

Kryptografiopgaver bilag

Historisk kryptografi

1. Caesar ROT

Jeg har klartekst: Hej jeg hedder alperen

Kryptotekst: urw wrt urqqre nycrera

Algoritme: ROT-13

Modtaget fra min medstuderende: Alend

Kryptotekst: Urw wrt urqqre Nyraq

Klartekst: hej jeg hedder Alend

fra mig: til Alend

The screenshot shows the Cryptool software interface. On the left, under 'Recipe', there is a green box labeled 'ROT13' with several checkboxes: 'Rotate lower case chars' (checked), 'Rotate upper case chars' (checked), and 'Rotate numbers' (unchecked). Below these checkboxes is a 'Amount' field set to '13'. In the center, the 'Input' section contains the text 'hej jeg hedder alperen'. At the bottom of the input section, there are file operation icons. The 'Output' section shows the encrypted text 'urw wrt urqqre nycrera'. At the bottom of the output section, there are file operation icons. The top of the window has a toolbar with various icons.

fra medstuderende Alend

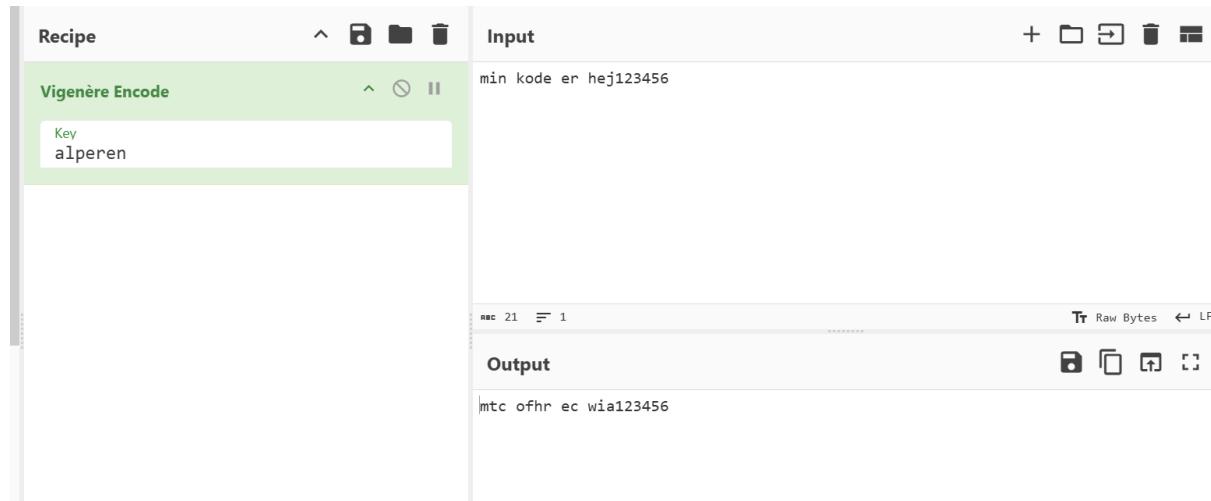
The screenshot shows the Cryptool software interface. On the left, under 'Recipe', there is a green box labeled 'ROT13' with several checkboxes: 'Rotate lower case chars' (checked), 'Rotate upper case chars' (checked), and 'Rotate numbers' (unchecked). Below these checkboxes is a 'Amount' field set to '13'. In the center, the 'Input' section contains the text 'Urw wrt urqqre Nyraq'. At the bottom of the input section, there are file operation icons. The 'Output' section shows the decrypted text 'Hej jeg hedder Alend'. At the bottom of the output section, there are file operation icons. The top of the window has a toolbar with various icons. A message at the top of the window says 'Last build: A month ago - Version 10 is here! Read about the new features here'.

2. Vigenére

Fra mig til alend

Min key: alperen

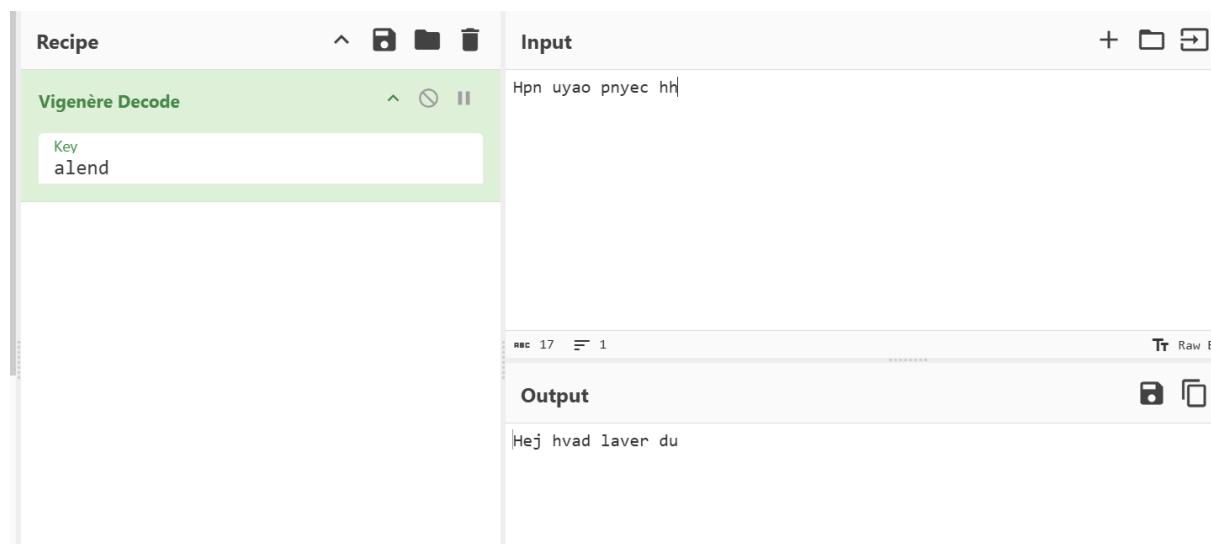
Output: mtc ofhr ec wia123456



Fra alend til mig

hans key: alend

Output: Hpn uyao pnyec hh



3. Steganografi

Vi gør brug af denne <https://stylesuxx.github.io/steganography/>



Hidden message

Steganografi (af græsk steganos, "dække", og gráphein, "at skrive") er et underemne inden for kryptologien, der beskæftiger sig med at skjule beskeder i en eller anden form for kontekst. Steganografi adskiller sig fra kryptering, da man ved kryptering forudsætter, at en opponent kender til beskedtransporten. Ved steganografi prøver man i stedet at

Input



dette er mit billede jeg sender til alend.



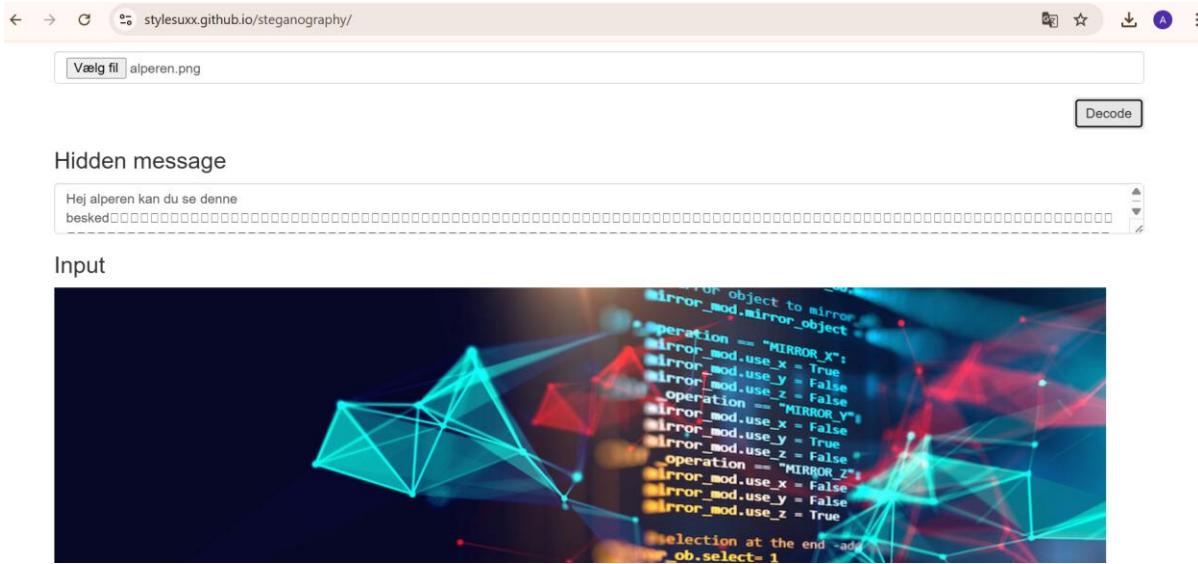
Binary representation of your message

0110100011001010110101000100000011000010110110001100101011011001100100

Original



dette er det jeg har modtaget fra alend som jeg har decryptet



Moderne kryptografi

1. Symmetrisk kryptering

Afprøv DES, Triple DES og AES i Cyberchef. Send en krypteret besked, og afkod den når modtaget.

DES

Fra mig til alend

Min key: zealandd

iv: zealandd

Output: 2a8c5b77bb15447c0a62ec8ac7c54f9efc25f92f8c96d37a

mangler screen

Fra alend til mig

hans key: Cykelhah

IV: Hjelmsdd

Output: 904ae99c3295b245

Last build: A month ago - Version 10 is here! Read about the new features [here](#)

Recipe ^

DES Decrypt ^

Key Cykelhah	UTF8 ▾
IV Hjelmsdd	UTF8 ▾
Mode CBC	
Input Hex	Output Raw

Input
904ae99c3295b245|

Output
Hej

Hex 16

TRIPLE DES

Triple Des:

Fra mig til alend

Key: Zealandersejduer

IV:Zealandd

OUtput: 3e7447f9011706a91635ff10e27f53ca00041514c0365fd1

Fra alend til mig

Key: Min hemmelig nøgle xddd

IV:cykelhah

OUtput: 1046f18a5072cdd9dc1edea46d68b0efba3866c3f7b5faae

Recipe

Triple DES Encrypt

Key: Zealandersejduer, UTF8

IV: Zealanddd, UTF8, Mode: CBC

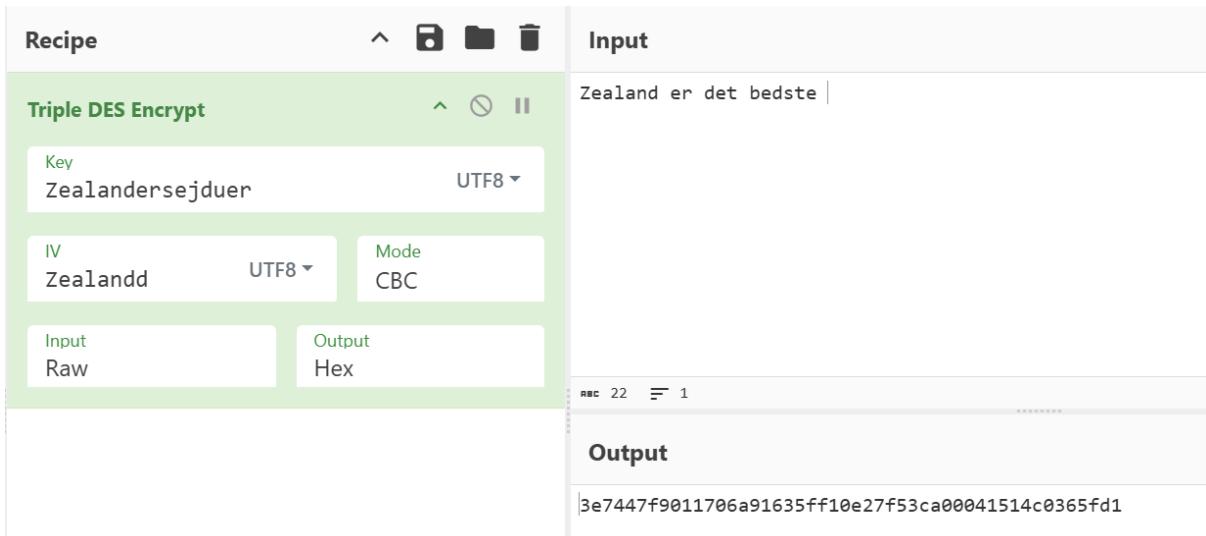
Input: Raw, Output: Hex

Input

Zealand er det bedste |

Output

3e7447f9011706a91635ff10e27f53ca00041514c0365fd1



Recipe

Triple DES Decrypt

Key: Min hemmelig nøgle xddd, UTF8

IV: cykelhah, UTF8, Mode: CBC

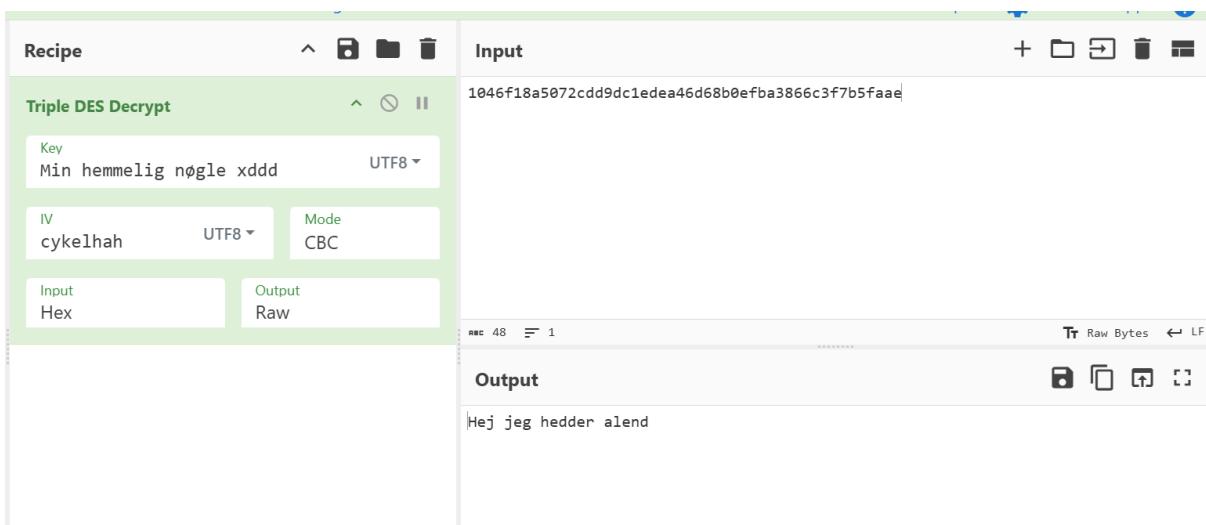
Input: Hex, Output: Raw

Input

1046f18a5072cdd9dc1edea46d68b0efba3866c3f7b5faae|

Output

Hej jeg hedder alend



AES

Fra mig til alend

Key: zealandersejhejd

IV zealandersejhejd

OUtput: 6ff8bde309b92a65cc17032796104bb78c419907f1641fea74a0070b12b9f45b

Recipe: AES Encrypt

Input: hej mit navn er alperen

Key: zealandersejhejd

IV: zealanderse... Mode: CBC

Output: Hex: 6ff8bde309b92a65cc17032796104bb78c419907f1641fea74a0070b12b9f45b

Fra alend til mig

Key: Cykelhjelmxxxxxx

IV:Dukenderikkkoden

OUtput: 0e61b8d203d77ae768d2774b9a77a0193d3d9b324b8fe591ae19b336ef6553d6

Recipe: AES Decrypt

Input: 0e61b8d203d77ae768d2774b9a77a0193d3d9b324b8fe591ae19b336ef6553d6

Key: Cykelhjelmxxxxxx

IV: Dukenderikkkoden Mode: CBC

Input: Hex: 0e61b8d203d77ae768d2774b9a77a0193d3d9b324b8fe591ae19b336ef6553d6

Output: Raw: Kan du læse min bsked XD

2. Asymmetrisk kryptering

Skab et sæt RSA nøgler (public & private) med [openssl](#) eller CyberChef

- a. RSA Encrypt din besked med din makkers public key, (Encode med Base64) og send til din makker. Makker skal Decode med Base64 og bagefter RSA Decrypt med sin private key.

```

-----BEGIN PUBLIC KEY-----
MIIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDWRMgjMTORB4coI/CZEDS4blym
CGkkfxFF+lpN2lsa4zf2PL4piGC2Q0//DJnQ+uoTGFY09ZPhgvuvsh54re62D0xM
m1joM5v0Idw1SohwK9H51r9HuHN04sbC1kR1AgktACTLwKFk5x8T7wrzMrU+/K01
ML0iaoDRXC172vf5QIDAQAB
-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDWRMgjMTORB4coI/CZEDS4blymCGkkfxFF+lpN2lsa4zf2PL4p
iGC2Q//DJnQ+uoTGFY09ZPhgvuvsh54re62D0xM1joM5v0Idw1SohwK9H51r9H
uHN04sbC1kR1AgktACTLwKFk5x8T7wrzMrU+/KQ1ML0iaoDRXC172vf5QIDAQAB
AoGADV5jQ1baicz3ch1NUeekndITo+tx7op4LzbD4p1rtIjZOCpek9bgEnb1lg
63oMSr707GYEIQjkHTU2036+qv4VNTTxLyGVyLDC8j7z+kzTEwqoUMEy6xEOnZ2
Dyj5Q2TsLHD7D7xwTsQ1f9Y53P9Ajuv519fQ8de50eEugIECQDr8C104hev27dx
Wo9dA1L7p7MYc5yC9nBzOoCQERq05D78U+K/DjkcNcLyiSRQYMc7iDEAmGv8CLof
KBUWhpJFAkEA6HzpACxVL5oLeFBQdgiN8uttR7j0Kwdf9zkyBCoMd4AP/7YDD9r
rtxYB1JJXE6hoZVghx1GF5Q5D9yM/qSnIQJBj0iziIGrRChz2Aod/LxzqBq/gvP
iuk/SgNPLAF1e+BIttag/ExLaH01zB9+387Dz0q0YMiowUQRqrhQ7Xm6FECQQCV
R4dQ3iaAnzgZPw5tcpVzx2X09NqL0nwLQUV1WQ6SOL+NIPNbko1y6Pb5FIQYakDs
gP7v1wPbpggrwDskUtMhAkAmI4G4nwlv2VL9LyHKfd02859EpLo8aoIPQZodprdy
y8LU3tPZmw6QAbjQ4Pk1L6CPO3YzKGHheR8UR11raXo
-----END RSA PRIVATE KEY-----

```

Ln 17, Col 65 | 1.160 tegn | 100% | Windows (CRLF) | UTF-8

Recipe	Input	Output
RSA Encrypt	alperen	<pre> -----BEGIN PUBLIC KEY----- MIIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDWRMgjMTORB4coI/CZEDS4blym CGkkfxFF+lpN2lsa4zf2PL4piGC2Q0//DJnQ+uoTGFY09ZPhgvuvsh54re62D0xM m1joM5v0Idw1SohwK9H51r9HuHN04sbC1kR1AgktACTLwKFk5x8T7wrzMrU+/K01 ML0iaoDRXC172vf5QIDAQAB -----END PUBLIC KEY-----</pre> <pre> -----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQDWRMgjMTORB4coI/CZEDS4blymCGkkfxFF+lpN2lsa4zf2PL4p iGC2Q//DJnQ+uoTGFY09ZPhgvuvsh54re62D0xM1joM5v0Idw1SohwK9H51r9H uHN04sbC1kR1AgktACTLwKFk5x8T7wrzMrU+/KQ1ML0iaoDRXC172vf5QIDAQAB AoGADV5jQ1baicz3ch1NUeekndITo+tx7op4LzbD4p1rtIjZOCpek9bgEnb1lg 63oMSr707GYEIQjkHTU2036+qv4VNTTxLyGVyLDC8j7z+kzTEwqoUMEy6xEOnZ2 Dyj5Q2TsLHD7D7xwTsQ1f9Y53P9Ajuv519fQ8de50eEugIECQDr8C104hev27dx Wo9dA1L7p7MYc5yC9nBzOoCQERq05D78U+K/DjkcNcLyiSRQYMc7iDEAmGv8CLof KBUWhpJFAkEA6HzpACxVL5oLeFBQdgiN8uttR7j0Kwdf9zkyBCoMd4AP/7YDD9r rtxYB1JJXE6hoZVghx1GF5Q5D9yM/qSnIQJBj0iziIGrRChz2Aod/LxzqBq/gvP iuk/SgNPLAF1e+BIttag/ExLaH01zB9+387Dz0q0YMiowUQRqrhQ7Xm6FECQQCV R4dQ3iaAnzgZPw5tcpVzx2X09NqL0nwLQUV1WQ6SOL+NIPNbko1y6Pb5FIQYakDs gP7v1wPbpggrwDskUtMhAkAmI4G4nwlv2VL9LyHKfd02859EpLo8aoIPQZodprdy y8LU3tPZmw6QAbjQ4Pk1L6CPO3YzKGHheR8UR11raXo -----END RSA PRIVATE KEY-----</pre>

The screenshot shows the Enigma software interface with the following details:

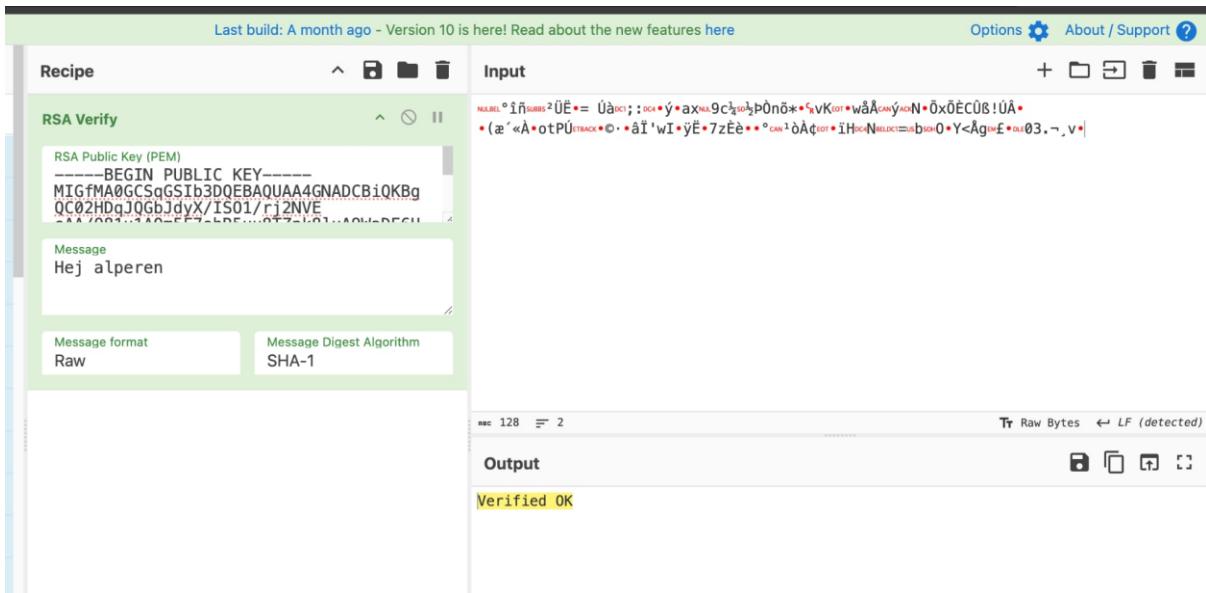
- Recipe:** RSA Decrypt
- Input:** A large block of encoded data (hex and ASCII representation) starting with "Mk...".
- Encryption Scheme:** RSA-OAEP
- Message Digest Algorithm:** SHA-1
- Output:** The decrypted message "hej jeg hedder alend".

rsa sign

The screenshot shows the Enigma software interface with the following details:

- Recipe:** RSA Sign
- Input:** The message "hejaland".
- Encryption Scheme:** RSA-OAEP
- Message Digest Algorithm:** SHA-1
- Output:** A large block of encoded data (hex and ASCII representation) starting with "qYKf...".

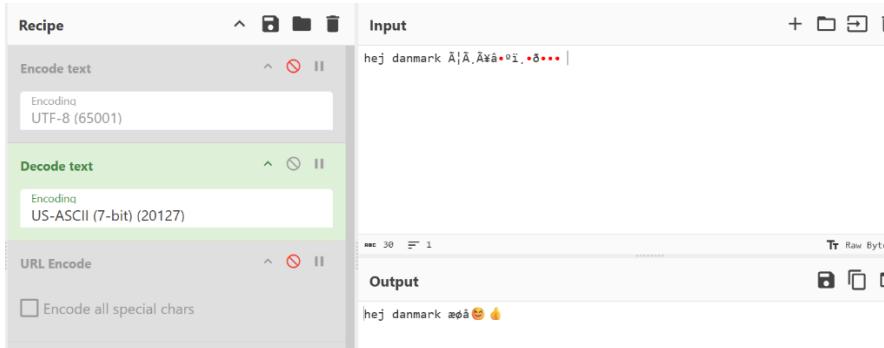
b. makker. Din makker skal *RSA Verify* med din public key.



jeg har rsa verify min makkers alends med hans public key.

3. Encoding

- Afprøv encoding på en dansk tekst, som indeholder ÆØÅ og emojis 😊 👍
- Prøv at konvertere UTF-8 til ASCII, og læg mærke til datatabet



Prøv URL Encode

The screenshot shows a software interface for URL encoding. On the left, there's a "Recipe" sidebar with sections for "Encode text" (using UTF-8 encoding), "Decode text" (using US-ASCII encoding), and "URL Encode". Under "URL Encode", there's a checkbox for "Encode all special chars". The main area is titled "Input" and contains the text "hej danmark æøå😊🔥". Below it is an "Output" section showing the encoded result: "hej%20danmark%20%C3%A6%C3%B8%C3%A5%20%98%BA%EF%20%9F%91%8D%20%0D%0A".

Prøv Base64 og Base32

This screenshot shows a software interface for encoding text into various formats. The "Recipe" sidebar includes "Decode text" (US-ASCII), "URL Encode" (disabled), "To Base32" (using an alphabet of A-Z2-7), and "To Base64" (using an alphabet of A-Za-z0-9+/=). The "Input" field contains the same text as the previous screenshot: "hej danmark æøå😊🔥". The "Output" section shows the Base64 encoded version: "aGVqIGRhbm1hcmmsgw6bDuM014pi677iP8J+RjSANCg==".

● 4. PGP

Afprøv også PGP i Cyberchef, hvor du krypterer og signerer en besked, og du dekrypterer og verificerer. (Du kan lave dine nøgler i cyberchef med PGP Generate Keypair.)

Først laver jeg mine nøgler med PGP Generate Keypair. Derefter kryptere jeg og signere en besked.

Her dekryptere og verificerer jeg beskeden.

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
MIIBIjANBQKHPYTxRtYEbpuyk3h
hvwhG07qcxv1lRJF6DRm804=
=7qCL
-----END PGP PUBLIC KEY BLOCK-----

-----BEGIN PGP PRIVATE KEY BLOCK-----
MIIBIjANBQKHPYTxRtYEbpuyk3h
hvwhG07qcxv1lRJF6DRm804=
=q7/A
-----END PGP PRIVATE KEY BLOCK-----

Private key password
hej123

```

Input

```

-----BEGIN PGP MESSAGE-----
scLe16evXMYHSS2f2w7GWL3thPRGiw5OsQDBDug37U0EVwf09fYQt4vTtjngS931
ND1EkZfaeazUzaSuvzA0U8vFXCk8qCIobCDi01f3tX9Y7vm6HmTond6LtA3bgNLA
TQFM2UCw2npmTHwsuMQkD+Go21mWgksrz6v5jphb7LosAJK8NhPWuiiaGqCGlw4
60jFLCkq3wQrdHSzN4kzHDD0zcr168Rw5eGgTIQjs01bf+2U+2mAazskQWQT8gT3
hkNUePOXhzJ/bSH0umInJC5hHz2ib2ZOpcaxhloHw3h1J65cqQqvfThguUV3CK6
exoWGoS8Um1GkfxtUr6039PlgfdBbh08Zj04ihC6ufcGsjeIk5rnD5mkZPKHP7LW
31pDgYYUhTXU7s6u8ypb68R0jzwlgJ15uv51s92yEFFcUDbTHd1xtwHc92T1hqEH
p05NEgauzIQRSgyoHtQmTghyA2IwrEk7wvMclm0F
=6Hg0
-----END PGP MESSAGE-----

```

Output

```

Signed by PGP key ID: 6B596268
PGP fingerprint: 9abaca32d22efcbc95d1d8317969b94b6b596268
Signed on Wed, 24 Sep 2025 12:30:47 GMT
-----
hej mit navn er alperen og jeg er dej

```

5. Hashing

Lav en kort besked, og beregn forskellige hashværdier af den (MD4, MD5, SHA1, SHA2, SHA3).

- b. Send dem til din makker.
- c. Din makker skal vha. hashværdien verificere, at beskeden er ægte.
- d. [Gentag evt. med at beregne hashen af en fil](#)

Beregning af hashværdier:

Recipe

- MD4
- MD5
- SHA1
 - Rounds: 80
- SHA2
 - Size: 512
 - Rounds: 160
- SHA3
 - Size: 512

Input

```

hej jeg er dej

```

Output

```

d5f73f37fc53913e695f4d92fc71baed16f7f92b3a1f2df7ebf0c147db2ec4b5a69531e8f34192557
d38652489320caa47db9d62ab52f8b780d4d923803887e7

```

Beregning af hash af en fil: bruger powershell.

```
Windows PowerShell

PS C:\Users\alper> Get-FileHash -Path "C:\Users\alper\Documents\hashingtest.txt" -Algorithm MD5
Algorithm      Hash                               Path
-----      ----
MD5          2514EBD26B8489510E5136DA49F4A2EE  C:\Users\alper\Documents\hash...

PS C:\Users\alper> Get-FileHash -Path "C:\Users\alper\Documents\hashingtest.txt" -Algorithm SHA1
Algorithm      Hash                               Path
-----      ----
SHA1         9A78C6B9F8EBA4BE72691287E94794D9D127F0A7  C:\Users\alper\Documents\hash...

PS C:\Users\alper> Get-FileHash -Path "C:\Users\alper\Documents\hashingtest.txt" -Algorithm SHA256
Algorithm      Hash                               Path
-----      ----
SHA256        EF61F52771BB875E25DBAE407C678AEFAC5311BF057E296247153D0C822289D7  C:\Users\alper\Documents\hash...

PS C:\Users\alper> Get-FileHash -Path "C:\Users\alper\Documents\hashingtest.txt" -Algorithm SHA512
Algorithm      Hash                               Path
-----      ----
SHA512        B1C10A5362274E9D427377D567B914F68BD96464222C840DE9A895635B7D507FFDD...  C:\Users\alper\Documents\hash...
```

6. Cracking med crackstation

Lav en svag hash af et simpelt, engelsk password. Din makker skal cracke hashen med [Crackstation](#). Snak om, hvordan “salt” kan ændre billedet.

The screenshot shows the CrackStation web application interface. At the top, there's a green header bar with the text "Last build: 3 months ago - Version 10 is here! Read about the new features [here](#)". To the right of the header are "Options" and "About / Support" links. The main interface has two main sections: "Recipe" on the left and "Input" on the right. In the "Recipe" section, there is a single item named "MD5". In the "Input" section, the password "admin1" is entered into the input field. Below the input field is a "Raw Bytes" section showing the hex dump of the hash: "e00cf25ad42683b3df678c61f42c6bda". There are also icons for file operations like copy, paste, and save.

CrackStation

CrackStation · Password Hashing Security · Defuse Security

Defuse.ca · Twitter

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e00cf25ad42683b3df678c61f42c6bda



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

e00cf25ad42683b3df678c61f42c6bda

Hash

Type

Result

md5 admin1

Recipe	Input	
MD5	password123	+
		Raw Bytes
	482c811da5d5b4bc6d497ffa98491e38	

CrackStation

CrackStation · Password Hashing Security · Defuse Security

Defuse.ca · Twitter

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

482c811da5d5b4bc6d497ffa98491e38



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

482c811da5d5b4bc6d497ffa98491e38

Hash

Type

Result

md5 password123

Color Codes: Exact match Partial match Not found

7. ECC Elliptic Curve Cryptography

Elliptic Curve Cryptography (EC eller ECC) er en anden moderne asymmetrisk krypto-algoritme ligesom RSA, og den kan yde samme sikkerhed med kortere nøgler. Desværre er der ikke kryptering og dekryptering med EC i CyberChef, men du kan prøve at generere en key-pair med Generate ECDSA keypair.

Sign en besked med ECDSA, og verificer samme besked. (Hvis det driller i CyberChef, prøv med <https://emn178.github.io/online-tools/ecdsa/verify/>)

Først har jeg genereret en key-pair med ec i Cyberchef.

```
-----BEGIN PUBLIC KEY-----  
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAECCtH7KmYTo51JTYut7eLBjrK4kZE  
H04yA88EjkTCY7WraCnBlgh+bHv0HaxXOFyLx8nhqtyLuJ3KE/OiS/nVGg==  
-----END PUBLIC KEY-----
```

```
-----  
W+LTZUWW4I1ACuOpewuM7TmPm  
-----  
ECDSA Private Key (PEM)  
qHfVDGMBRLR2USm0s7L+BzuEGTo3ULrN0pjC  
FZQMINRuNpW0ZZWt0043  
-----END PRIVATE KEY-----  
IVATE KEY-----
```

Message Digest Algorithm: SHA-256 Output Format: ASN.1 HEX

Output:

```
304502210095ee6a505f8  
ecd2cc79c6ac261001e19
```

nu signerer jeg beskeden.

jeg verificerer beskeden, output er som følgende verified ok.

8. Hashcat

Jeg har gennemført en øvelse i brute-force cracking af MD4-hashes med Hashcat. Først genererede jeg MD4-hashes af passwords med 3–7 bogstaver i CyberChef og gemte dem i en fil.

```
(kali㉿kali)-[~/Desktop]
$ hashcat -D 1 -O -m 900 -a 3 hashes.txt '?l?l?l?l?l?l?' --increment --increment-min=3 --increment-max=7

hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-sandybridge-12th Gen Intel(R) Core(TM) i5-1235U, 1435/2934 MB (512 MB allocatable), 4MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 55
Hashes: 5 digests, 5 unique digests, 1 unique salts
```

Jeg har brugt denne kommando: hashcat -D 1 -O -m 900 -a 3 hashes.txt '?l?l?l?l?l?l?' --increment --increment-min=3 --increment-max=7

og efter har jeg brugt denne kommando til at tjekke, hvilke hashes der var knækket:

```
cat /home/kali/.local/share/hashcat/hashcat.potfile
```

```
(kali㉿kali)-[~/Desktop]
$ cat /home/kali/.local/share/hashcat/hashcat.potfile
7da57b69cc4d05ccfc1cb3758c999973:alp1
9e68e57d46dcaad88ea688335a7fd7ff:alp
643a76b9441b7d65c9f5686eb97236ea:alper
95f640b5aef2492fc7aadcf8c247bd7e:alpere
d74cf1517f3fa737d5552c8d5693693c:alperen
```

9. Crack et passwordbeskyttet zip-fil

Efterprøv [denne øvelse](#) i Kali, hvor du laver en passwordbeskyttet zip-fil, og du cracker den bagefter.

Jeg har i denne øvelse i Kali, lavet en passwordbeskyttet zip-fil, og cracket den med fcrackzip.

```
(kali㉿kali)-[~/6.10]
$ mkdir 6.10; cd 6.10; touch one two three; zip -e numbers.zip one two three
Enter password:
Verify password:
adding: one (stored 0%)
adding: two (stored 0%)
adding: three (stored 0%)
```

```
(kali㉿kali)-[~/6.10/6.10]
$ ls /usr/share/wordlists/
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
(kali㉿kali)-[~/6.10/6.10]
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

(kali㉿kali)-[~/6.10/6.10]
$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt numbers.zip

PASSWORD FOUND!!!!: pw = password
```

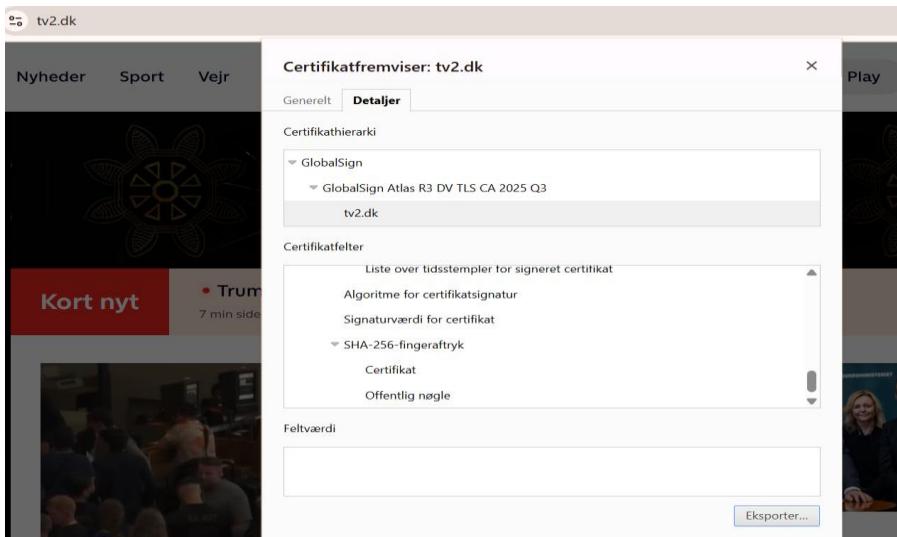
Resultat er således at, password er fundet, som er = password. øvelsen er gennemført succesfuldt og jeg har formået at cracke en pass-beskyttet zip-fil.

Dette viser at svage adgangskoder nemt kan knækkes og afsløres med en brute force angreb.

Anvendt kryptografi

1. TLS certifikater i browsere

Jeg har besøgt tv2, her har jeg undersøgt hvilket certifikat den bruger, og tv2 anvender et TLS-certifikat for at sikre forbindelsen mellem brugerens browser og serveren.



Jeg har også eksporteret den, her er følgende oplysninger:

A screenshot of a certificate export interface. The main table shows the following fields and values:

Felt	Værdi
Serienummer	014c557689e28dba27517ff6d...
Signaturalgoritme	sha256RSA
Hashalgoritme for signatur	sha256
Udsteder	GlobalSign Atlas R3 DV TLS CA...
Gyldigt fra	19. september 2025 19:02:12
Gyldigt til	21. oktober 2026 19:02:11
Emne	tv2.dk
Offentlig nøgle	RSA (2048 Bits)

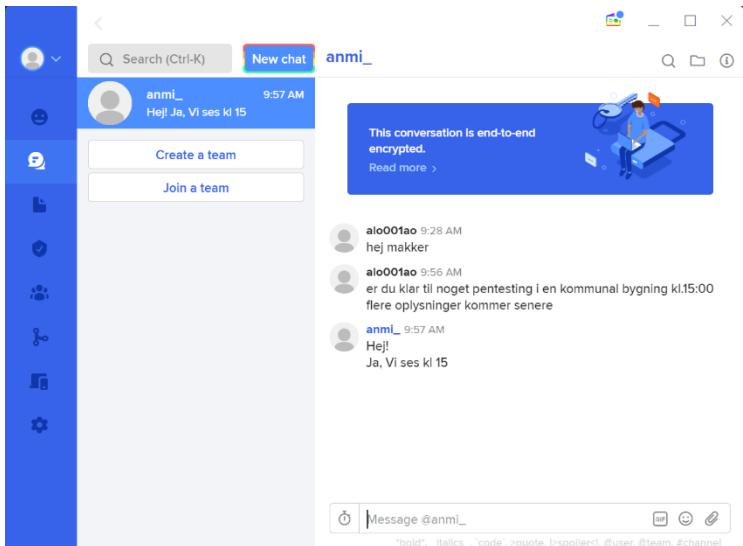
A sidebar on the right lists navigation items: 'Vis:' dropdown set to '<Alle>', 'Navn', 'I dag', 'tv2.d', and 'I går'.

Der er spændende informationer, som at certifikatet bruger RSA med sha256, som hashfunktion, samt hash algoritme er baseret på sha256.

2. Keybase.io

Afprøv Keybase.io til at sende sikre beskeder med. (Send til din makker, modtag fra din makker, signer en besked, og verificer en besked.)

(Ekstra: Kast et blik på [Keybase Book](#), hvor du kan lære om hvordan de sikrer informationsoverførsel.)

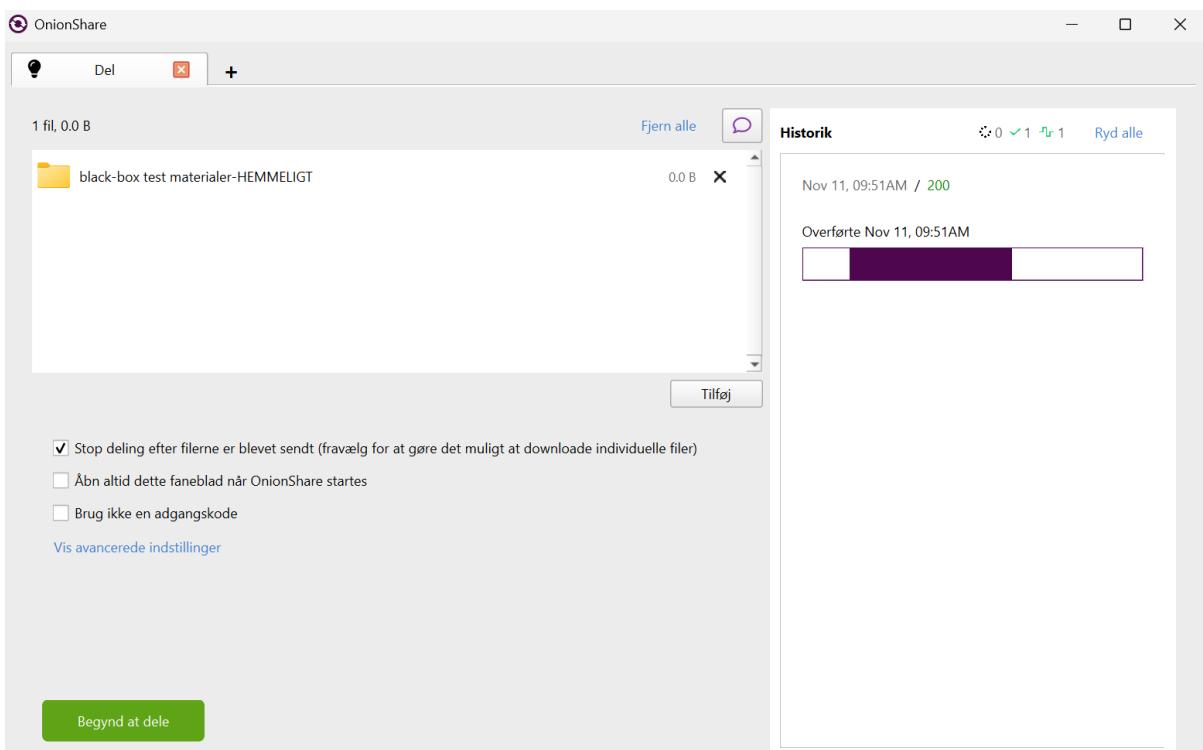


3. Onionshare

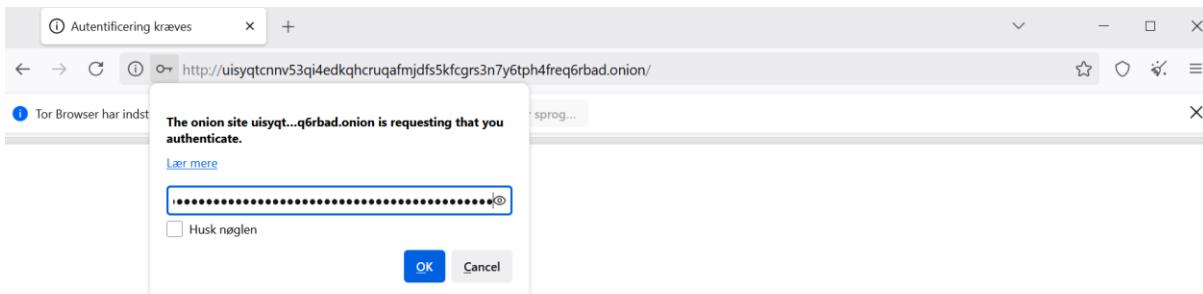
Send en fil til din makker sikkert med [OnionShare](#). Hvordan er det anderledes end Keybase?

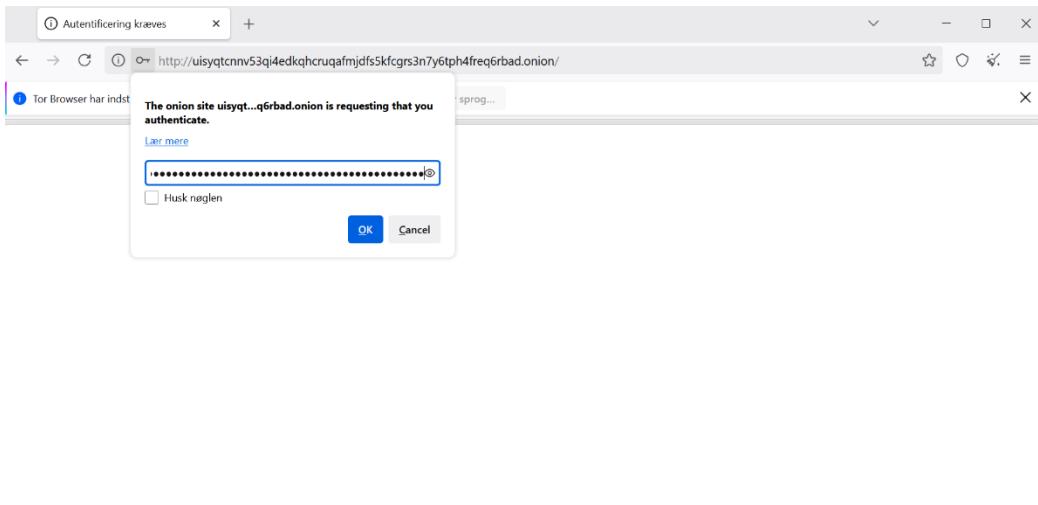
Sender en fil til min makker:

A screenshot of the OnionShare web interface. At the top, there are buttons for 'Del' (Delete) and '+'. Below this, it says '1 fil, 0.0 B'. A folder icon labeled 'black-box test materialer-HEMMEPLIT' is shown with a file size of '0.0 B'. At the bottom, there is a red button labeled 'Stop deling'. Below the button, text reads 'Alle med OnionShare-adressen kan downloade dine filer, med Tor Browser: ⓘ'. Underneath, it says 'Send først OnionShare-adressen herunder:' followed by a text input field containing the URL 'http://jiuljqak573c15znmi2xrhgquibxpzn66oykf5eho7rep5467tlrbsid.onion'. There are two buttons below the URL: 'Kopér adresse' and 'Vis QR-kode'. Further down, it says 'Send herefter den private nøgle for at give adgang til din OnionShare-tjeneste:' followed by a text input field containing a long string of asterisks ('*****'). Below this are three buttons: 'Kopér privat nøgle', 'Vis QR-kode', and 'Vis'.



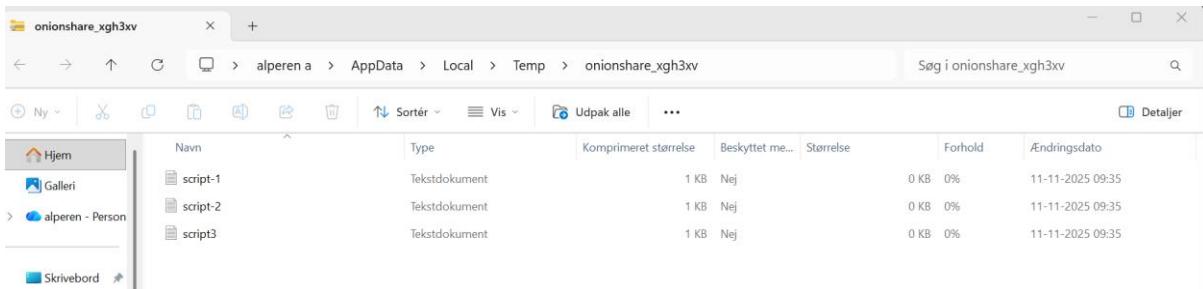
Modtager fil fra makker:





The screenshot shows an OnionShare interface with the URL <http://uisyqtcnv53qi4edkqhcruqafmjdfs5kfcgrs3n7y6tph4freq6rbad.onion/>. The page title is "OnionShare". It displays three files: "script-1.txt", "script-2.txt", and "script3.txt", all with a size of 0.0 B. A "Download Files" button is visible. The status bar at the bottom indicates "Total size: 326.0 B (compressed)".

The screenshot shows an OnionShare interface with the URL <http://uisyqtcnv53qi4edkqhcruqafmjdfs5kfcgrs3n7y6tph4freq6rbad.onion/>. The page title is "OnionShare". It displays three files: "script-1.txt", "script-2.txt", and "script3.txt", all with a size of 0.0 B. A "Download Files" button is visible. A modal dialog box is open, prompting the user to "Åbn onionshare_xgh3xv.zip". It shows the file path "...cnnv53qi4edkqhcruqafmjdfs5kfcgrs3n7y6tph4freq6rbad.onion". The question "Hvad skal Tor Browser gøre med denne fil?" has "Åbn med Windows Stifinder (standard)" selected. Other options include "Gem fil" and "Gør dette automatisk med filer som denne fremover". At the bottom are "OK" and "Annuller" buttons.



4. Pcrypt

Undersøg [Pcrypt](#), som er en lokal virksomhed, der tilbyder kryptografi. Måske en praktikplads?

Jeg har undersøgt Pcrypt, synes det er fedt, at der er en lokal dansk virksomhed, som tilbyder en passwordmanager, som gør at man kan få et overblik over alle ens logins og koder. Samt kryptering foretages på en lokal enhed med 256 bit standard AES og ECC.

Pcrypt skal jeg søge som praktikplads, da det er fedt med at man kan hjælpe virksomheder med sikre adgangskoder og opfylde kravene til datasikkerhed.

5. Open source key management

Find og afprøv et open source password-værktøj, som kan bruges til sikker opbevaring og deling af passwords og andre “secrets”.

Jeg har valgt Bitwarden.

Her fremvises, hvordan man opbevarer password eller andet hemmeligt sikkert:

The screenshot shows the Bitwarden Password Manager interface. On the left, there's a sidebar with navigation links like 'Bokse', 'Send', 'Værktøjer', 'Rapporter', 'Indstillinger', 'Password Manager', 'Share your passwords', and 'Secrets Manager'. The main area has a 'Komme i gang' (Getting Started) section with three steps: 'Opret en konto', 'Importér data' (with a note about importing data from other services), and 'Installér webbrowserudvidelser' (with a note about browser extensions). Below this is a 'FILTRE' (Filter) section with a search bar and dropdown menus for 'Alle bokse', 'Min boks', 'Ny organisation', 'Alle emner', and 'Favoritter'. A table lists saved items:

	Navn	Ejer	⋮
<input type="checkbox"/>	facebook test1	Mig	⋮
<input type="checkbox"/>	vmware ubuntu server: alperentechserver1 SHA256:tdv2FVJRQIUg5mZ/IWbQ4tkwSt+tn5w5v...	Mig	⋮
<input type="checkbox"/>	vmware windows server - server1 admin	Mig	⋮

En passwordmanager, som Bitwarden er noget jeg helt sikkert skal bruge i mit fremtidige arbejde indenfor it-sikkerhed, da man har med mange digitale identiteter og gøre med, desuden opbevarer man adgangskoder og andet hemmeligt sikkert, samt kan dele dem, den er også brugervenligt og beskytter digitale identiteter.

6. Kryptografi i din software

I denne opgave skal du undersøge, hvad Web Crypto API er for noget.

Jeg har besøgt <https://copilot.cloud.microsoft/> og spugt følgende:

Hvad er Web Crypto API, og hvad kan den bruges til? Forklar til en bachelorstuderende i it-sikkerhed

Copilot

Web Crypto API er en **indbygget JavaScript API** i moderne webbrowsere, som giver udviklere mulighed for at udføre **kryptografiske operationer** direkte i browseren — uden at skulle bruge eksterne biblioteker eller sende data til en server.

Her er en forklaring målrettet en bachelorstuderende i it-sikkerhed:

kan du give et eksempel på brug?

Copilot

Selvfølgelig! Her er et konkret eksempel på, hvordan du kan bruge Web Crypto API til at kryptere og dekryptere tekst med AES-GCM, som er en moderne og sikker symmetrisk krypteringsalgoritme.

🔒 Eksempel: Kryptering og dekryptering med AES-GCM

Jeg er blevet klogere på hvad Web Crypto API er og fået eksempel på brug, men synes ikke det er simpelt og gøre brug af, det kræver en vis viden om kryptografi.

7. Sikker e-mail?

I denne opgave skal du afprøve mulighederne for at sende sikker e-mail. Spørg copilot om:
Jeg har spurgt co-pilot følgende:

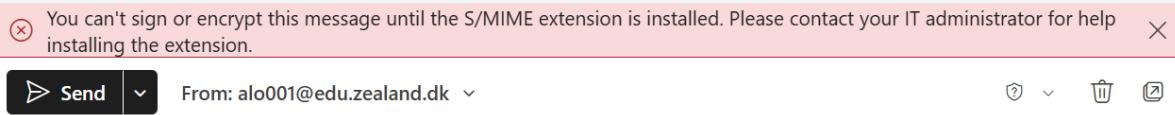
hvordan kan jeg sende sikker mail fra gmail (eller hotmail eller andet, erstat med din egen mailudbyder)
hvordan kan jeg sende sikker mail fra office 365 (din edumail på skolen)

Copilot

Her er en oversigt over, hvordan du kan sende sikker e-mail fra både Gmail (eller Hotmail/andre udbydere) og fra Office 365 (f.eks. din skolemail):

1. Send sikker mail fra Gmail (eller Hotmail/andre)

Jeg har prøvet at sende en sikker mail fra min skolemail, men får følgende besked:



S/MIME extension er ikke installeret. men jeg har valgt at bruge Protonmail i stedet for, til at sende en sikker mail til min makker. Som er meget nemt og enkelt at kryptere mails på.

sikker mail

Fra  alp.zea <alp.zea@proton.me>
Til Alendlsmail57@gmail.com

 Denne besked udløber tirsdag den 25. november 2025 kl. 10:46

Hej sender en sikker mail til dig, husk vores møde kl.13.00 idag.
med venlig hilsen
Alperen

Jeg har fået en forståelse for hvordan end-to-end kryptering fungerer i praksis. Så det kun er afsender og modtager, der kan læse mailen. Med dette sørger man også for at beskytte sit eget data eller indhold som beskeder, det er vigtigt især hvis man arbejder med it-sikkerhed.¹

8. Læs artiklen og beskriv det i 6 bullet points (no AI)

<https://samsik.dk/cybersikkerhed/temaer/overgangen-til-kvantesikker-kryptografi/>

Jeg har læst artiklen, og beskrevet det i 6 bullet points for neden, som giver mest mening, det har givet mig en læring oplevelse, at man selv sætter bullet points, som gør at man husker hvad man har læst og får en god viden om emnet.

1. Den nuværende trussel fra kvantecomputere

Kvantecomputere giver nye muligheder for at køre algoritmer, de traditionelle computere kan ikke løse de problemer som kvantecomputere kan. En af de algoritmer er Shors algoritme, der kan bryde de mest udbredte og moderne kryptografiske algoritmer, med en kvantecomputer. Den kan bryde nogle af de mest kendte, som RSA.

¹ <https://proton.me/security/end-to-end-encryption>

2. Indsamlnu – dekryptér senere:

Selvom kvantecomputere ikke findes, kan en fremtidige kvantecomputer udgør en trussel allerede nu, kan angriberne allerede via et angreb, indsamle krypteret data og dekryptere det i fremtiden, når teknologien er tilpas moden.

3. Identifikation og digital signatur

Kvantecomputere vil gøre det muligt at kunne forfalske digitale signaturer og identiteter, der er lavet med ikke kvante sikre kryptografiske algoritmer, en forudsætning er at der er tillid til at digitale signaturer, at de ikke kan forfalskes, en trussel kan være tillidsvækkende mod digitale systemer, som vi bruger i dag.

4. Ny kryptografi er på vej

Det amerikanske National Institute of Standards and Technology (NIST) står bag de fleste kryptografiske standarder, som anvendes i dag. For at man kan forhindre truslen fra kvantecomputere, har NIST i 2016 startet en konkurrence, som skulle finde algoritmer til en ny standard, der vil kunne modstå angreb fra kvantecomputere. NIST's nye standard, post-quantum cryptography (PQC), forventes klar i 2024, der vil blive den første kvantesikre kryptografi.

5. Hvad man kan gøre nu

Det forventes at nuværende kryptografiske algoritmer med tiden vil blive udskiftet med kvantesikker kryptografi. Standardiseringen af NIST PQC forventes afsluttet i 2024, opdatering bør sættes i drift. og systemer med følsom eller værdifuld data, er specifikke grunde til at idrøftsætte kvantesikker kryptografi, allerede nu. samt almindeligt anvendte systemer og software, samt eksisterende systemer, bør opdateres og opgraderes til kvantesikker kryptografi.

6. Mulige løsninger

Hybrid algoritme kan være en mulig løsning, således at man kombinerer dem korrekt. Den ene er en eksisterende standardiseret algoritme, som f.eks. RSA, som er afprøvet, men sårbar for at blive brutt af en kvantecomputer, samt en kvantesikker algoritme, der potentelt er sårbar, da den er ny, men sandsynligvis modstå angreb fra en kvantecomputer. Resultat ved at kombinere dem korrekt er krypteringen både sikker nu og ved angreb med en kvantecomputer, ulempene kan være flere ressourcer og øget kompleksitet forøger sandsynligheden for fejl, dette kan udgøre en sikkerhedsrisiko.²

² <https://samsik.dk/cybersikkerhed/temaer/overgangen-til-kvantesikker-kryptografi/>