. Her anvender han et meget videnskabeligt sprog. Når han derimod begynder at snakke om sine oplevelser, som f.eks.: “And Siobhan apologized. And now if I don’t know what someone is saying, I ask them what they mean or I walk away.”[25] Her er det tydeligt, at han stadig er et barn og derfor ikke anvender et voksent sprogbrug.

5.2 En aspergers søgen efter uafhængighed

Der er flere temaer, der gør sig gældende i romanen. Christophers stræben efter uafhængighed er et af dem. Han har svært ved at begå sig i omverdenen, især steder hvor han ikke er vant til at være. Han vil dog gerne være i stand til at tage sig af sig selv og være i stand til at bo alene, ligesom en hver anden teenager. Derfor gør han oprør mod sin far og finder sig selv i nye og uvante situationer, fordi han står helt alene. Efterforskningen af mordet på Wellington er med til at skubbe ham i retningen af at blive mere uafhængig, fordi han bevæger sig ud af sin tryghedszone ved at afhøre folk, han ikke kender, om situationen. Derudover betyder A-level testen i matematik også en del for Christopher, fordi den er med

[20] Ibid, s. 22.
[21] Ibid, s. 131.
[22] Ibid, s. 134.
[23] Ibid, s. 50.
[24] Ibid, s. 81.
[25] Ibid, s. 3.

til at vise ham, at han er god til noget, og at den kan bane vejen til college, som er Christophers endelige mål. Derudover kan et tema være det at leve med Aspergers syndrom. Christopher har svært ved at kommunikere normalt med andre mennesker, og det er et af de karakteristika, der kan komme til udtryk ved Aspergers syndrom. Selvom han har en højere IQ end de fleste andre, så er det kun på bestemte områder, hvor det gavner ham. De fleste af de personer, Christopher møder igennem romanen, behandler ham på en særlig måde, fordi de er klar over, at han lider af en udviklingsforstyrrelse. Derfor er det meste af Christophers hverdag skræddersyet efter hans behov. Dog møder han også personer, der ikke er klar over, at han lider af Aspergers syndrom, og derfor ikke indordner sig efter det. Disse situationer er svære for Christopher at navigere sig rundt i, fordi han er vant til at være omgivet af folk, der kender til hans situation. Det gør derfor også, at han har et begrænset antal venner, eller personer der er tæt på ham, og har svært ved at få nye relationer, fordi han ikke er god til at socialisere med personer, han ikke kender.

6. Mere end en kriminalroman?

Det er svært at definere bogens genre, da den har forskellige genretræk. Christopher indleder med at fortælle, at det er en kriminalroman, han skriver. Her går han ind og definerer, hvad en kriminalroman er:

> "In a murder mystery novel someone has to work out who the murderer is and then catch them. It is a puzzle. If it is a good puzzle you can sometimes work out the answer before the end of the book."[26]

Genren passer delvist på romanen, fordi den i starten følger de typiske genretræk for en kriminalroman. Christopher beskriver en forbryderisk handling og prøver at finde frem til motivet bag for til sidst at kunne opklare kriminalgåden.[27] Derudover er romanens titel en reference til Sherlock Holmes novellen "The Adventure of Silver Blaze" af Arthur Conan Doyle.

[26] Ibid, s. 5
[27] Fibiger, Johannes & Lütken, Gerd (2009): *Litteraturens Veje*, s. 504.

> ”Is there any point to which you would wish to draw my attention?... To the curious dog in the night-time… The dog did nothing in the night-time… That was the curious incident,” remarked Sherlock Holmes.”[28]

Derfor lægges der allerede ud fra romanens titel op til, at det er en kriminalroman, vi har med at gøre. Christopher fortæller også selv, at han er stor fan af Sherlock Holmes bøgerne, så derfor er det også mest oplagt for ham at skrive en kriminalroman. Dog bliver morderen hurtigt afsløret, og derfor ændres genren også i midten af bogen. Efter Christopher finder ud af, at hans far har myrdet hunden og har løjet om morens død, begiver Christopher sig ud for at finde hans mor i London. Han bliver udfordret i mødet med omverdenen, men finder dog frem til moren igen. Han går fra at være en usikker dreng, der ikke har prøvet at være på egen hånd, til at være selvstændig nok til at kunne rejse rundt i London uden hjælpe fra andre. Her kan man sige, at genren er skiftet til en dannelsesroman, fordi den følger kontraktmodellen (hjemme-ude-hjemme). Christopher starter hjemme i trygge rammer hos faren, herefter begiver han sig ud på en udfordrende rejse, og han ender til sidst derhjemme igen efter en lærerig oplevelse, og harmonien er genopstået. Dog kan man også argumentere for, at det ændres til en udviklingsroman, fordi forældrenes ægteskabsproblemer stadig ikke er løst, og Christopher stadig er ved at genopbygge forholdet til sin far.

6.1 En bog til børn eller voksne?

Da Mark Haddon udgav bogen i 2003, blev der lavet én forside til børn og én forside til voksne. Derfor kan der også være tvivl om, hvorvidt bogen er skrevet til børn eller voksne. Mark Haddon har selv udtalt, at hans intention med bogen var, at det skulle være en roman til voksne. [29] Bogen har efterfølgende vundet en pris som børnebog, og derfor vurderes det, at bogen både er til børn og voksne. Romanen appellerer især til dets unge publikum, fordi Christophers sprog er så ukompliceret. Derudover kan mange børn relatere sig til hans situation som teenager med forældre, der bliver skilt og har svært ved at fungere sammen. Romanen vurderes også at være relevant for voksne, fordi Christophers måde at ser verden på er så interessant og anderledes.

---

[28] Doyle, Arthur Conan: *”The Adventure of Silver Blaze”.*
[29] Falconer, Rachel (2008): *The Crossover novel*, s. 96.

7. En aspergers afkodning af verden

Ligesom for Christopher kan det være svært for andre med Aspergers syndrom at afkode andre menneskers intentioner og følelser. I en samtale mellem to personer, hvor den ene har Aspergers syndrom, kan det være svært at holde en samtale kørende, fordi de to personer har forskellige sproglige koder, og derfor nemt misforstår hinanden. Som tidligere nævnt, så har Christopher besvær med at afkode andre, når de f.eks. anvender humor i deres sprog. Det opfanger han ikke, og i stedet misforstår han, hvis andre begynder at grine midt i samtalen.

Endvidere er det besværligt for folk med Aspergers syndrom at afkode andres ansigtsudtryk og kropssprog, ligesom det ses med Christopher i romanen. Hvis man kigger på sammenhængen mellem RSA-kryptering og Christophers situation, så kan Christopher sammenlignes med den udefrakommende person fra figur 1, der prøver at hacke sig ind i systemet - dog uden held. Man kan sige, at Christopher ikke har den nøgle, der kræves for at kunne dekryptere og derved forstå den sendte besked. I stedet finder han oftest sig selv i situationer, hvor han har svært ved at forstå den måde, hvorpå andre mennesker kan forstå hinanden. Ligesom han har svært ved at dekryptere andres kropssprog og ansigtsudtryk, så har han også selv svært ved at enkryptere sig eget. Det vil sige, at han har svært ved at udtrykke sig på en bestemt måde, så at andre vil forstå ham bedre. Netop denne model er blevet opstillet af Stuart Hall, som forklarer kommunikationsprocesser ud fra enkryptions- og dekryptions-princippet[30]. Her forklarer han, at det er yderst vigtigt at begge parter har den samme baggrundsforståelse inden for et bestemt emne, for at en samtalen kan holdes kørende. Et eksempel på en mislykkedes samtale ses bl.a. i bogen, da Christopher vil købe en billet på togstationen, men misforstår manden i billetlugens spørgsmål:

> "And the man said, "Single or return?" And I said, "What does single or return mean?" And he said, "Do you want to go one way, or do you want to go and come back?" And I said, "I

[30] Pressbooks (2018): "Communications Process: Encoding and Decoding".

> want to stay there when I get there." And he said, "For how long?" And I said, "Until I go to university." "And he said, "Single, then,"…"[31]

Her forstår Christopher ikke intentionen med mandens spørgsmål, og derfor bliver spørgsmålet misforstået. Christopher har ikke den baggrundsviden, der skal til for, at han forstår spørgsmålet. Selvom samtalen mislykkedes, når de dog alligevel frem til, hvilken billet Christopher har brug for.

Man kan også diskutere, om det egentlig er alle andre, der ikke har den rigtige kode til at kunne forstå personer som Christopher. Måske er han den eneste, der rent faktisk har noget særligt at sige, men alle andre har ikke muligheden for at kunne forstå det rigtigt? Hvis andre forstod hans måde at tænke på, ville det også være langt nemmere for Christopher at komme ud med den viden, han har indenfor matematikkens verden. Rachel Falconer pointerer i sin bog "The Crossover Novel", at mysteriet ligger i at forstå Christophers tankegang: "The incident is certainly mysterious, but for the reader, the deadpan voice and mathematically precise gaze may pose an even greater mystery to unravel."[32] Her nævner hun altså, at selvom der bliver lagt op til, at mordet på Wellington er romanens mysterium, så finder de fleste ud af, at Christopher selv er det største mysterium. Der er så mange ting ved den måde, Christopher agerer på, som er anderledes end læserens. Derfor ligger den store gåde i at forstå hans intentioner og følelser midt i al det kaos, han oplever.

I forbindelse med dette kan man inddrage Niklas Luhmanns sociologiske teori om autopoiese[33], som går ud på, at alle mennesker har et psykisk system, der organiserer sig i sociale systemer. Hver persons psykiske system er dannet ud fra personens oplevelser og erfaringer. Derfor opfatter hver person verden anderledes, og det er aldrig muligt for nogen at kunne forstå verden præcis på samme måde som en anden person. Det kan man relatere til Christophers situation, fordi han både føler, at andre ikke forstår ham, og at han ikke forstår andre. Ifølge Niklas Luhmann er det altså fordi, at Christopher danner sit eget psykiske system, som andre ikke har mulighed for at forstå på samme måde som Christopher selv. Og det samme gælder for Christopher, som ikke har mulighed for at træde ind i

[31] Haddon, Mark (2010), s. 189.
[32] Falconer, Rachel (2008), s. 106.
[33] David Seidl (2004): "Luhmann's theory of autopoetic social systems".

andres psykiske systemer og afkode deres individuelle opfattelse af verden. Ved en person med Aspergers syndrom bliver denne teori således meget tydelig, netop fordi forståelsen af verden bliver set fra et så anderledes perspektiv.

7.1 En særlig evne

Selvom personer med Aspergers syndrom har svært ved at kommunikere med andre mennesker, så har flere studier vist, at mange har særlige evner inden for matematik og andre fag, der kræver en logisk tænkning. En undersøgelse fra Standford University School of Medicine og Lucile Packard Children's Hospital[34] viser, at autistiske børn viser en særlig evne indenfor matematikkens verden. Dette skyldes, at de har en særlig logisk sans, som de fleste andre ikke besidder. Det ses også hos Christopher i bogen, som går meget op i, at hans matematiske og logiske evner viser, hvad han egentlig er i stand til. Altså har Christopher den hemmelige nøgle til en verden, som ikke mange har adgang til. Han er selv klar over, at han har denne særlige evne til at se ting, andre ikke kan se: "And that is why I am good at chess and maths and logic, because most people are almost blind and they don't see most things and there is lots of spare capacity in their heads…"[35] Han har en helt særlig forståelse af verden, og hvordan den fungerer. Kærligheden til det simple i matematikken nævner Ioan James i sin undersøgelse "On Mathematics, Music and Autism": "the feeling of mathematical beauty, of the harmony of numbers and forms, of geometric elegance. This is a true aesthetic feeling which all real mathematicians know."[36] Her forklarer han altså, at alle matematikere finder harmoni i det simple og logiske ved matematikken. Han nævner derudover også, at for at flygte for den kaotiske verden, så søger matematikerne tilflugt i matematikken. For at forklare sit syn på verden anvender Christopher matematiske systemer, som skaber en form for orden i en ellers kaotisk verden. Derfor skabes der også en særlig forståelse for Christopher ud fra hans brug af matematikken i hverdagen. Hvis ikke matematikken havde været til stede i romanen, ville det have været endnu sværere for læseren at forstå Christophers situation, og hvordan han ser ting fra sig eget perspektiv og ud fra sit psykiske system. Personer med Aspergers syndrom har altså en helt særlig evne til at vige fra det normale. De fordyber sig i tingene og forsøger at finde logikken i det hele. De sætter spørgsmålstegn ved mange ting, og det

[34] Bergeron, Louis (16.06.2013): "Autistic kids who best peers at math show different brain organization, study shows".
[35] Haddon, Mark (2010), s. 178.
[36] James, Ioan, s. 605.

er tit denne evne, der skaber nye opdagelser og fremskridt i verden.[37] Man kan sige, at de har den hemmelige nøgle til en verden, som vi andre endnu ikke har opdaget.

Konklusion

Der redegøres for talteorien bag RSA-kryptering, herunder primtalsfaktorisering, Euklids algoritme og Bezouts identitet. Derudover introduceres til RSA-kryptering med dannelsen af nøgler, enkryptering og dekryptering, som videre bliver brugt til at kryptere ordet ANNA, hvorefter der opstilles et bevis for RSA-kryptering. Hovedpersonen i Mark Haddons roman "The Curious Incident of the Dog in the Night-Time", Christopher, antages at lide af Aspergers syndrom og har derfor svært ved socialisering, men han har dog en stor interesse for matematik. Den antagne diagnose kommer til udtryk gennem Haddons skrivestil i romanen, som er stærkt præget af Christophers unormale adfærd og logiske tankegang. Selvom romanen i starten bliver præsenteret som en kriminalroman, ender den ud i en dannelsesroman, netop fordi Christopher bliver mere selvstændig efter at have begivet sig ud på en udfordrende rejse. RSA-kryptering kan bruges som en metafor for Christophers adfærd, tanker og omverdensrelationer, fordi han prøver at afkode de ting, han ikke forstår. Desuden er det også svært for læseren at afkode Christopher, og i virkeligheden er Christopher måske det største mysterium i bogen. Han har en evne til at forstå og se ting, som andre ikke kan.

[37] McFarland, Matt (3.04.2015): "Why shades of Asperger's Syndrom are the secret to building a great tech company".

Litteraturliste

Bøger

- Falconer, Rachel (2008): *The Crossover Novel*. Routledge.
- Fibiger, Johannes & Lütken, Gerd (2009): *Litteraturens Veje*. Systime.
- Haddon, Mark (2010): *The Curious Incident of the Dog in the Night-Time*. David Fickling Books.
- Hansen, Johan P. & Spalk, Henrik Gadegaard (2002): *Algebra og Talteori*. Gyldendal.
- Landrock, Peter & Nissen, Knud (1997): *Kryptologi - fra viden til videnskab*. Abacus.
- Riber, Peter (2008): *Kryptering*. Systime A/S.

Hjemmesider

- Bergeron, Louis (16.08.2013): ”Autistic kids who best peers at math show different brain organization, study shows”. Internetadresse: https://med.stanford.edu/news/all-news/2013/08/autistic-kids-who-best-peers-at-math-show-different-brain-organization-study-shows.html (Besøgt d. 8.03.2020).
- David Seidl (2004): “Luhmann’s theory of autopoetic social systems”. Internetadresse: https://www.zfog.bwl.uni-muenchen.de/files/mitarbeiter/paper2004_2.pdf (Besøgt d. 15.03.2020).
- Doyle, Arthur Conan: ”The Adventure of Silver Blaze”. Internetadresse: https://etc.usf.edu/lit2go/40/the-memoirs-of-sherlock-holmes/573/adventure-1-silver-blaze/ (Besøgt d. 11.03.2020).
- James, Ioan: ”On Mathematics, Music and Autism”. Internetadresse: https://archive.bridgesmathart.org/2006/bridges2006-605.pdf (Besøgt d. 12.03.2020).
- Jankvist, Uffe (2008): ”RSA og den heri anvendte matematiks historie - et undervisningsforløb til gymnasiet”. Internetadresse: http://milne.ruc.dk/imfufatekster/pdf/460.pdf (Besøgt d. 10.03.2020).
- L&R Uddannelse: ”Projekt 0.6 RSA kryptering”. Internetadresse: http://www.lr-web.dk/Lru/microsites/hem/fra_gymportal/1projekt_0.6_rsa_kryptering.pdf (Besøgt d. 4.03.2020).

- McFarland, Matt (3.04.2015): ”Why shades of Asperger’s Syndrom are the secret to building a great tech company”. Internetadresse: https://www.washingtonpost.com/news/innovations/wp/2015/04/03/why-shades-of-aspergers-syndrome-are-the-secret-to-building-a-great-tech-company/ (Besøgt d. 15.03.2020).
- Pressbooks (2018): ”Communications Process: Encoding and Decoding”. Internetadresse: https://ecampusontario.pressbooks.pub/commbusprofcdn/chapter/1-2/ (Besøgt d. 15.03.2020).
- Vestergaard, Erik (2007): ”RSA-kryptosystemet”. Internetadresse: https://www.matematikfysik.dk/mat/noter_tillaeg/RSA.pdf (Besøgt d. 4.03.2020).

Bilag

Bilag A: Eratosthenes' si

	2	3	~~4~~	5	~~6~~	7
~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~
~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~
~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~
29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~
~~36~~	~~37~~	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~