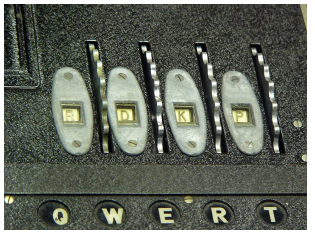


Velkommen til

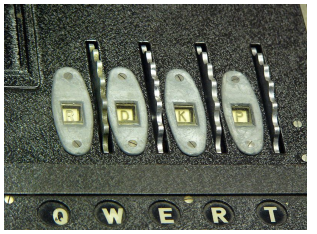
Kryptering: status for politikere og andre interesserede

Folkemødet 2017

Henrik Lund Kramshøj hlk@kramse.org

PDF available kramse@Github

Status på sikkerhed og kryptering



Dette indlæg er også et oplæg til debat

men fair warning jeg har tænkt over disse ting siden Crypto Wars 1.0 i 1990erne - så der skal nok vægtige argumenter til - come at me ☺

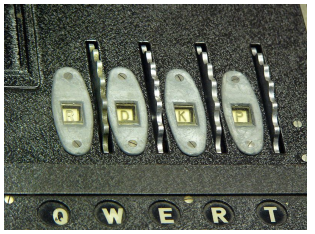
Jeg driver eksempelvis velvilligt nogle af Danmarks største Tor-servere som hjælper kriminelle, men også andre.

Jeg er indædt modstander af sessionslogningen

Jeg kæmper imod censur og *blokeringsordningen* i Danmark

PS Beklager at dette slideshow er lidt tungt med meget tekst, hent det som PDF senere

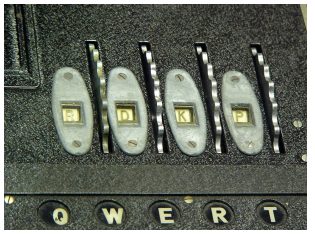
Kryptering

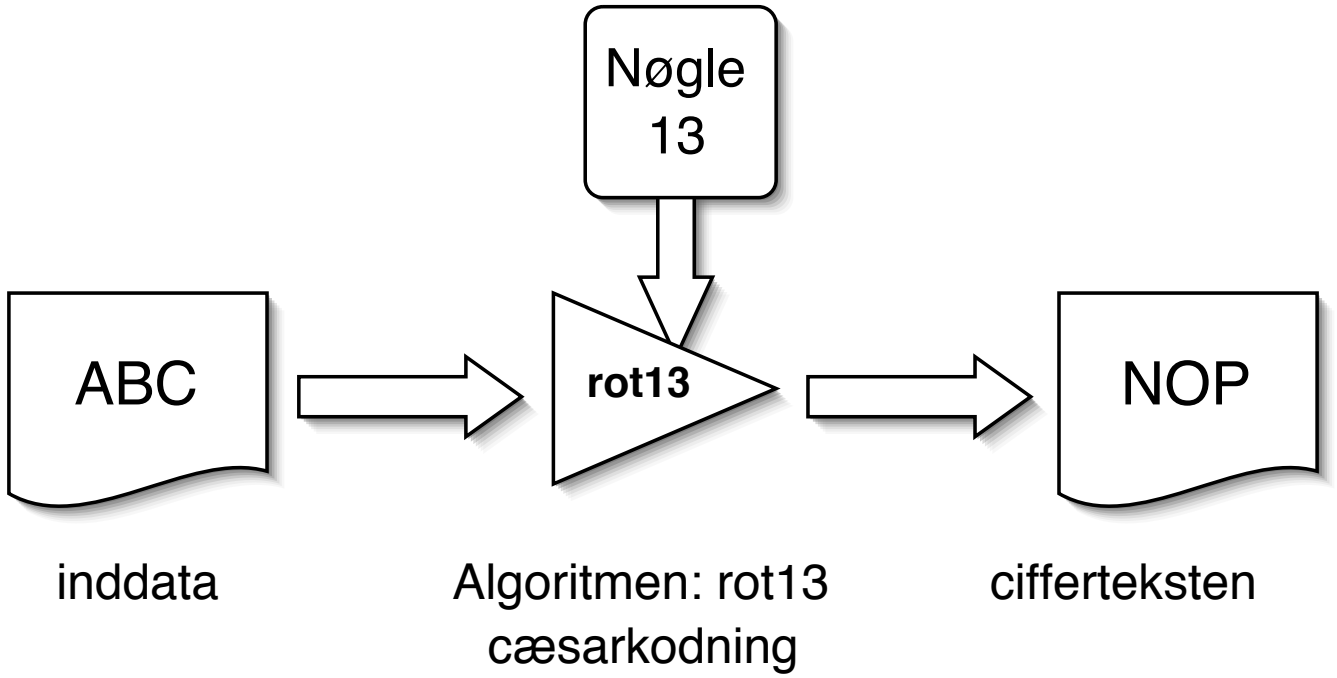


Definition Kryptering er et område inden for kryptologien, der beskæftiger sig med hemmeligholdelse af information, der kan opsnappes af en tredjepart. Den omfatter bl.a. hemmeligholdelse under transmission over en ikke-sikker kommunikationskanal (f.eks. e-mails eller internet-kommunikation), samt sikring af data (f.eks. filer på en computer, der kan blive stjålet eller hacket).

Kilde: https://da.wikipedia.org/wiki/Kryptering

Kryptografiske algoritmer

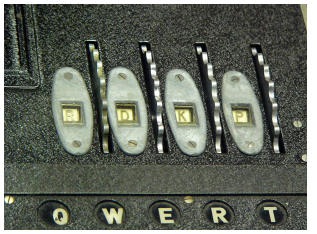


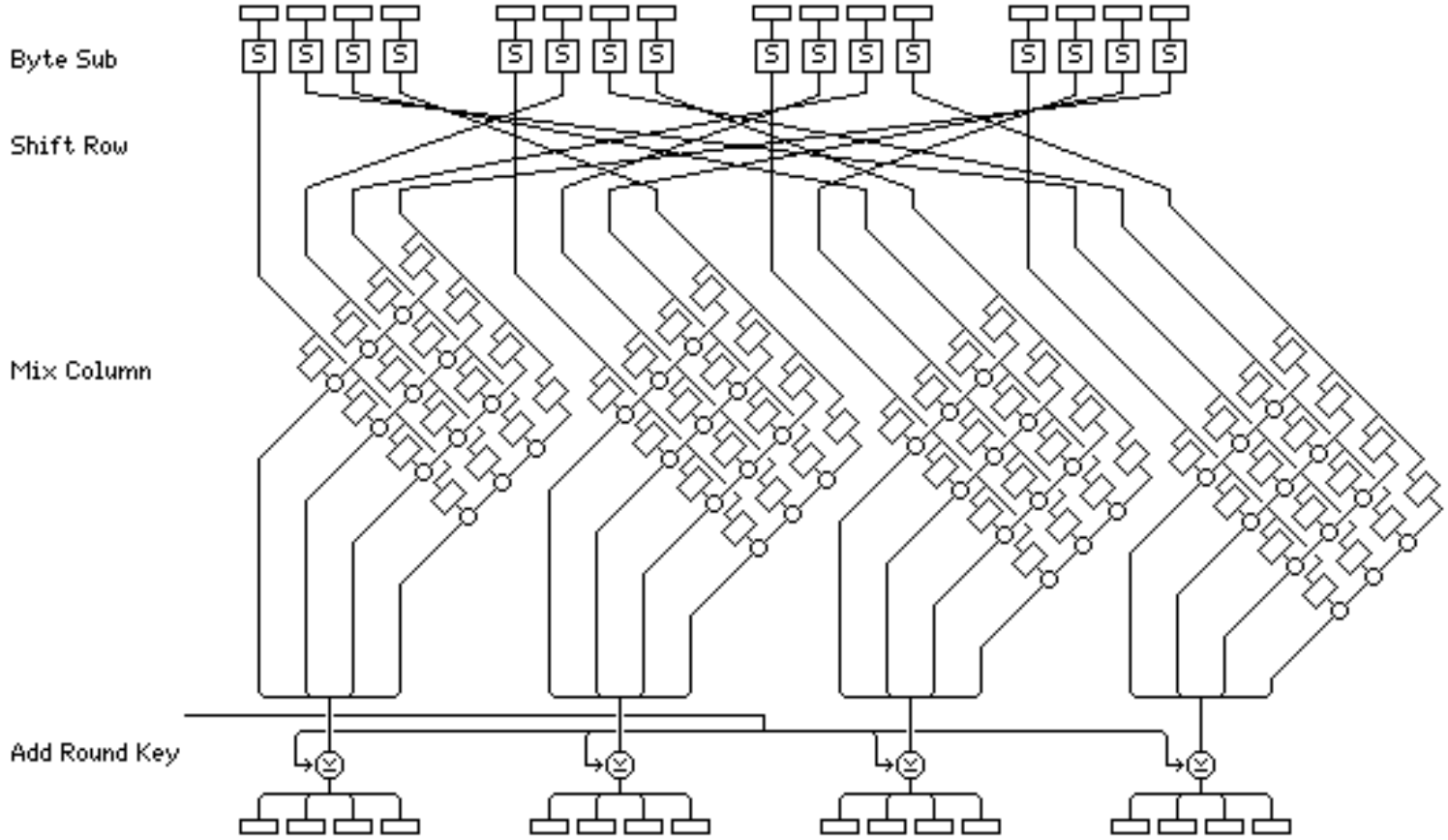


Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en ciffertekst - der kun kan læses ved hjælp af den tilhørende nøgle

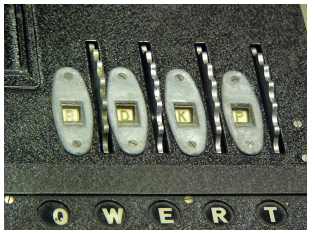
Moderne krypteringsalgoritmer





Idag bruges i hele verden Rijndael/AES udviklet i Europa af Belgiske kryptografer, Vincent Rijmen og Joan Daemen

Kryptering er overalt



Vi bruger mere https end http - dvs vores web sites bliver oftere krypteret.

Det er godt, andre kan ikke lytte med. Vi kan trygt besøge sites, læse indhold, uploade indhold, tale privat om alt og ingenting. Snowden om privacy

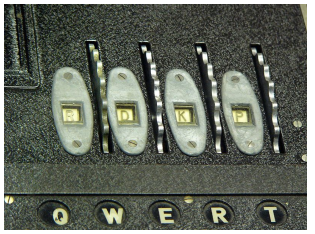
> Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say," Snowden omkring "nothing to hide"

Forenede nationer om overvågning og privatliv

> surveillance threatens individual rights – including to privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society.

Vi har ret til privatliv, privatliv er en menneskeret.

Kryptering er stærkt



Når vi læser Snowden afsløringerne så ser vi at der er lavet verdensomspændende forsøg på aflytning, og det har mange politiske konsekvenser - glem dem lige nu

Vi kan dog se at hvis vi bruger moderne metoder, bygget på sund matematik så er det stærkt.

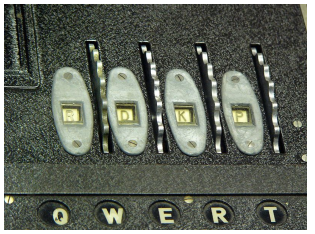
Ingen kan åbne vores kommunikation hele tiden - altid
(NSA kan rigtigt meget hvis du er interessant nok)

Solidaritetskryptering

Når vi krypterer giver vi andre beskyttelse. Vi kan bruge kryptering i Danmark, det er lovligt. Vi kan være talerør for andre, vi kan publicere for andre, vi kan være mængden der gør at andre kan skjule sig.

Giv mig Danmark tilbage, ligesom i de gamle dage hvor vi stod for ytringsfrihed, fælleskab, støtte til de svage

Kryptering hjælper alle

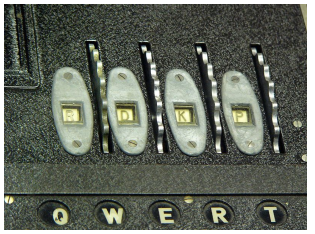


Kryptering er fundamentet for vores moderne digitale samfund. Vores velfærd er afhængig af effektiv - stærk - kryptering

Uden kryptering:

- Ingen fjernarbejde
- Ingen digitalisering
- Ingen banktransaktioner
- Ingen recepter over Norsk Helsenett
- Ingen e-Handel

Kryptering bruges af terrorister



Ja, desværre

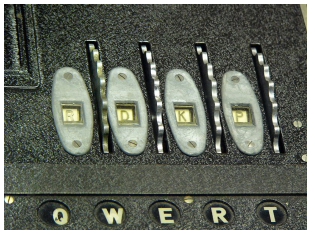
Sager som lukkede telefoner og beskeder sendt via krypteret kommunikation sker ...

Myte, hvis det ikke var krypteret ville man kunne stoppe terror. Desværre er det ofte personer som allerede er kendt, og ikke blev stoppet.

Hvis vi svækker kryptering via regulering og lovgivgning, så svækker vi vores konkurrenceevner, hjælper industrispionage, taber fordelene

... og vil dem som vi ønsker at ramme følge loven, tvivlsomt!

Gode bagdøre findes ikke

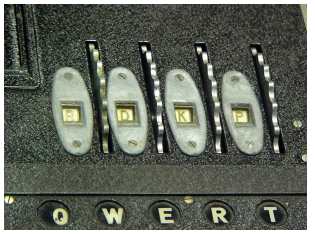


Passwords at the Border Vestlige *demokratier* er begyndt at bede om koderne til at åbne enheder som laptops og telefoner - skidt udvikling

Keys Under Doormats:
mandating insecurity by requiring government access to all data and communications

> Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels “going dark,” these attempts to regulate the emerging Internet were abandoned.
>
> ...

Gode bagdøre findes virkeligt ikke! Forstå det



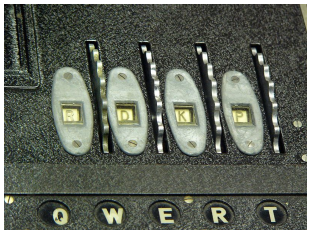
> We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago.
>
> In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dy- namics online should be approached with caution.

Forfatterne der udtaler dette er et dreamteam af teknologer, kryptografer

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

I bruger allesammen deres teknologier og viden - hver dag!

Know technology

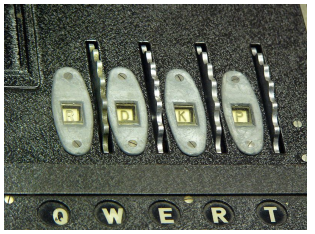


Aaron Swartz once said, ”It’s no longer OK not to understand how the Internet works.”

I skal som politikere kende til teknologierne, ellers ødelægger i mulighederne og fordelene.

Source: https://boingboing.net/2017/06/04/theresa-may-king-canute.html

Danske bagdøre



`@KimAarenstrup ønsker ikke bagdøre i software. #fmdk`

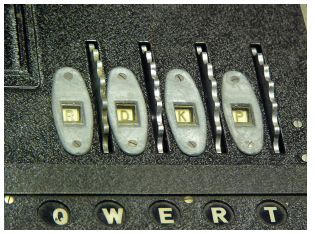
Kilde: twitter via Steen Thomassen @steenthomassen
https://twitter.com/steenthomassen/status/875334247120330753

Rygtet vil vide at dansk politi ikke ønsker bagdøre

Mange tak til Kim for den udmelding, han risikerer et internetkram fra hele det danske internet community!

Vi har ellers rockerloven som indført efter Tvindsagerne med netop harddisk kryptering som giver muligheder for trokanske heste m.v.!

Forsøg på internet-censur og lovgivning fejler ofte



> The Net interprets censorship as damage and routes around it.

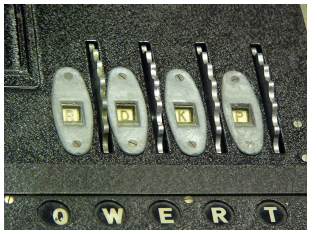
John Gilmore, As quoted in TIME magazine (6 December 1993)

Det samme vil ske med kryptering, nedlukning af internet, osv.

Kilder: arabiske forår, Myanmar, Kinesiske firewall

Nørder og hackere er ekstremt kreative

Anonymitet og kryptering



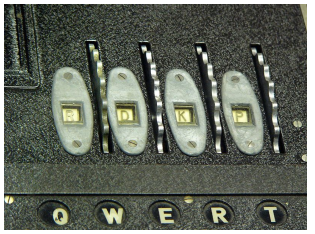
Vi taler altid ekstremer med kryptering, men hvad med:

- Stalking-sager, Graverjournalister og andre mediefolk, Partnervold/konfliktskilsmisse
- Diplomatiske forbindelser, Undercover agenter, ja FBI bruger Tor
- Citizen journalism https://en.wikipedia.org/wiki/Citizen_journalism
- Whistleblowere - https://www.veron.dk/
- Studerende der undersøge terror, google: ISIS =¿ ekstremist
- LGBT rettigheder - du risikerer at dø!
- Journalister overalt i verden, Tyrkiet

Der er mange situationer som fordrer mere anonymitet, uden at man nødvendigvis ”har noget at skjule” eller er kriminel

Brug Tor https://www.torproject.org/ en mere anonym browser

Kryptering hjælper dog ikke alle vegne

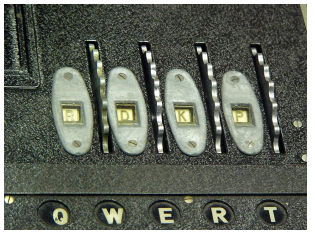


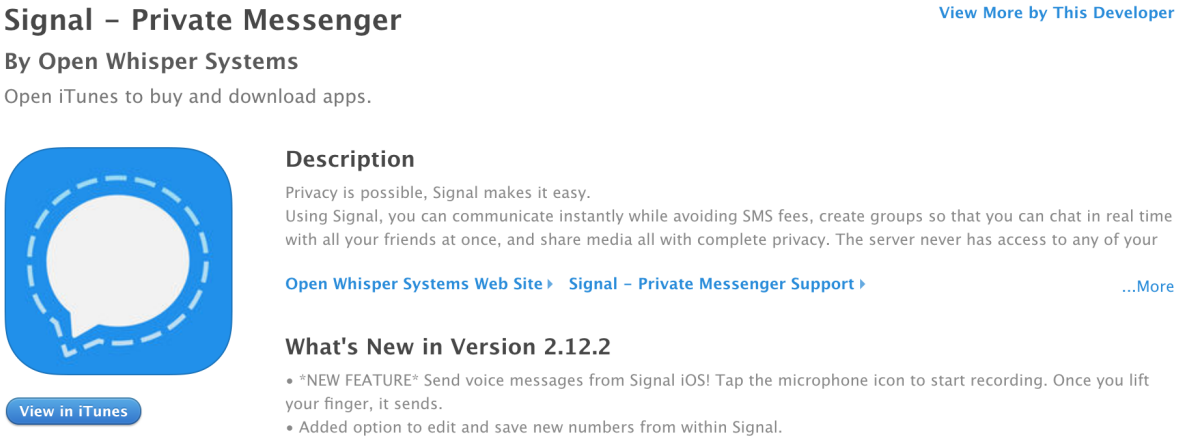
Digitale valghandlinger med kompleks kryptografi, fejlbehæftede stemmemaskiner, dyrt og ubrugeligt - sorry. Vi har et godt beskrevet valgapparat som alle kan forstå, som tillader genoptælling.

Specielt med den seneste udvikling - Rusland der måske influerer valg, drop hellere ideen nu!

IT og teknologi er ikke magisk, der er grænser for hvor det finder anvendelse

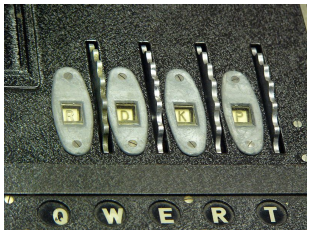
Signal iPhone App Store





- Texting with regular SMS is not private
- You have something to hide, it's called privacy
- You like to send your partner interesting messages
- You are taking pictures intended for a single recipient
- You need to send someone a password (initial pw of course, change immediately)

Signal Android Google Play Store



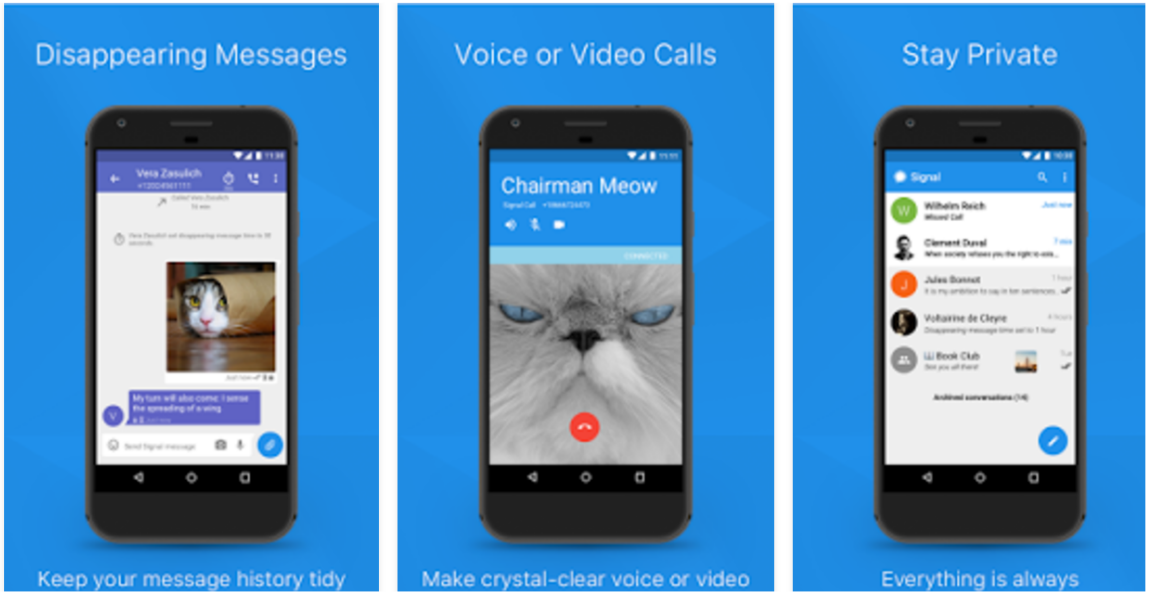
Signal Private Messenger

Open Whisper Systems **Communication** ★★★★½ 139,927

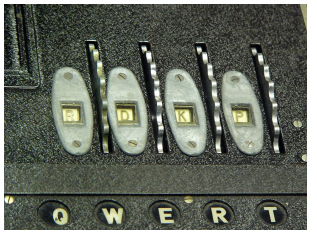
PEGI 3

This app is compatible with all of your devices.

Add to Wishlist **Install**



Jeres opgave

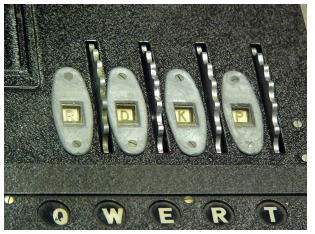


Installer signal - Whisper Systems Signal, findes til iPhone og Android

Brug en nyere mobiltelefon, fuld krypteret telefon beskytter jeres data

Slå fuld disk kryptering til på laptoppen. Det gør Folketinget allerede, MED en supernøgle som IT-afdelingen kan bruge hvis du glemmer koden :-)

Comments and questions

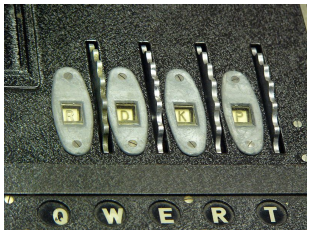


You are always welcome to send me questions later via email

Henrik Lund Kramshøj hlk@kramse.org

Twitter: @kramse Phone: 2026 6000

Kilder og henvisninger



Vi når ikke alt, så derfor er der lidt links til inspiration

- https://en.wikipedia.org/wiki/Nothing_to_hide_argument
- https://www.schneier.com/ Bruce Schneier kryptering, terror og sikkerhed generelt
- https://en.wikipedia.org/wiki/LGBT
- https://www.information.dk/information.dk/overv%C3%A5gning
  SERIE Overvågning: Made in Denmark
- https://tails.boum.org/ USB baseret operativsystem, indeholder Tor
- https://www.torproject.org/ Tor en mere anonym browser m.m.
- https://en.wikipedia.org/wiki/Data_at_rest
  https://en.wikipedia.org/wiki/Data_in_transit