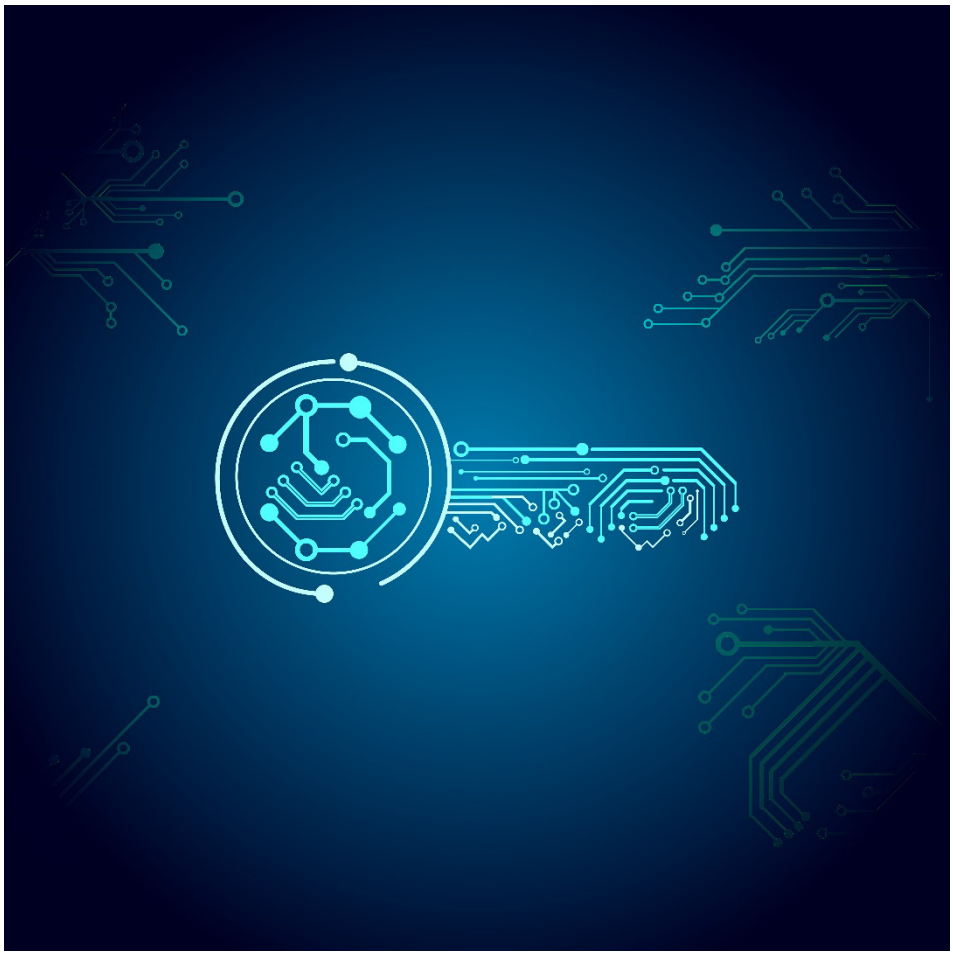
Kryptologi

Introduktion med opgaver i hånden og i Maple



Billedliste

Side 6: ©Alamy.com (Bogillustration med Blaise de Vigenère).

Side 8: Via Wikimedia Commons. Public Domain (William F. Friedman).

Side 17: ©iStock.com/ Nadezhda Kozhedub (PKCS).

1. Indledning

Kryptologi er læren om hemmeligholdelse af information. Det kommer af det græske ord *kryptos*, som betyder "hemmelig" og *logi* som er "læren om". Kryptering har været anvendt langt tilbage i historien, både i militære og diplomatiske sammenhænge. I militæret var det afgørende at holde oplysninger hemmelige for at opnå strategiske fordele over fjenden, mens det i diplomatiske kredse blev brugt til at sikre fortrolig kommunikation mellem stater og ledere. I dagens moderne samfund finder kryptering mange andre anvendelser: Internetkommunikation, beskyttelse af data på mobiltelefoner, i online banker, i cloud-lagring, beskyttelse af kunde- og patientoplysninger, i kryptovalutaer og meget andet. Udover *konfidentialitet* (fortrolighed/hemmeligholdelse) ønsker man ofte i dag også at data opfylder andre krav: *Autenticitet* (ægthed), *integritet* (ikke-manipuleret, uberørt) samt *ikke-afvisning* (kan ikke afvises/benægtes).

I dette lille dokument skal vi først se på nogle hands-on eksempler på et *monoalfabetisk kryptosystem* og et *polyalfabetisk kryptosystem* samt kort studere kodemaskinen *Enigma*, som blev anvendt under 2. Verdenskrig af tyskerne. Til sidst vil vi se på principperne bag *Public-Key* kryptosystemer, som anvendes i vores moderne samfund. Først nogle begreber: Med *klarteksten* menes den oprindelige tekst, der kan læses. Med *kryptoteksten* menes den krypterede og uforståelige tekst. Man kan *kryptere* klarteksten for at få kryptoteksten eller *dekryptere* kryptoteksten og få klarteksten.

Det er hensigtsmæssigt at klarteksten skrives med små bogstaver, mens kryptoteksten skrives med store bogstaver, så der ikke opstår tvivl om, hvad der er hvad.

2. Monoalfabetisk kryptosystem

Et monoalfabetisk kryptosystem er et system, hvor hvert bogstav hver gang bliver krypteret til et bestemt ofte andet bogstav. Det kan for eksempel være, at bogstavet `a` altid bliver krypteret til et `E`, at `b` altid bliver krypteres til et `O`, etc. Krypteringen kan beskrives ved en *nøgle*, som vist herunder.

Klartekst:	a b c d e f g h i j k l m n o p q r s t u v w x y z æ ø å
Kryptotekst:	E O L T N A H D Æ K U P X Ø I F B Å C Q S G Z R M Y V J W

Nøglen kan også bruges til dekryptering, idet vi da blot starter i nederste række og ser, hvad et bogstav svarer til i klartekst i linjen over. Undertiden vil vi også kalde ovenstående for et *kryptoalfabet* eller et *substitutionsalfabet*.

Eksempel 1

Vi har givet følgende klartekst:

"Ved daggry kl. 7 angriber vi".

Vi fjerner alle specialtegn såsom punktummer, og tallet 7 skriver vi som syv. Desuden fjerner vi mellemrummene mellem ordene, fordi de kun vil gøre det nemmere for fjenden at dekryptere. Ved brug af nøglen på forrige side får vi:

Klartekst:	v	e	d	d	a	g	g	r	y	k	l	s	y	v	a	n	g	r	i	b	e	r	v	i
Kryptotekst:	G	N	T	T	E	H	H	Å	M	U	P	C	M	G	E	Ø	H	Å	Æ	O	N	Å	G	Æ

Kryptoteksten er altså: "GNTTEHHÅMUPCMGEØHÅÆONÅGÆ".

Opgave 2

Lasse og Marie er forelskede, men ønsker ikke at røbe det til kammeraterne. De kunne have sendt en SMS til hinanden, men for spændingens skyld og fordi de netop har haft emnet kryptologi i matematik, vælger de at aflevere en krypteret besked til hinanden på en lap papir. I forvejen har de udvekslet følgende nøgle med hinanden:

Klartekst:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	æ	ø	å
Kryptotekst:	U	M	T	S	E	C	G	R	D	L	Q	J	X	H	Æ	K	Å	A	I	W	V	O	P	N	F	Ø	Z	B	Y

Lasse vil kryptere følgende klartekst:

"Mød mig klokken 14 i kantinen".

Husk at fjerne mellemrum og skrive 14 som "fjorten". Krypter derefter teksten med ovenstående nøgle.

Opgave 3

To elever har udvekslet følgende nøgle til et monoalfabetisk kryptosystem:

Klartekst:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	æ	ø	å
Kryptotekst:	H	F	Å	J	S	Æ	G	K	Ø	T	R	E	Q	W	O	U	N	Z	I	M	X	C	V	L	Y	B	A	P	D

Christoffer sender følgende kryptotekst til William: " "JSZSZÆZSJHGIÅHÆSØJHG". William dekrypterer. Hvilken klartekst får han?

Opgave 4 (Opgave i Maple)

Læs teksten i Maple filen (venstreklik for at downloade):

krypter_og_dekrypter_monoalfabetisk_system.mw

og løs de tre opgaver i filen.

Imidlertid er monoalfabetiske kryptosystemer ikke så svære at bryde – altså uden brug af nøgle. De er sårbare overfor *frekvensanalyse*. Ved at sammenligne frekvenserne af de enkelte bogstaver i kryptoteksten med frekvenserne af de enkelte bogstaver i en almindelig dansk tekst, kan man hurtigt komme med kvalificerede bud på, hvilke bogstaver i kryptoteksten, som svarer til de mest forekommende bogstaver i det danske alfabet: *e*, *r*, *n*, *t*, *a*, … Frekvenserne for de såkaldte *bigrammer* og *trigrammer* i kryptoteksten kan også være nyttige til at lede én fremad i kodebrydningen. Et bigram og et trigram er henholdsvis et par af bogstaver og tre bogstaver, som står ved siden af hinanden i teksten. Hvis bare teksten har en nogenlunde længde, så vil klartekstens bogstavfrekvenser ofte ligge ret tæt på bogstavfrekvenserne i en almindelig dansk tekst, og så vil det mest forekommende bogstav i kryptoteksten ofte svare til et *e* i klartekst. Derfra kan man langsomt trevle teksten op. Da processen er lidt upraktisk at udføre i hånden, vil vi bruge Maple, fordi programmet kan stille de hidtidige gæt op på en hensigtsmæssig måde. Læseren opfordres til at løse opgave 5 herunder.

At anvende frekvensanalyse som middel til at bryde en krypteret tekst kendes så langt tilbage som til det 9. århundrede. Muslimen *Al-Kindi* (ca. 801- ca. 873) var en prominent figur i *Visdommens Hus* (*Bayt al-Hikma*) i Bagdad i den arabiske videnskabelige guldalder, hvor der blev studeret matematik, astronomi, filosofi, kemi, medicin, optik m.m. Blandt Al-Kindis mange bidrag er bogen *Risalah fi Istikhraj al-Mu'amma*, som kan oversættes til "Manuskript om dechifrering af kryptografiske meddelelser". Specielt vigtigt er, at han i bogen omtaler frekvensanalyse. Det tyder på, at Al-Kindis teknik gik i glemmebogen, for det er først i renæssancen, at man i Europa begynder at bruge frekvensanalyse.

Opgave 5 (Opgave i Maple)

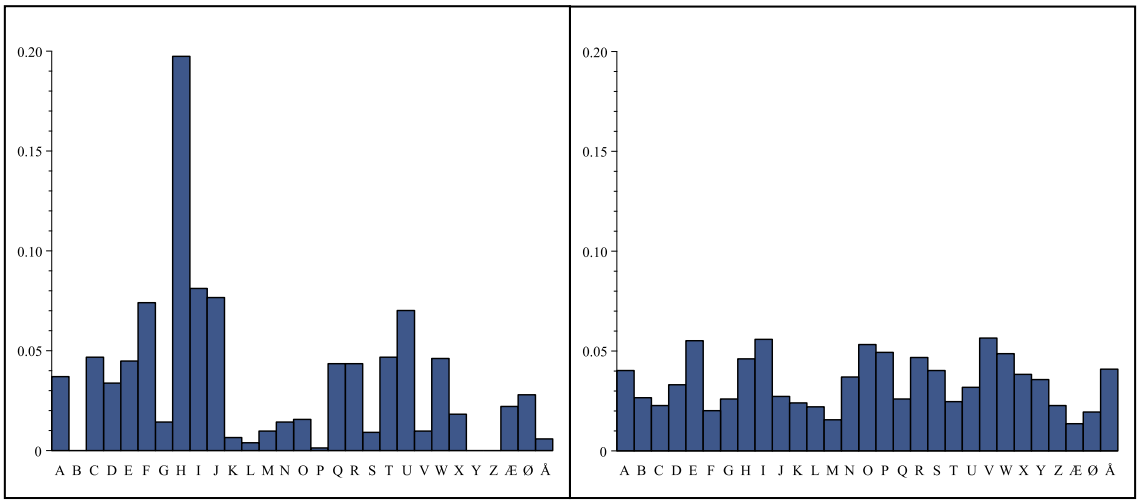
Du får her brug for både at se en video og at arbejde i det tilhørende Maple dokument (venstreklik for at åbne/downloade):

bryd_monoalfabetisk_system.mp4
bryd_monoalfabetisk_system.mw

I videoen forklares skridt for skridt processen med at bruge Maple og frekvensanalyse til at dekryptere en kryptotekst, som er krypteret med et monoalfabetisk kryptosystem. Ovenstående Maple fil er netop den Maple fil, som gennemgås i videoen.

3. Polyalfabetiske kryptosystemer

Leon Battista Alberti (1404-1472), som desuden var en fremragende arkitekt, omtales som en af de første, der har anvendt flere alfabeter til at kryptere med. Det gør det sværere at knække koden, fordi bogstavfrekvenserne i kryptoteksten normalt bliver mere udjævnet. Vi har krypteret den samme klartekst med henholdsvis et monoalfabetisk kryptosystem og et polyalfabetisk kryptosystem og afbildet bogstavfrekvenserne for de to kryptotekster på figuren nedenfor. Det illustrerer tydeligt påstanden om, at bogstavfrekvensen i den kryptotekst, som stammer fra det polyalfabetiske system, er meget mere jævn.



Bogstavfrekvens: Monoalfabetisk kryptosystem

Bogstavfrekvens: Polyalfabetisk kryptosystem

Blandt de bedst kendte eksempler på et polyalfabetisk kryptosystem er det såkaldte *Vigenère-chiffer*. Det er opkaldt efter den franske kryptograf Blaise de Vigenère (1523-1596), selv om det faktisk var kendt før. Systemet er karakteriseret ved at man har en såkaldte *nøgle*, som er en tekststreng. Bogstaverne heri fortæller, hvilke alfabeter, der benyttes hvornår. På næste side er der et eksempel på, hvordan systemet anvendes. Et godt eksempel på, hvor Vigenère-chifferet blev anvendt i historien, er under den amerikanske borgerkrig 1861-1865. John C. Pemberton, som havde kommandoen over de konfødererede styrker i Mississippi, sendte den 26. december 1862 en meddelelse til Joseph E. Johnston, der havde overordnet kommando over Konføderationens vestlige styrker. Meddelelsen var krypteret med Vigenère-chifferet. Se [L1]. I øvrigt led Pemberton senere nederlag til Unionshærens generalmajor Ulysses S. Grant ved Vicksburg.

Blaise de Vigenère (1523-1596)

Eksempel 6

I en anvendelse af Vigenère-chifferet antager vi, at nøgleordet er `HEJ` og at klarteksten er "Matematik er skønt". Først skriver vi klarteksten med små bogstaver. Dernæst skriver vi nøgleordet ovenover. Hvis det er kortere end klarteksten, gentager vi blot nøgleordet. For at finde ud af, hvad `m` i klarteksten krypteres til, kigger vi ovenfor i nøglen og ser, at der står `H`. Vi kigger nu i Vigenère tableauet nedenfor: I søjlen under `M` i øverste række og i det vandrette alfabet ud for bogstavet `H` i venstre side finder vi bogstavet `T`. Derfor krypteres `m` til `T`. Næste bogstav i klarteksten er `a`, og over det står `E`. Derfor kigger vi i søjlen under `A` i øverste række og ud for alfabetet `e` i venstre side. Det giver, at `a` krypteres til et `E`. Sådan fortsætter man indtil man har den færdige kryptotekst: `TEÅLQJÆMTLVØRCWÆ`.

Nøgle:	H E J H E J H E J H E J H E J H
Klartekst:	m a t e m a t i k e r s k ø n t
Kryptotekst:	T E Å L Q J Æ M T L V Ø R C W Æ

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B
D	D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C
E	E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D
F	F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E
G	G H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F
H	H I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G
I	I J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H
J	J K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I
K	K L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J
L	L M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K
M	M N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q
S	S T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R
T	T U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S
U	U V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S T
V	V W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S T U
W	W X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S T U V
X	X Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S T U V W
Y	Y Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S T U V W X
Z	Z Æ Ø Å A B C D E F G H I J K L M N O P Q R S T U V W X Y
Æ	Æ Ø Å A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ø	Ø Å A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ
Å	Å A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Æ Ø

Lad os prøve at gå den anden vej, altså dekryptere kryptoteksten "TEÅLQJÆMTLVØRCWÆ". Dette gøres ved i øverste række i tableauet at finde det første nøglebogstav, som er et H. Derefter opsøger man det sted i søjlen under H, som indeholder første bogstav i kryptoteksten, altså T, og går ud til venstre. Det giver et M, så første bogstav i klarteksten er altså et m. Man gentager processen med det næste nøglebogstav, etc., indtil man har den fulde klartekst, som er matematikerskønt.

Nøgle:	H E J H E J H E J H E J H E J H
Kryptotekst:	T E Å L Q J Æ M T L V Ø R C W Æ
Klartekst:	m a t e m a t i k e r s k ø n t

□

Opgave 7

I en anvendelse af Vigenère-chifferet antager vi, at nøgleordet er GIRAF og at klarteksten er "Studietur i London". Benyt Vigenère-tableauet til manuelt at bestemme kryptoteksten.

Opgave 8

Givet kryptoteksten "KUCWHIÅCPEVOYMB", som er krypteret med Vigenère-chifferet med nøgleordet "HUSK". Benyt Vigenère-tableauet til manuelt at bestemme klarteksten.

Opgave 9 (Opgave i Maple)

Læs teksten i Maple filen (venstreklik):

krypter_og_dekrypter_vigenere_system.mw

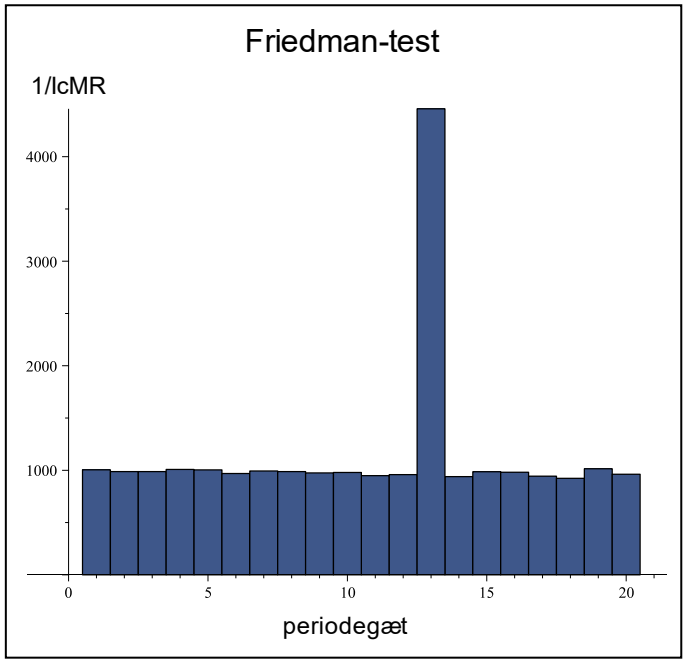
og løs de fire opgaver i filen.

I lang tid efter opfindelsen af Vigenère-chifferet troede man, at det nærmest var ubrydeligt. Men i 1863 publicerede den tyske infanteriofficer *Friedrich Kasiski* (1805-1881) en metode til at angribe et polyalfabetisk kryptosystem såsom Vigenère-chifferet. Metoden går under navnet *Kasiski-testen*. Vi skal ikke komme ind på den nærmere her. Englænderen *Charles Babbage* havde dog allerede i 1846 udviklet en lignende metode. Vigenère-chifferet fik for alvor sit banesår i 1920, da en kryptolog i den amerikanske hær, *William F. Friedman* (1891-1969) opfandt begrebet *index of coincidence*, som kan oversættes til *indeks for sammenfald*. Det gjorde det nemmere og

William F. Friedman (1891-1969)

mere effektivt at bestemme nøglens længde, altså perioden. Hvis man tænker lidt over det, vil man kunne indse, at hvis perioden for eksempel er 5, så ved man, at hvert femte bogstav i kryptoteksten er krypteret med det samme alfabet! Hvis man derfor opdeler teksten i 5 blokke, kan man sige at hver blok er krypteret med et monoalfabetisk system! En komplikation er dog, at man mister den sammenhængende struktur af ord og sætninger. En anden dum ting er, at man i hver blok kun får en tekstlængde, som er 1/5 af den oprindelige, hvilket gør det sværere at bruge statistik. Under alle omstændigheder er det en stor hjælp at have perioden. Et gode er imidlertid, at man har flere blokke, så man kan bruge *krydsreferering*. Det er også muligt at foretage såkaldte *kendt-klartekst-angreb*. hvor man gætter på fraser, som eventuelt måtte figurere i den ukendte klartekst. Vi skal ikke gå nærmere ind på de omtalte tests her. Den interesserede læser opfordres til at studere deres virkemåde nærmere i kilden [1]. Vi skal derimod blot benytte Friedman-testen, som er indbygget i Kryptologi-pakken i Maple.

Figuren herunder viser et stolpediagram, som bygger på en videreudvikling af den oprindelige Friedman-test. Førsteaksen indeholder gæt på nøglelængden og andenaksen indeholder en størrelse, som fremgår af [1]. Vi skal ikke gå i detaljer. Pointen er, at den værdi for periodegættet, som har den højeste søjle, er et godt bud på perioden (nøglelængden). Det aktuelle stolpediagram fås frem ved i Kryptologi-pakken i Maple at fodre kommandoen *friedmanTest* med den samme kryptotekst, som giver anledning til det højre histogram på side 6. Vi konstaterer, at 13 er et rigtig godt bud på nøglelængden!



Opgave 10

Læs teksten i Maple filen (venstreklik):

bryd_vigenere_system.mw

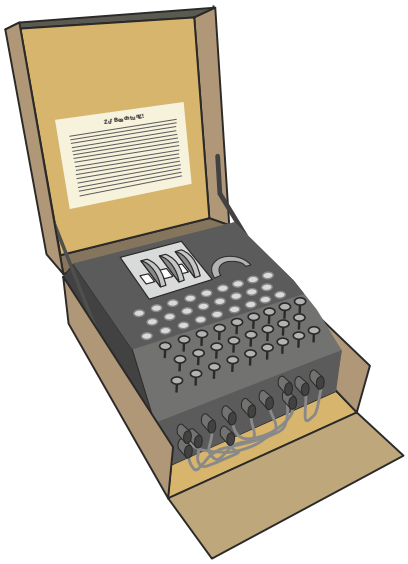
og løs de to opgaver i filen.

4. Enigma kodemaskinen

Den mest legendariske elektromekaniske maskine til at generere hemmelige meddelelser er uden tvivl den tyske kodemaskine *Enigma*, som blev anvendt under 2. Verdenskrig. Årsagen til det er først og fremmest at historien om den er så spektakulær og på grund af vigtigheden af at bryde koden. Tyskerne troede igennem hele krigen, at det var umuligt at bryde Enigma. Virkeligheden var, at tusinder af smarte, især unge britiske mænd og kvinder var samlet under stor hemmeligholdelse på et landligt sted kaldet *Bletchley Park*, nord for London. De var desuden ledt an af den geniale og excentriske matematiker *Alan Turing*, som leverede vigtige bidrag i kodebrydningen. Store og vigtige fremskridt i brydningen af Enigma var endda i al hemmelighed opnået i Polen allerede før krigen. Historien om brydningen af Enigma er filmatiseret i den meget anmelderroste biografffilm "Imitation Games".

En anden grund til, at jeg tager beskrivelsen af Enigma med i denne lille note er, at krypteringsmetoden i maskinen er et eksempel på en realisation af et polyalfabetisk kryptosystem. Hver gang man trykker et bogstav ind på Enigma-maskinen, som lidt ligner en gammeldags skrivemaskine, rykker et hjul fremad, hvilket betyder, at der skiftes alfabet. *Perioden*, som er det antal tastetryk, der skal til, før maskinen vender tilbage til sin oprindelige tilstand, er meget stor, nemlig 16900. Da meddelelser normalt aldrig er så lange, kan man i kodebrydningen ikke udnytte, at alfabeter gentages. Nedenfor og på næste side er vist en skitse af krypteringsproceduren for Enigma. En mere fyldestgørende forklaring kan ses i en video, som der er link til på næste side. Her gennemgås krypteringsproceduren på en Enigma simulator, som læseren eventuelt selv kan afprøve.

Enigma - krypteringsprocedure



Givet på forhånd:
Antal hjul (Walzen)
Hvilken reflektor (Umkehrwalze)

Kodebogen (Schlüsselbuch) med daglig nøgle:
Hvilke hjul skal bruges og i hvilken rækkefølge
Ringindstillingerne for hjulene (Ringstellung)
Plugboard indstillingerne (Steckerverbindungen)

Operatøren vælger:
Indikatorinstilling (Grundstellung)
Meddelelsesnøgle (Spruchschlüssel)

Krypteringer:
Hjulene indstilles efter indikatorindstillingerne,
hvorefter meddelelsesnøglen krypteres.
Hjulene indstilles efter meddelelsesnøglen,
hvorefter klarteksten krypteres.

En meddelelse sendes:
Indikatorindstillingerne
Den krypterede meddelelsesnøgle
Kryptoteksten
med mere …

Nedenfor ses en fiktiv, men realistisk del af en side fra en kodebog med de daglige nøgler til Enigma-maskinen. Kodebogen blev distribueret - typisk månedligt - ud til de enkelte tyske militærenheder, under ekstrem hemmeligholdelse. Vi forestiller os, at datoen er 29. april 2025. På linjen ud for denne dato kan ses hvilke hjul, som skal bruges og i hvilken rækkefølge. Dernæst er der hjulenes *ringindstillinger* (*Ringstellung*), *plugboard-indstillingerne* (*Steckerverbindungen*) og *Kenngruppen*. Sidstnævnte indeholder information om, hvem den krypterede meddelelse er henvendt til.

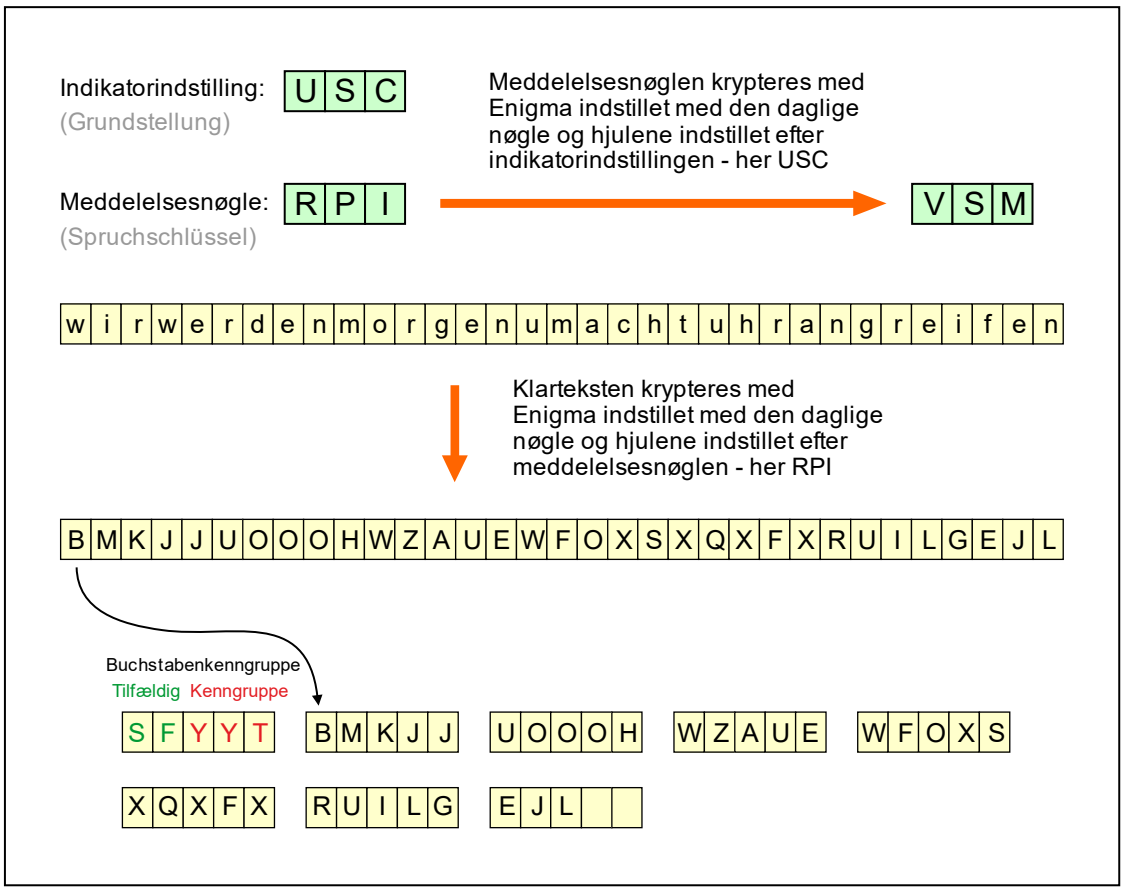
Geheime Kommandosache!
Nicht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. X
für April 2025

fiktive værdier!

	Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
St	**30.**	V I III	22 04 16	TU RQ PL SI NF XW DZ GA YV MB	oab hvs ilg wtm
St	**29.**	I IV II	12 04 21	AQ CT LP MF ES KB YZ HW DR UG	hax oqa kpa yyt
St	**28.**	II III IV	14 25 11	BI XC OF RT MG DV SK JE HL UW	nal clo xaz bab
St	**27.**	V II I	17 23 08	ZA TD WI VR OX PQ FS CM HY BU	kwq rsu uvt rmw
St	**26.**	III I IV	07 10 25	AE GH MT KQ CW JV XZ BI RS UY	xaz nal kcs isg
St	**25.**	II I III	23 02 19	IR NP EM UY KX ST BG DJ HW CV	lai pps lis yao

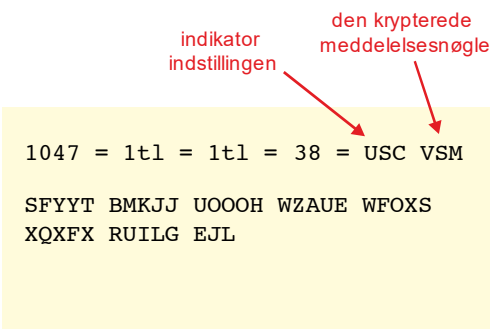
Herunder er vist en illustration af krypteringsproceduren, hvor klarteksten er følgende: "Wir werden morgen um acht uhr angreifen".



Venstreklik på nedenstående link for at se video:

ENIGMA_kryptering_video.mp4 (13:29)

Den endelige krypterede meddelelse afleveres med nogle praktiske oplysninger, som vist på figuren herunder. Vigtigst at forstå her er, at følgende oplysninger er til stede: Den ukrypterede indikatorindstilling og den krypterede meddelelsesnøgle. Derudover indeholder de tre sidste bogstaver i den første 5-blok (her YTT) information fra kodebogens Kenngruppen. Dermed kan enheder, der opsnapper radiomeddelelsen, vide, om meddelelsen er stilet til dem. Endelig indeholder de øvrige 5-blokke den krypterede tekst.



Den krypterede besked blev sendt via morsekode over radio af en radiotelegrafist. Tyske enheder (skibe, ubåde, hærdivisioner osv.) aflyttede radiosignalerne. En modtagende radiotelegrafist skrev den krypterede besked ned. Beskeden blev indtastet i Enigma-maskinen, der var sat til dagens kodeindstillinger, hvorefter beskeden blev dekrypteret. En ansvarlig officer læste herefter klarteksten i beskeden. Radiosignalerne kunne naturligvis også blive opfanget af de allierede, og det blev de. Derfor var det vigtigt for tyskerne, at meddelelserne var krypterede. Lad os i det følgende se på dekrypteringsproceduren hos den modtagende tyske enhed.

Enigma - dekrypteringsprocedure

Kodebogen:

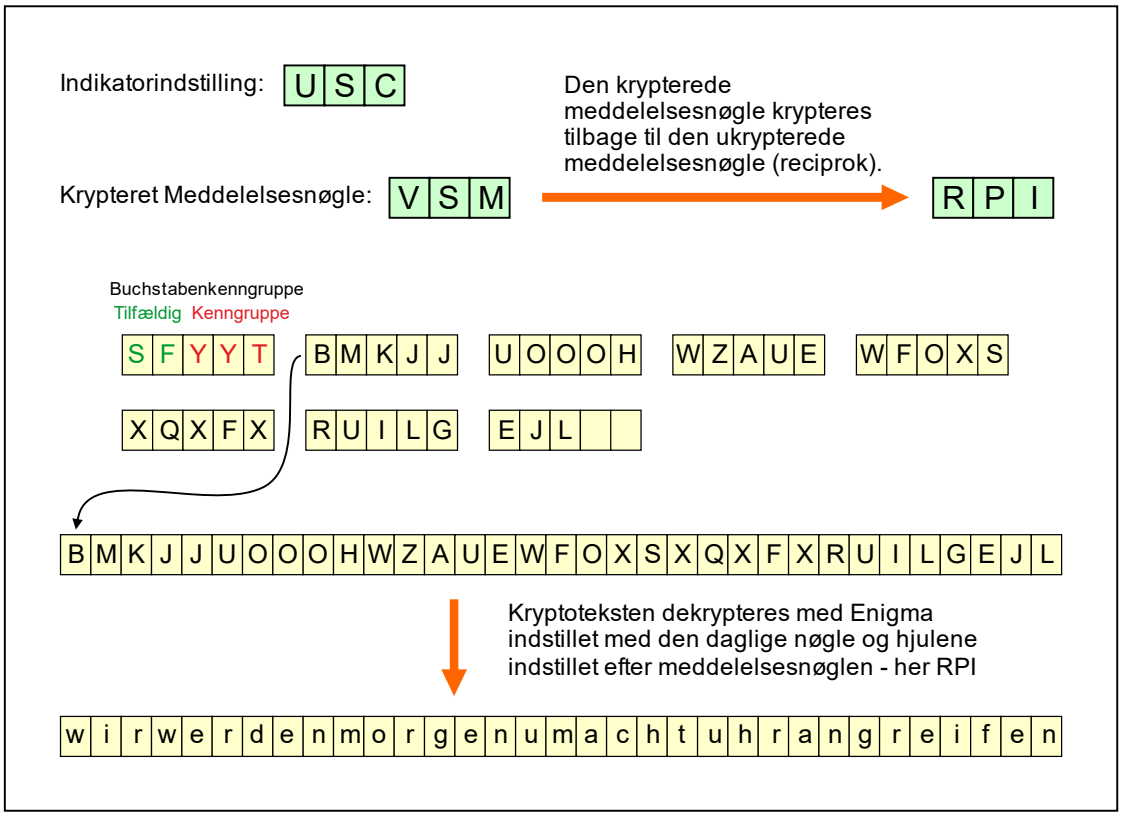
I overensstemmelse med den daglige nøgle:

- De tre hjul med rækkefølge anbringes
- Hjulenes ringindstillinger foretages
- Plugboard indstillingerne foretages

Krypteringer:

- Hjulene indstilles efter indikatorindstillingerne.
- Den krypterede meddelelsesnøgle tastes ind, hvorved den dekrypteres.
- Hjulene indstilles efter meddelelsesnøglen.
- Kryptoteksten efter første 5-blok tastes ind, hvilket giver klarteksten.

På figuren nedenfor er vist dekrypteringsproceduren. Man ender med klarteksten, som i dette tilfælde er "Wir werden morgen um acht uhr angreifen".



Oversættelsen mellem bogstaver og tal fremgår af følgende liste:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Den interesserede læser kan se en video om dekrypteringen demonstreret ved hjælp af en Enigma-simulator. Venstre-klik på linket for at se videoen.

ENIGMA_dekryptering_video.mp4 (5:34)

Enigma-simulatoren, som er meget livagtig, er programmeret af belgieren Dirk Rijmenants. Simulatoren er imidlertid kun til Windows-computere. Se [L3] for et link til siden, hvorfra programmet kan downloades og benyttes gratis.

Selv om matematikken i Enigma-maskinen er nok så interessant, er hovedsigten med denne note en anden. Matematikken kan studeres nærmere på min hjemmeside [L4]. Overordnet skal det dog nævnes, at de matematiske objekter kaldet *permutationer* kan benyttes til at beskrive, hvad der sker i Enigma-maskinen, når et bogstav trykkes ind. Man kan vise, at de involverede permutationer udelukkende består af såkaldte 2-cykler. Det gør Enigma på en gang praktisk, men også lidt sårbar. Praktisk fordi dekrypteringsproceduren

er den samme som krypteringsproceduren forstået på den måde, at man indstiller maskinen efter den daglige nøgle samt meddelelsesnøglen og så bare trykker ind. Trykker man klarteksten ind, fås kryptoteksten. Hvis kryptoteksten trykkes ind, fås klarteksten. Vi siger, at Enigma er *selvreciprok*. Men egenskaben med 2-cykler betyder også en sårbarhed, for et bogstav kan dermed ikke krypteres til sig selv! Folkene i Bletchley Park udnyttede selvfølgelig alle tænkelige svagheder ved Enigma og ikke mindst måden den blev anvendt på. Det vil føre alt for vidt at komme ind på det her. Uanset hvad, var det dog en umådelig stor opgave at knække Enigma. Det krævede et væld af folk og stor opfindsomhed. Med opfindelsen af de såkaldte *Bombs*, som meget snedigt var udtænkt af især matematikeren Alan Turing, kunne man bringe antallet af de Enigma-indstillinger, man skulle afprøve, ned på et tåleligt antal. Selv da var der perioder af krigen, hvor det ikke lykkedes at knække koden – for eksempel når tyskerne introducerede ændringer i Enigma. Lad os slutte afsnittet af med et foto af en rigtig Enigma-maskine.

Opgave 11

a) Du har den 30. april 2025 opsnappet den radiomeddelelse, som fremgår af sedlen til højre. Benyt oplysningerne herpå samt kodebogen side 11 til at indstille Enigma rigtigt. Dekrypter derefter kryptoteksten.

```
1138 = 1tl = 1tl = 48 = DHM HWS

UBILG ZZDCN SSRUG CRVKV BLRWD
KXUII HNGQF VGVOV IFKTA TUW
```

NB! De danske bogstaver Æ, Ø og Å skrives som henholdsvis AE, OE og AA.

b) Find selv på en klartekst på 1-2 linjer. Den må kun indeholde bogstaverne fra A til Å. Vælg derefter selv tre bogstaver for en indikatorindstilling og tre bogstaver for meddelelsesnøglen. Benyt kodebogen side 11 for den 28. april 2025. Krypter din klartekst og send meddelelsen til en anden fra klassen. Denne skal så dekryptere.

□

5. Moderne kryptologi – Public Key systemer

De kryptosystemer, som vi har kigget på hidtil, er eksempler på de traditionelle *symmetriske kryptosystemer*, hvor man bruger den samme nøgle til at kryptere og dekryptere med. En af ulemperne med disse systemer er, at man skal *udveksle* nøglerne på en måde, så de ikke kommer i hænderne på personer, der ikke må kunne læse de krypterede meddelelser. En anden ulempe er, at han skal distribuere en masse forskellige nøgler, måske helt op til at ethvert par af personer, som skal kommunikere hemmeligt. Så er der også en *digital signatur*, som ikke kan etableres ved hjælp af et symmetrisk kryptosystem. Altså en sikker måde at kunne underskrive på digitalt. Et klassisk symmetrisk kryptosystem er helt utilstrækkeligt til et moderne informationssamfund med Internet, netbanker, webshops, emails, MitId, bitcoin, etc.

I 1976 publicerede de to matematikere Whitfield Diffie og Martin Hellman den banebrydende artikel *New Directions in Cryptography* (se [2]). Dermed var visionen om et Public-Key kryptosystem skabt. De to var de første til at offentliggøre idéen om asymmetrisk kryptografi, hvori der introduceres nøgleudveksling uden en sikker kanal. Tanken er at hver bruger skal udstyres med et par af nøgler, hvor den ene er offentlig og den anden privat. Den offentlige nøgle må alle i princippet kende, mens den private nøgle skal holdes strengt privat.

Året efter publicerede tre andre matematikere, Ron Rivest, Adi Shamir og Leonard Adleman artiklen *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (se [3]). Heri beskrev matematikerne det i dag berømte RSA-system, som bygger på talteori – man arbejder med meget store tal, som er sammensat af store primtal. Det såkaldte RSA-system var den første praktiske implementering af Diffie og Hellmans vision. Vi skal ikke gå i detaljer med det her. Den interesserede læser kan konsultere [1] og/eller [5]. Derimod skal vi forsøge at forstå mekanismerne i et Public-Key system.

For at forstå principperne bag Public-Key systemet bedre har det været kutyme at anvende et sigende Alice-Bob eksempel. Jeg har på de næste sider konstrueret tre forskellige måder, hvorpå Bob sender en meddelelse til Alice. Meddelelsen kan for eksempel være følgende: "Jeg elsker dig. Lad os mødes i kantinen til middag". En sådan besked kan selvfølgelig uden videre sendes ukrypteret, men måske ønsker Alice og Bob at holde romancen hemmelig. Måske er der personer, som de to ikke ønsker lytter med. Det kan endda være, at der er andre, som ikke bare lytter med, men måske agerer negativt i forhold til deres relation, og kan Alice i det hele taget være sikker på, at meddelelsen kommer fra Bob? Kan der fuskes med meddelelsen undervejs? Kan Bob nægte at have sendt meddelelsen? I tegneserien to sider fremme lytter Malene med på linjen. Hun er lun på Bob.

I et Public-Key system er hver person udstyret med både en offentlig og en privat nøgle. I det følgende lader vi P_A og S_A betegne henholdsvis Alices offentlige nøgle og Alices private nøgle – *P* for Public og *S* for Secret. De tilsvarende nøgler for Bob er P_B og S_B. Uden at gå i detaljer med, hvordan det foregår i praksis, forestiller vi os, at vi kan anvende en nøgle på en besked *m*. Det medfører at teksten ændres, dvs. krypteres. Således betyder $P_A(m)$, at vi opererer på *m* med Alices offentlige nøgle. En vigtig pointe er nu, at en persons offentlige og private nøgle ophæver hinandens virkning, altså $S_A(P_A(m)) = m$ og $P_A(S_A(m)) = m$. Tilsvarende for Bob. På den måde er de to nøgler *inverse* til hinanden. Og hvad der er mindst lige så vigtigt: En meddelelse, som er krypteret med en persons offentlige nøgle, kan i praksis *kun* dekrypteres med personens private nøgle! Der er fire sikkerhedsegenskaber i spil her:

Konfidentalitet	Fortrolighed. Sikrer, at beskedens klartekst kun er tilgængelig for den eller dem, der er autoriseret til at se den.
Autenticitet	Ægthed. Man kan verificere, om beskeden kommer fra den person, som har sendt meddelelsen.
Integritet	Uberørt. Sikrer, at hvis beskeden er blevet ændret eller manipuleret under transmission, så vil modtageren kunne verificere det.
Ikke-afvisning	Sikrer, at afsenderen ikke kan nægte at have sendt beskeden.

Lad os kigge på de tre situationer i omtalte tegneserie. Meddelelsen, som Bob sender, er følgende: *m* = "Jeg elsker dig. Lad os mødes i kantinen til middag". Malene, som er lun på Bob, lytter med på den åbne kanal.

Situation 1

Bob krypterer meddelelsen *m* med Alices offentlige nøgle og sender resultatet til Alice via den ubeskyttede kanal. Alice modtager og dekrypterer den modtagne kryptotekst med sin egen private nøgle. Kun Alice kan gøre det. Malene ser kun noget uforståelig tekst, da hun ikke kan dekryptere det, hun opsnapper.

Situation 2

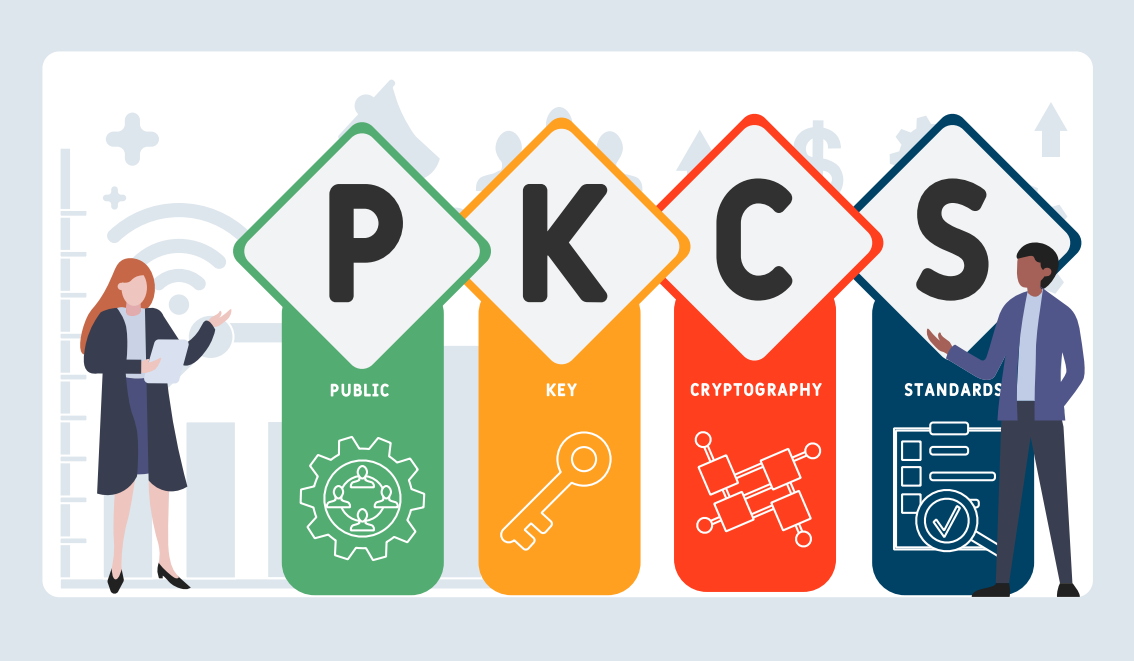
Bob krypterer m med sin egen hemmelige nøgle og sender resultatet til Alice. Alice kan læse beskeden efter at have dekrypteret med Bobs offentlige nøgle. Malene kan også dekryptere og ser Bobs besked. Bobs offentlige nøgle er jo frit tilgængelig.

Situation 3

Bob krypterer først m med sin egen hemmelige nøgle og derefter med Alices offentlige nøgle. Alice kan dekryptere og læse Bobs klartekst, mens Malene ikke kan.

Opgave 12 (Spørgsmål til tegneserie)

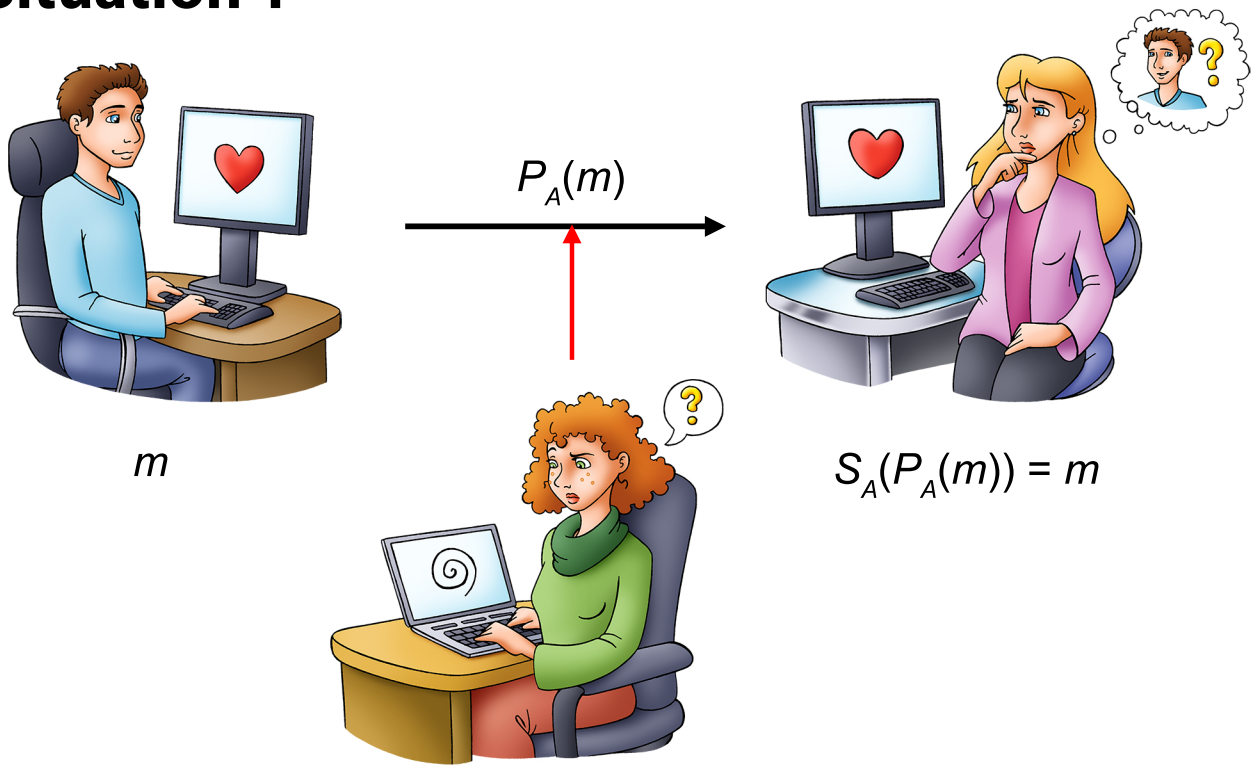
a) Hvorfor kan Alice dekryptere beskeden, mens Malene ikke kan i situation 1.
b) Hvorfor mon Alice ser mere afklaret ud i situation 2 end i situation 1?
c) Hvordan kan Malene dekryptere den opsnappede kryptotekst i situation 2?
d) Hvad må Alice gøre for at få klarteksten i situation 3?
e) Hvorfor kan Malene ikke dekryptere i situation 3.
f) Gå sikkerhedsegenskaberne igennem i de tre situationer: Hvilke er opfyldt i hver enkelt situation? Resultatet er side 19.



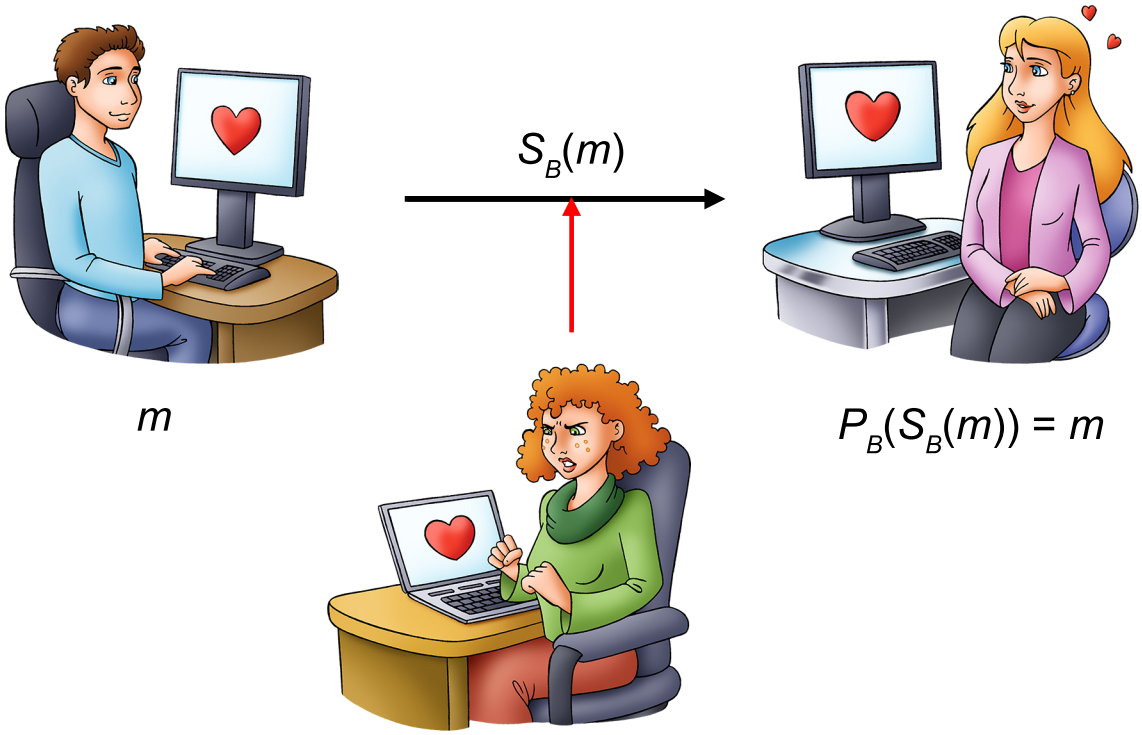
Med tegneserien er nogle principper bag public-key system søgt illustreret. Det er dog kraftigt simplificeret for at få de vigtige pointer med to nøgler – en offentlig og en privat – ud over rampen. For eksempel vil man i praksis anvende en *hybrid-model*, hvor dele af krypteringerne er foretaget med et almindelig symmetrisk kryperingsværktøj såsom *AES* (*Advanced Encryption Standard*). Det skyldes, at disse kan foretages 10-1000 gange så hurtigt, som hvis man benyttede RSA eller ECC, som er egentlige Public-key systemer. Sidstnævnte gør brug af såkaldte elliptiske kurver.

Public Key kryptering

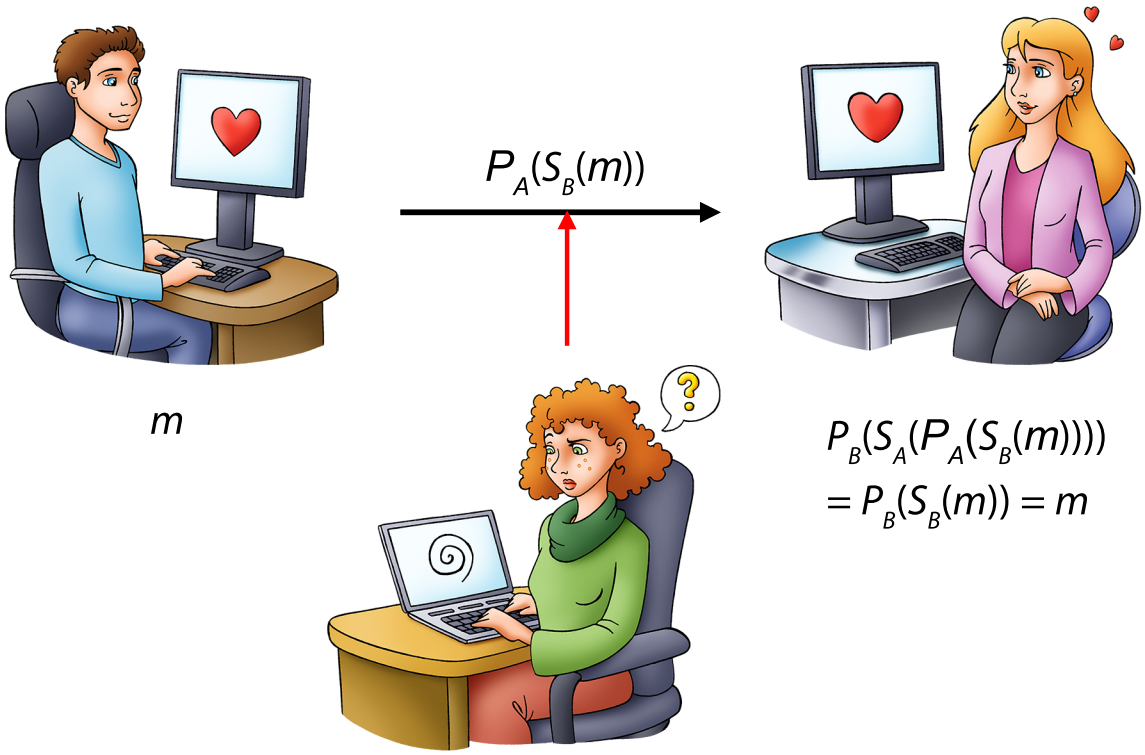
Situation 1



Situation 2



Situation 3



Sikkerhedsegenskaber

Situation	1	2	3
Konfidentalitet	✓	✗	✓
Autenticitet	✗	✓	✓
Integritet	✗	✓	✓
Ikke-afvisning	✗	✓	✓

Digital signatur

I situation 2 i tegneserien er princippet bag begrebet *digital signatur* uden hemmeligholdelse demonstreret. Alice kan med sikkerhed vide, at meddelelsen er fra Bob, for han har "underskrevet" meddelelsen. Hvordan det? Jo, fordi enhver vil ved anvendelse af Bobs offentlige nøgle på kryptoteksten kunne konstatere, at det giver noget meningsfuldt (klarteksten). Dermed må kryptoteksten være krypteret med Bobs private nøgle, som kun han har! Dermed haves Autenticitet. Der er også integritet, for hvis der var blevet ændret i kryptoteksten undervejs, ville der med uhyre stor sandsynlighed være kommet noget uforståeligt ud af det, når Bobs offentlige nøgle blev anvendt. Man har også egenskaben ikke-afvisning: Bob kan ikke afvise, at meddelelsen kommer fra ham, for kun han kan bruge Bobs private nøgle. Først i situation 3 får man udover den digitale signatur også hemmeligholdelse, altså konfidentialitet. For at opsummere: Man kan altså "underskrive" et dokument med sin private nøgle!

En simplifikation, som vi har foretaget i tegneserien er, at Bob i situation 2 krypterer hele meddelelsen med sin private nøgle. Det ville aldrig foregå i virkeligheden. Der er to grunde til det: Dels er metoden for omkostningstung regnet i tid, hvis bare teksten har en vis længde. Den anden grund er, at vi jo heller ikke kan have – som tilfældet var ovenfor – at vi skal afgøre om man opnår noget "meningsfuldt" ved at anvende en nøgle. Det er for upræcist. I stedet anvender man en såkaldt *hash*-funktion på hele teksten. Det vil føre for vidt at komme ind på den i detaljer. Her skal det blot tænkes på som en funktion, der tager et slags "fingeraftryk" af hele meddelelsen og leverer en hash-værdi, som er en streng af en fast længde. Denne streng krypteres så med Bobs private nøgle (dvs. underskrives) og resultatet sendes sammen med hele meddelelsens klartekst. I den anden ende kan modtageren så anvende Bobs offentlige nøgle til at dekryptere hash-værdien. Derefter anvendes hash-funktionen på klarteksten i selve meddelelsen. Hvis resultatet af denne handling er identisk med den dekrypterede hash-værdi, har man autenticitet, integritet og ikke-afvisning opfyldt. Man kan selvfølgelig også kryptere selve meddelelsen, fx med AES. Den interesserede læser kan læse meget mere om det i [4].

Public-key infrastruktur

Når man skal bruge Public-key i praksis, kræver det en slags infrastruktur. Selvom det i sagens natur ikke kræver en sikker kanal at bruge en offentlig nøgle, så kræves der autentificerede kanaler til distribution af de offentlige nøgler. Hertil benyttes *certifikater*. Certifikaterne binder en brugers identitet til deres offentlige nøgle. Ikke mere om det her.

Opgave 13 (ChatGPT/Copilot)

a) Spørg ChatGPT/Copilot om fordele og ulemper ved et symmetrisk kryptosystem sammenlignet med et asymmetrisk kryptosystem.

b) Spørg ChatGPT/Copilot om hvad *Man-in-the-middle* problematikken er, og hvordan det er løst i Public-key systemet.

Opgave 14 (ChatGPT/Copilot)

Når man bruger Internettet, står der i URL'en på adresselinjen `http://` eller `https://` foran det egentlige domænenavn. Benyt ChatGPT/Copilot til at besvare nedenstående.

a) Undersøg hvad elementerne `http://` og `https://` er godt for i en URL. Hvad er forskellen på de to?
b) Spørg ChatGPT/Copilot om følgende: "hvorfor er udelukkende brug af symmetrisk kryptografi ikke tilstrækkeligt til at realisere Internettets funktion?".
c) Spørg ChatGPT/Copilot om følgende: "Hvilke kryptografiske elementer er i spil i forbindelse med brugen af SMS?".
d) Prøv at stille samme spørgsmål hvad angår email.

Opgave 15

Lad os sige, at vi i et Public-key system også har brug for at udveksle en symmetrisk nøgle K mellem to brugere over en usikker kanal.

a) Forklar hvordan denne udveksling kan finde sted på en hensigtsmæssig og sikker måde ved brug af Public-key systemet. *Hjælp*: Tænk på situation 3.
b) Hvorfor er denne udveksling en udfordring, hvis man ikke er brugere i et Public-key system?

Links

[L1] Civil War Ciphering: Confederate Coding in the Vicksburg Campaign, 1863:
https://cwrgmblog.org/civil-war-ciphering-confederate-coding-in-the-vicksburg-campaign-1863/

[L2] Confederate Ciphers during the Civil War: Various Vigenere Keywords:
https://cryptiana.web.fc2.com/code/civilwar4.htm#SEC3

[L3] Enigma simulator til Windows ved Dirk Rijmenants:
https://www.ciphermachinesandcryptology.com/en/enigmasim.htm

[L4] Den tyske kodemaskine Enigma:
https://matematiksider.dk/enigma.html

[5] Enigma Simulator til Mac:
http://www.terrylong.org/

[6] Alice and Bob:
https://en.wikipedia.org/wiki/Alice_and_Bob
https://cryptocouple.com/

[7] Public Key Cryptography - VIDEO
Asymmetric Encryption - Simply explained:
https://www.youtube.com/watch?v=AQDCe585Lnc

[8] Security in Computing - Modern Cryptography - VIDEO
https://www.youtube.com/watch?v=7I0rOMiuCc4

Litteratur

[1] Peter Landrock, Knud Nissen. *Kryptologi – fra viden til videnskab*. Forlaget ABACUS, 1997.
[2] Whitfield Diffie, Martin Hellman. *New Directions in Cryptography*. IEEE Transactions on Information Theory, vol IT-22, No. 6, November 1976.
[3] Rivest, Shamir, Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM. 21 (2) side 120–126.
[4] Christof Paar, Jan Pelzl. *Understanding Cryptography – A Textbook for Students and Practitioners*. Springerverlag 2010.
[5] Erik Vestergaard. *RSA kryptosystemet*.
https://www.matematikfysik.dk/mat/noter_tillaeg/RSA.pdf