

Kryptografiopgaver

| | |
|---------------------------------------|-----------|
| Historisk kryptografi | 1 |
| 1. Caesar ROT | 1 |
| Fra Mig til Medstuderende | 2 |
| 2. Vigenére | 3 |
| 3. Steganografi | 4 |
| 4. (Ekstraopgave) Enigma og Bomba | 6 |
| Moderne kryptografi | 7 |
| 1. Symmetrisk kryptering | 7 |
| 2. Asymmetrisk kryptering | 11 |
| 3. Encoding | 15 |
| 4. PGP | 18 |
| 5. Hashing | 19 |
| 6. Cracking med crackstation | 23 |
| 7. ECC Elliptic Curve Cryptography | 24 |
| 8. Hashcat | 26 |
| 9. Crack et passwordbeskyttet zip-fil | 27 |
| Anvendt kryptografi | 28 |
| 1. TLS certifikater i browsere | 28 |
| 2. Keybase.io | 29 |
| 3. Onionshare | 29 |
| 4. Pcrypt | 31 |
| 5. Open source key management | 32 |
| 6. Kryptografi i din software | 32 |
| 7. Sikker e-mail? | 33 |

Historisk kryptografi

1. Caesar ROT

Afprøv Caesar (ROT) i [Cyberchef](#) med makker. Send en krypteret besked til din makker, og modtageren skal dekryptere. Prøv også at rotere med 13

løsning

Jeg har klartekst: Hej jeg hedder Alend

Alend Nezar Mustafa Ismail

Kryptotekst: Urw wrt urqqre Nyraq

Algoritme: ROT-13

Modtaget fra min medstuderende: Alperen

Kryptotekst: urw wrt urqqre nycrera

Klartekst: hej jeg hedder alperen

Fra Mig til Medstuderende

The screenshot shows a software interface for encrypting text using the ROT-13 algorithm. On the left, under 'Recipe', 'ROT13' is selected. Under 'Input', the text 'Hej jeg hedder Alend' is entered. Under 'Output', the encrypted text 'Urw wrt urqqre Nyraq' is displayed. The 'Amount' field is set to 13. Various checkboxes for character rotation are checked: 'Rotate lower case chars', 'Rotate upper case chars', and 'Rotate numbers'. There are also icons for file operations like '+' (New), '-' (Delete), and folder navigation.

Fra Medstuderende til mig

The screenshot shows a software interface for decrypting text using the ROT-13 algorithm. On the left, under 'Recipe', 'ROT13' is selected. Under 'Input', the encrypted text 'urw wrt urqqre nycrera' is entered. Under 'Output', the decrypted text 'hej jeg hedder alperen' is displayed. The 'Amount' field is set to 13. Various checkboxes for character rotation are checked: 'Rotate lower case chars', 'Rotate upper case chars', and 'Rotate numbers'. There are also icons for file operations like '+' (New), '-' (Delete), and folder navigation.

2. Vigenére

Afprøv Vigenére i Cyberchef med makker. Send den krypterede besked, og modtager skal dekryptere.

Fra mig til medstuderende.

Min key: alend

Output: Hpн uyaо pnyec hh

The screenshot shows the CyberChef interface with a 'Vigenère Encode' recipe selected. The 'Input' field contains the message 'Hej hvad laver du'. The 'Key' field is set to 'alend'. The 'Output' field displays the encrypted message 'Hpн uyaо pnyec hh'.

Fra medstuderende til mig

Hans key: alperen

Output: mtc ofhr ec wia123456

The screenshot shows the CyberChef interface with a 'Vigenère Decode' recipe selected. The 'Input' field contains the encrypted message 'mtc ofhr ec wia123456'. The 'Key' field is set to 'alperen'. The 'Output' field displays the decrypted message 'min kode er hej123456'.

3. Steganografi

Steganografi: Find beskeden i det kattebillede, som du kan finde på dette link:

<https://gist.github.com/andracs/c2b6a7ae6efb179043b6728e312222ac>

Steganography Online

Encode Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

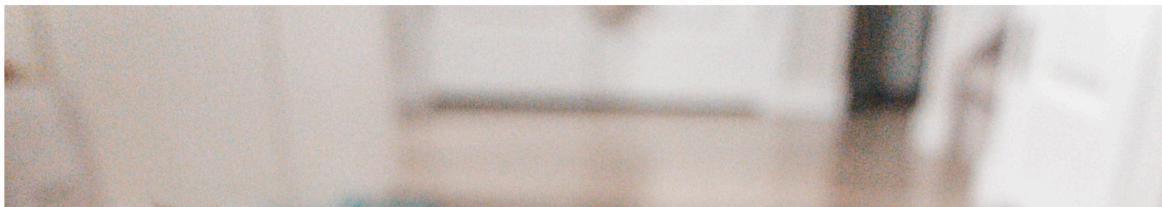
Vælg fil 162002597-5e9c2b73-2e73-47e2-8b4d-5c49aa1dcc97 (1).png

Decode

Hidden message

Steganografi (af græsk steganos, "dækket", 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 skjule,

Input



Skjul en besked i et billedfil. Byt filen med makker, og i skal finde den skjulte besked i hinandens billeder.

Mit billede til medstuderende.

Steganography Online

Encode

Decode

Encode message

To encode a message into an image, choose the image you want to use, enter your text and hit the **Encode** button.

Save the last image, it will contain your hidden message.

Remember, the more text you want to hide, the larger the image has to be. In case you chose an image that is too small to hold your message you will be informed.

Neither the image nor the message you hide will be at any moment transmitted over the web, all the magic happens within your browser.

Vælg fil programming_on_screen-1100x600.jpg

Hej alperen! kan du se denne besked

Encode

Binary representation of your message

```
0100100001100101011010100010000011000010110110001110000011001010111001001100101011100010000001101011011000010110111000100000011001000111010  
100100000011100110110010100100000011001000110010001100101011011001101001010000001100010011001011100110110101101100101011001001110100100
```

Original



medstuderendes billede med skjult tekst til mig.

Steganography Online

Encode

Decode

Decode image

To decode a hidden message from an image, just choose an image and hit the **Decode** button.

Neither the image nor the message that has been hidden will be at any moment transmitted over the web, all the magic happens within your browser.

Vælg fil download.png

Decode

Hidden message

hej alend

Input



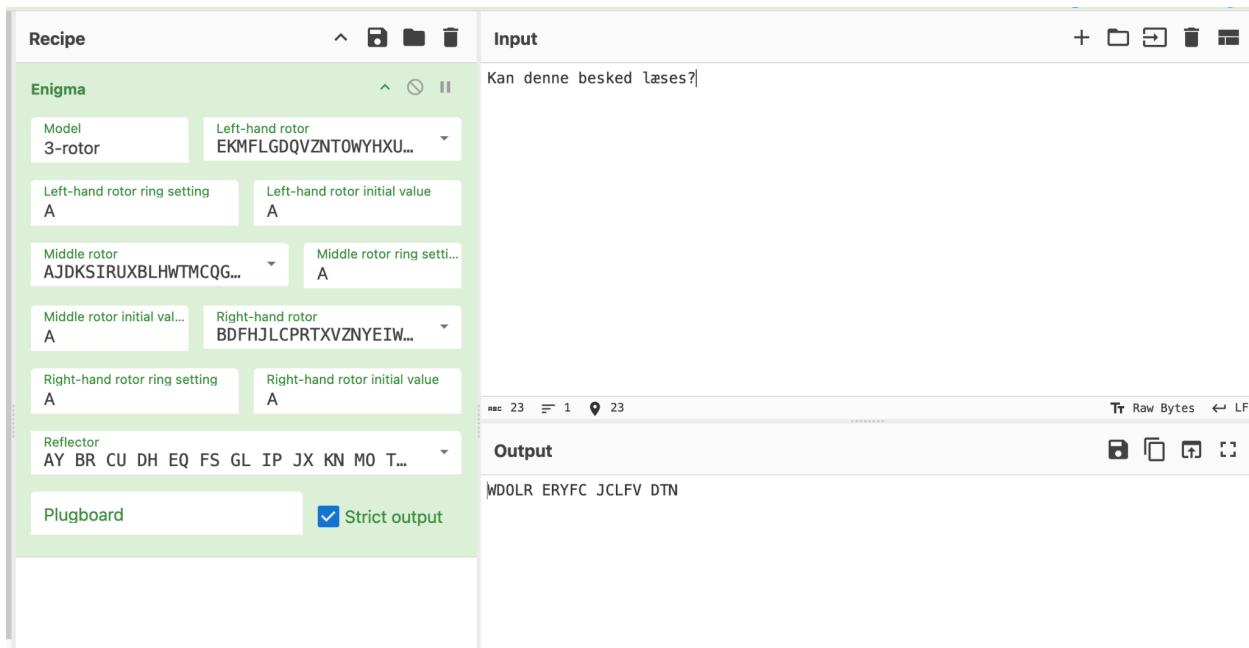
4. (Ekstraopgave) Enigma og Bomba

(Ekstraopgave) Afprøv Enigma i Cyberchef. Prøv at se, hvordan beskeden kan brydes med Bomba.

Enigma:

Input: Kan denne besked læses?

Output: WDOLR ERYFC JCLFV DTN



Bombe:

Input: WDOLR ERYFC JCLFV DTN

Output: Kandennebeskedlses?

Alend Nezar Mustafa Ismail

The screenshot shows the CyberChef interface with the 'Bombe' recipe selected. In the 'Input' section, the ciphertext 'WDOLR_ERYFC_JCLFV_DTN' is entered. The 'Output' section displays the decrypted message: 'Bombe run on menu with 0 loops (2+ desirable). Note: Rotor positions are listed left to right and start at the beginning of the crib, and ignore stepping and the ring setting. Some plugboard settings are determined. A decryption preview starting at the beginning of the crib and ignoring stepping is also provided.' Below this, a table provides 'Decryption preview' for various rotor stops:

| Rotor stops | Partial plugboard | Decryption preview |
|-------------|-------------------|------------------------|
| AAZ | ?? | IMIBURTXSZWRKPPWM |
| AAA | ?? | KANDENNEBESKEDLSES |
| AAB | ?? | GJNUTKTGGWYQYWOAIY |
| AAC | ?? | YLAINYDGDKSOVRKMGZ |
| AAD | ?? | EIKUTWXZBQKYXCWISB |
| AAE | ?? | QVNMGDCVJKOKABJCGUI |
| AAF | AW DQ OP | AAAWNLZOYUFWZRXUT |
| ΔΔC | ?? | ΩΙΙMPUTTI WΑΓCYMI C7NH |

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 medstuderende

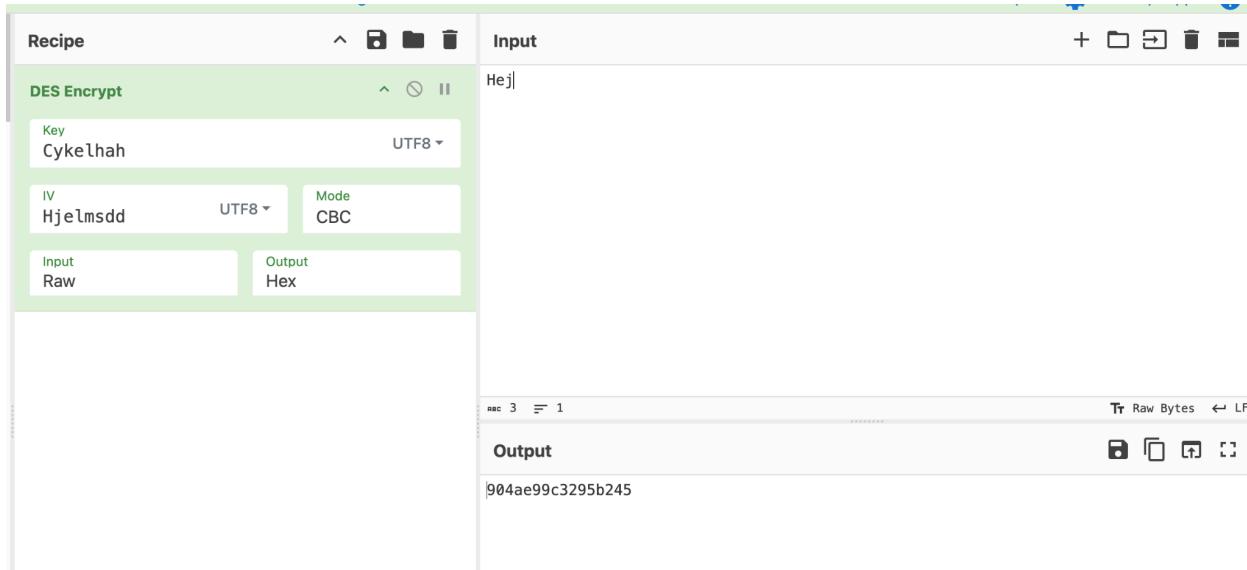
Key: Cykelhah

IV:Hjelmsdd

BEsked: Hej

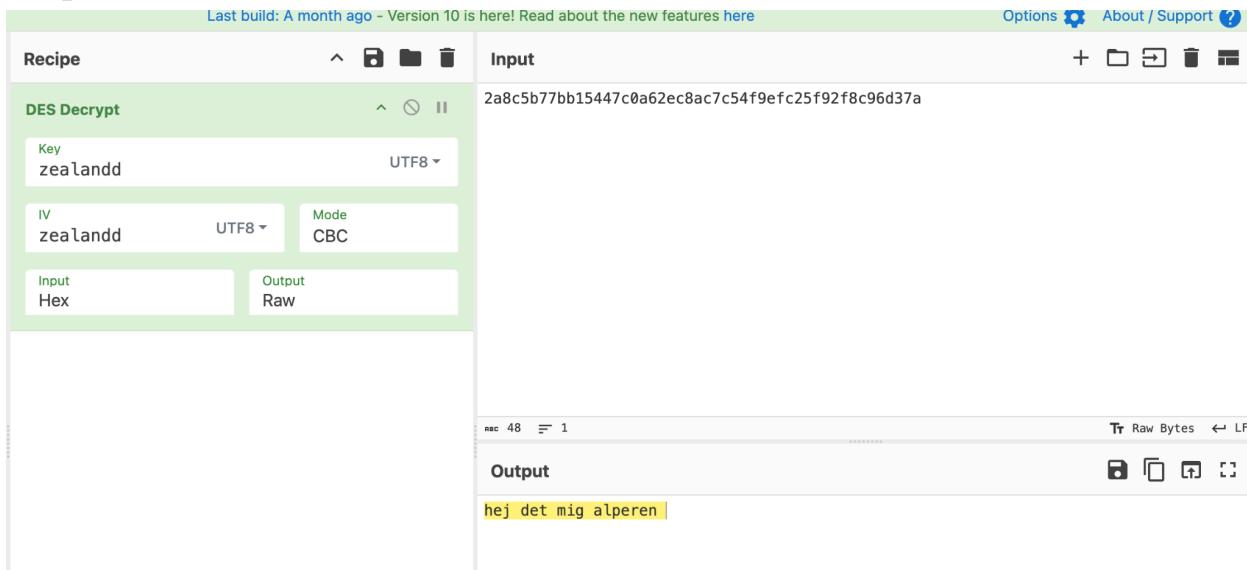
OUtput: 904ae99c3295b245

Alend Nezar Mustafa Ismail



Fra medstuderende til mig
hans key: zealandd
iv: zealandd

Output: 2a8c5b77bb15447c0a62ec8ac7c54f9efc25f92f8c96d37a



Triple Des:

Fra mig til medstuderende
Key: Min hemmelig nøgle xddd
IV:cykelhah
BEsked: Hej jeg hedder alend

Alend Nezar Mustafa Ismail

OOutput: 1046f18a5072cdd9dc1edea46d68b0efba3866c3f7b5faae

The screenshot shows the CryptTool application interface. In the 'Recipe' section, a 'Triple DES Encrypt' recipe is selected. It has a 'Key' field containing 'Min hemmelig nøgle xddd' and a 'Mode' field set to 'CBC'. The 'Input' section shows the text 'Hej jeg hedder alend'. The 'Output' section displays the encrypted hex output: '1046f18a5072cdd9dc1edea46d68b0efba3866c3f7b5faae'.

Fra medstuderende til mig

Key: Zealandersejduer

IV:Zealandd

OOutput: 3e7447f9011706a91635ff10e27f53ca00041514c0365fd1

The screenshot shows the CryptTool application interface. In the 'Recipe' section, a 'Triple DES Decrypt' recipe is selected. It has a 'Key' field containing 'Zealandersejduer' and a 'Mode' field set to 'CBC'. The 'Input' section shows the encrypted hex input: '3e7447f9011706a91635ff10e27f53ca00041514c0365fd1'. The 'Output' section displays the decrypted raw output: 'Zealand er det bedste'.

AES:

Fra mig til medstuderende

Key: Cykelhjelmxxxxxxxx

IV:Dukenderikkoden

Besked: Kan du læse min bsked XD

Alend Nezar Mustafa Ismail

OUpput:

0e61b8d203d77ae768d2774b9a77a0193d3d9b324b8fe591ae19b336ef6553d6

The screenshot shows the Cryptpad web interface. On the left, under 'Recipe', there is an 'AES Encrypt' recipe. It has a 'Key' field containing 'Cykelhjelmxxxxxx' and a 'Mode' field set to 'CBC'. The 'Input' field contains the text 'Kan du læse min bsked XD'. On the right, under 'Output', the encrypted hex output is shown: 0e61b8d203d77ae768d2774b9a77a0193d3d9b324b8fe591ae19b336ef6553d6.

Fra medstuderende til mig

Key: zealandersejhejd

IV zealandersejhejd

OUpput:

6ff8bde309b92a65cc17032796104bb78c419907f1641fea74a0070b12b9f45b

The screenshot shows the Cryptpad web interface. On the left, under 'Recipe', there is an 'AES Decrypt' recipe. It has a 'Key' field containing 'zealandersejhejd' and a 'Mode' field set to 'CBC'. The 'Input' field contains the hex value 6ff8bde309b92a65cc17032796104bb78c419907f1641fea74a0070b12b9f45b. On the right, under 'Output', the decrypted raw output is shown: hej mit navn er alperen.

2. Asymmetrisk kryptering

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

- a. RSA Encrypt din besked med din private key, send til din makker. Makker skal RSA Decrypt med din public key. Fra mig til alperen med hans public key

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

Options About / Support

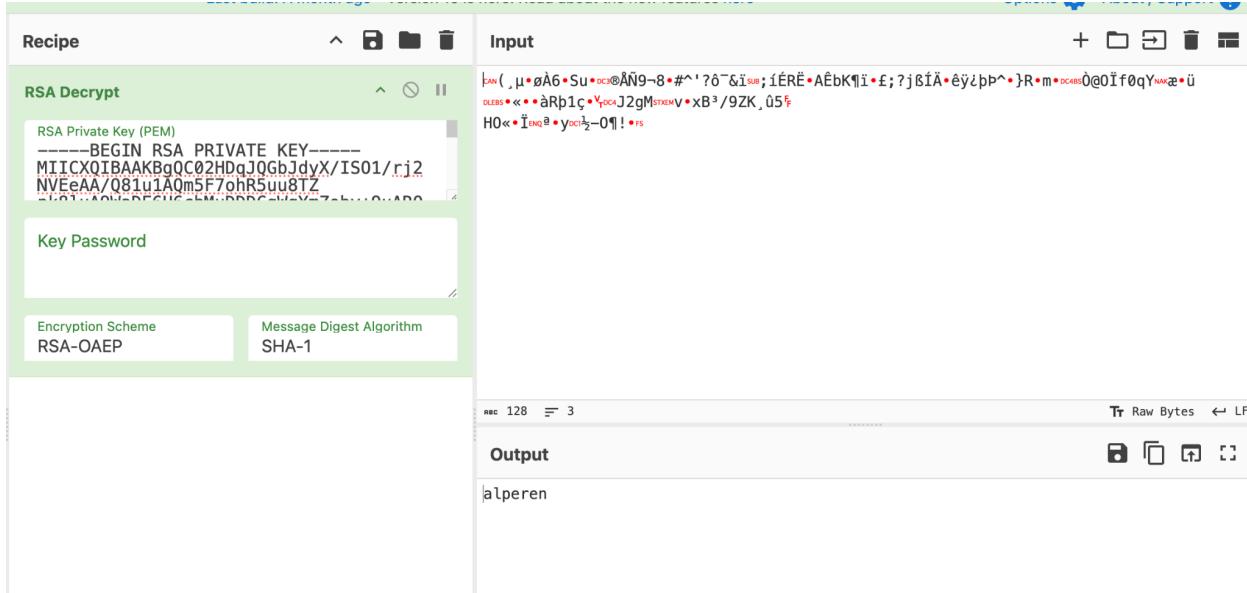
| Recipe | Input |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| RSA Encrypt | hej jeg hedder alend |
| <pre>-----BEGIN PUBLIC KEY-----\nMIICfQIBAAKCAQDwH5vAB7n5FZ0i\nio9TXG16kLe++LgwvSHA1ClQIU\nzr59VHy/tow8JPXWwQIDAQAB\n-----END PUBLIC KEY-----</pre> | |
| Encryption Scheme RSA-OAEP | Message Digest Algorithm SHA-1 |

Output

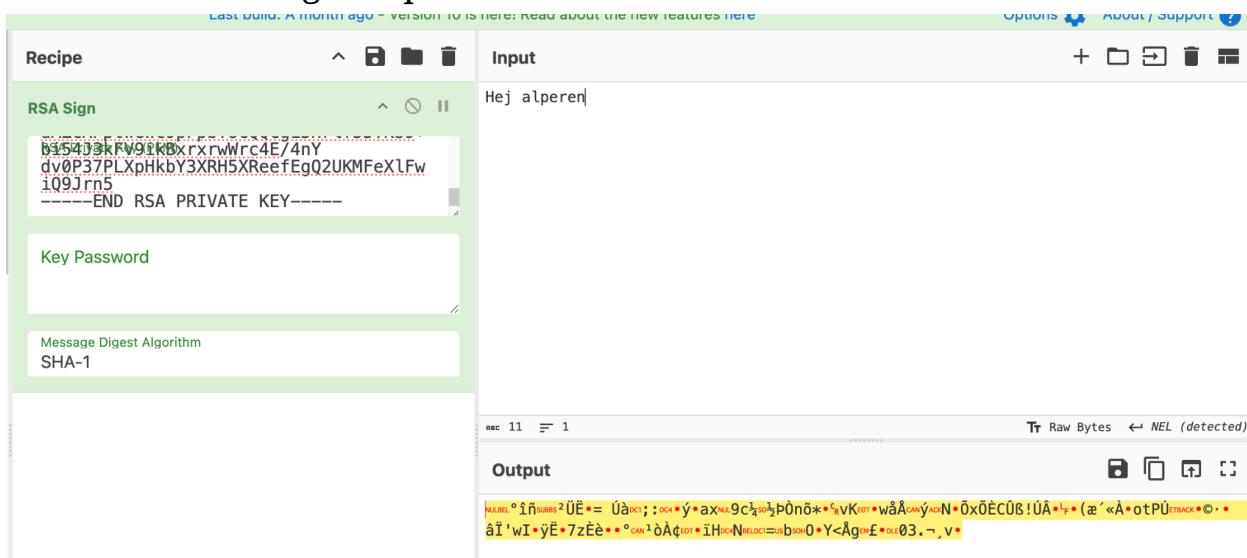
```
esc 20 = 1 Tr Raw Bytes ← ↻\nM«¹Ü\íö ÜSv, SREC ` • Y• ÈòòqméDHII•%?LÆ•½È] *BÒ>DÒ>Ab1§±uHK§>cÍó~X9ù~A@CAN>À5•ídÀäo¡T:p\n•ÙYUÑ•ÀaNA#=<1ñK#£K•y`•C[½•Cº•ÙaÚF•dcÅS ÈL., sub4
```

Alend Nezar Mustafa Ismail

Fra medstuderende til mig med min public key. Jeg bruger min privat key til at se beskeden.



- b. RSA Signer din besked med din makkers public key, send til din makker. Din makker skal RSA Verify med sin private key.
Fra mig til alperen



Fra medstuderende til mig

Alend Nezar Mustafa Ismail

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

Options About / Support

Recipe

RSA Verify

RSA Public Key (PEM)
-----BEGIN PUBLIC KEY-----
MIIFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg
QC7ZC/WhmQRyIM0cvwF2d9+36BF
-----END PUBLIC KEY-----

Message
hejaland

Message format: Raw | Message Digest Algorithm: SHA-1

Input

qYKfU'•••!•nP••SUB•t•CAN!•L}•TX,\$åg•ÄÖSTUSOCÄöy,ù•ER•Ü}•XBO4E•y=ydÅ•tpÅLMÜuµ"•NÄ}•Y•Ü«?•?)µc•G•ok)þ•bas•l•Ü•2•L•E•9}•n•st•Ä•s•E•á•i,••t•E•E•

Output

Raw Bytes LF (detected)

Raw 128 1

Verified OK

c. Spoiler alert: [Løsning hint a](#) - [Løsning hint b](#) - [Mulig løsning](#)

Alend Nezar Mustafa Ismail

MIN NØGLE

----BEGIN PUBLIC KEY----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC02HDqJQG
bJdyX/ISO1/rj2NVE
eAA/Q81u1AQm5F7ohR5uu8TZpk8luA9WaDE6U6cbMuDDDCq
WqYmZoby+9uARQEpL
NGnMnE5pwFzUwSeXNC SUarFQUxC5xOo4JrdZMGJ3a2dlK8tDii
ztdAWFlxAFTQje
4iullF3iXs261Ar6kQIDAQAB
----END PUBLIC KEY----

----BEGIN RSA PRIVATE KEY----

MIICXQIBAAKBgQC02HDqJQGbJdyX/ISO1/rj2NVEeAA/Q81u1AQ
m5F7ohR5uu8TZ
pk8luA9WaDE6U6cbMuDDDCqWqYmZoby+9uARQEpLNGnMnE
5pwFzUwSeXNC SUarFQ
UxC5xOo4JrdZMGJ3a2dlK8tDii ztdAWFlxAFTQje 4iullF3iXs261Ar
6kQIDAQAB
AoGAAiG0/wWNpcsF9SKsW1SvZ+Uj6mkxs400jDRikiTJ+5qqF6s
N8HTV5P9s6ttS
jTn0M81fOd1YWStJbG6sH2IglP5lAlnyGOF2DBjhSb5Dz0ic+SWu
ZeG1j2XO/Hnd
FwrhIL7/3zA7mqBCW0ZbhMUhYEtWssTPx6z/nwXHmnwZTwM
CQQDjPlH5tXh5LIPV
fB0WCU1mgSAH4KBzkBgvSEmohRJRJMrxqSbqcHfOjM7X5dUM
VbU0PLh+gBsGoP+r
ACVAiAnXAkEAy7sIUpTna+WKRiGhHcMjuANOY/XIMd9frlwUU
kPfKBcw0wObgeEO
Y1C9cPIUvQ0FiZTwCa5curVsGNxyduoh1wJARuUEciEZasRoi+7i
rCNO0Hsaki8
BhGoWef1guuxITuXTPl2uKFJ31iyloyOwQBkPd3LuTuCMvk7ij/L
X2yRIQJBALWI
8hCL6G5nOb/mJWecw04rfAVsM7fk36BBIkZvfgB+MZ5Ff6LKhs
QpE1pGHugh8eh
dAZcXPptwGWc9pFpbT8CQQCgi5Hrlf55YKs9+bi54J3kFV9ikBxr
xrwWrc4E/4nY
dv0P37PLXpHkbY3XRH5XReefEgQ2UKMFeXlFwiQ9Jrn5

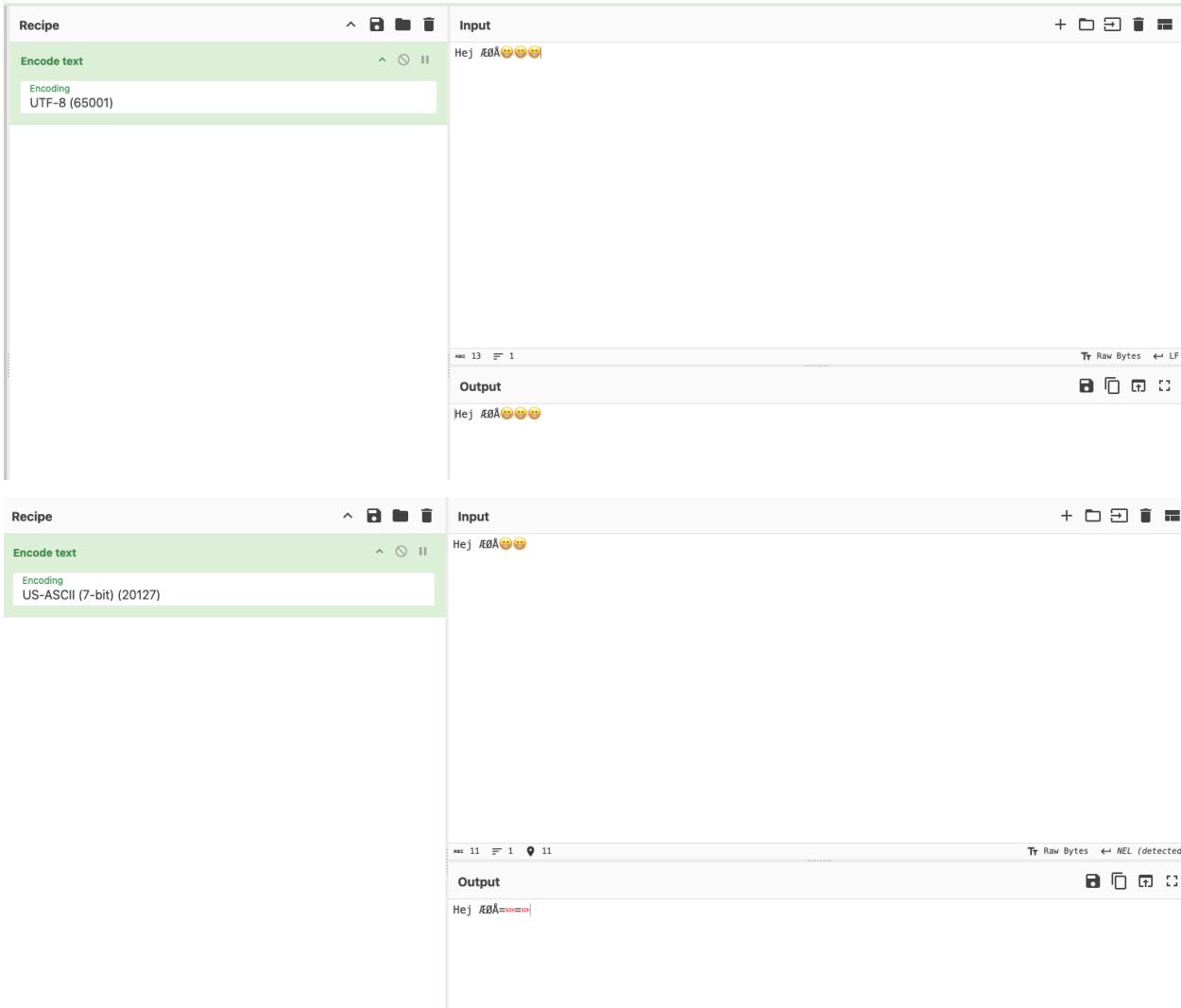
Alend Nezar Mustafa Ismail

-----END RSA PRIVATE KEY-----

3. Encoding

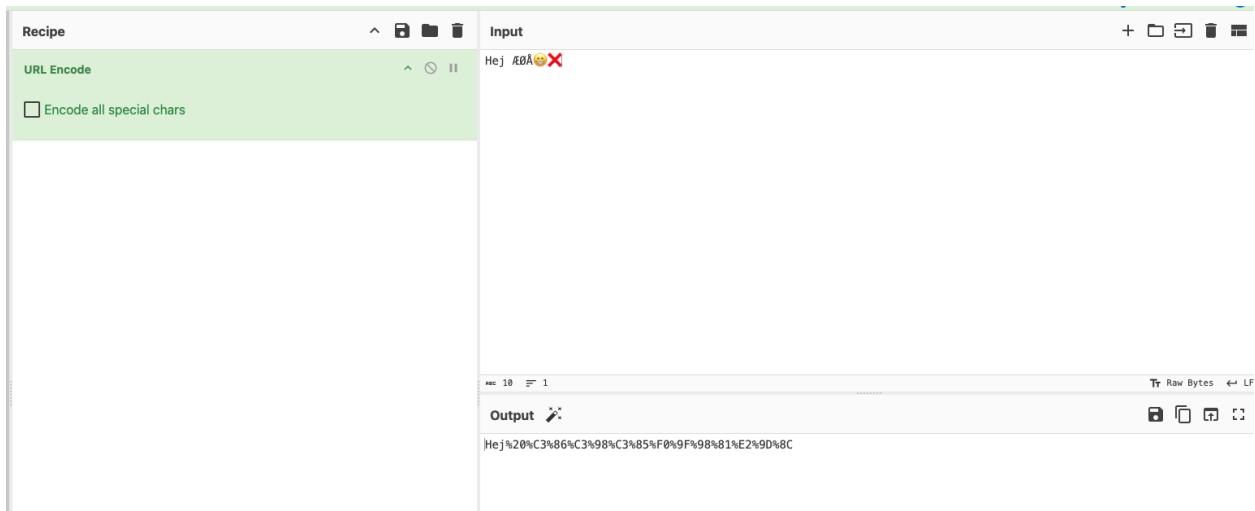
Afprøv encoding på en dansk tekst, som indeholder ÆØÅ og emojis 😊👍

Prøv at konvertere UTF-8 til ASCII, og læg mærke til datababet

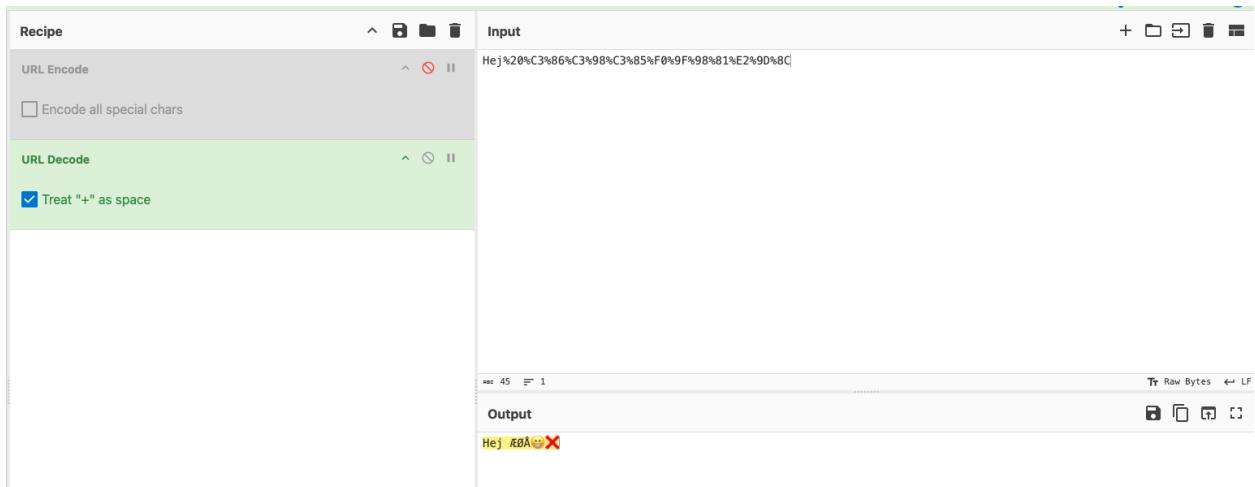


Alend Nezar Mustafa Ismail

URL Encode



URL decode



Base64:

Alend Nezar Mustafa Ismail

The image displays two side-by-side screenshots of a software application interface, likely a command-line tool or a web-based encoder/decoder.

Top Screenshot (Encoder):

- Recipe:** To Base64
- Input:** Hej ÅØÅ ☺✖
- Output:** SGVqIMOGw5jDhSDwn5iB4p2M

Bottom Screenshot (Decoder):

- Recipe:** To Base64
- Input:** SGVqIMOGw5jDhSDwn5iB4p2M
- From Base64:** Remove non-alphabet chars (checkbox checked)
- Output:** Hej ÅØÅ ☺✖

Base 32:

The screenshot shows two separate instances of the CyberChef interface demonstrating base32 encoding and decoding.

Top Instance (To Base32):

- Recipe:** To Base32
- Input:** Hej ÅØÅ 😊✖️
- Output:** JBSWUIGDQ3BZRQ4FEDYJ7GEB4KOYY==

Bottom Instance (From Base32):

- Recipe:** From Base32
- Input:** JBSWUIGDQ3BZRQ4FEDYJ7GEB4KOYY==
- Output:** Hej ÅØÅ 😊✖️

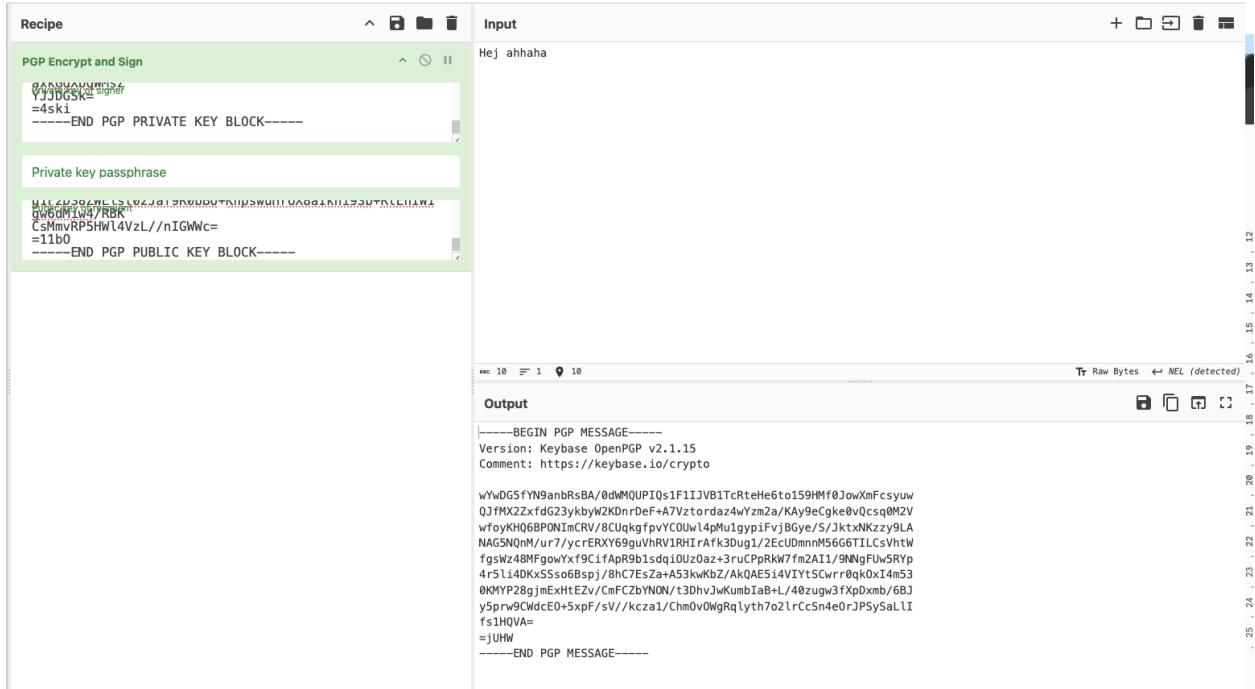
In the bottom instance, the "Remove non-alphabet chars" checkbox is checked.

4. PGP

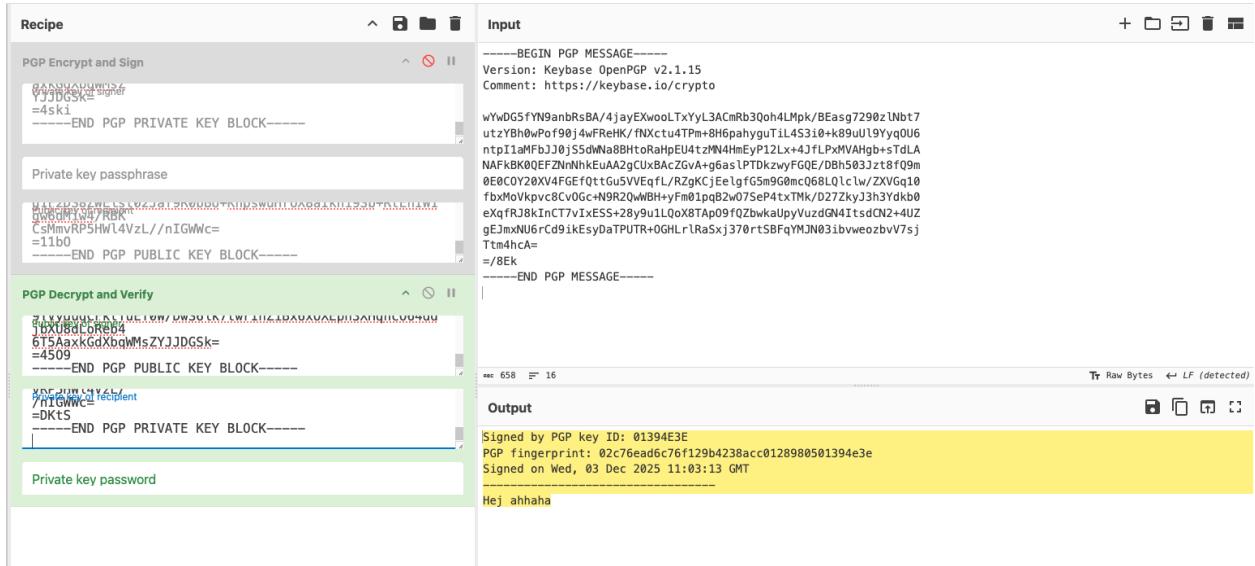
Afprøv også PGP i Cyberchef, hvor du krypterer og signerer en besked, og du dekrypterer og verificerer. (Du kan lave dine nøgler i cyberchef med PGP Generate Keypair.)

Alend Nezar Mustafa Ismail

PGP Encrypt and Sign



PGP Decrypt And verify



5. Hashing

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

d. Send dem til din makker.

The image displays two identical screenshots of a digital forensics or hashing application interface. Both screenshots show a 'Recipe' section on the left and an 'Input' and 'Output' section on the right.

Recipe:

- MD4
- MD5**
- SHA1
- SHA2
- SHA3

Input: Hej|

Output: 95c383ac224e259a5f5d08b4dab08cff

Recipe:

- MD4
- MD5
- SHA1**
- SHA2
- SHA3

Input: Hej|

Output: 7bcf82f95cf9662a995805b76b80006c65a79718

Alend Nezar Mustafa Ismail

The image consists of three vertically stacked screenshots of a password cracking application interface. Each screenshot shows a 'Recipe' sidebar on the left and an 'Input' field and 'Output' pane on the right.

- Screenshot 1:** The 'Recipe' sidebar lists MD4, MD5, SHA1, and SHA2. SHA2 is selected, with its 'Size' set to 512 and 'Rounds' set to 160. The 'Input' field contains 'Hej'. The 'Output' pane shows the hex output: `318bdecec2693e5122f6bd5b635308200406b933ba88f294079aefbd48d856a70341333369a04c10a137793fbf69e72bffa19548c30cc01094255a2ad7a751df`.
- Screenshot 2:** The 'Recipe' sidebar lists MD4, MD5, SHA1, and SHA3. SHA3 is selected, with its 'Size' set to 512. The 'Input' field contains 'Hej'. The 'Output' pane shows the hex output: `eec77aacde42aa83a37be1286fe3854dd03463ab62fe6f0b2f48f7c31ad5f55d97ba70d6c7b89e9181e38ca3eda1ac639f870c137537a7a57125aa18c535262`.
- Screenshot 3:** The 'Recipe' sidebar lists MD4, MD5, SHA1, SHA2, and SHA3. MD4 is selected, with its 'Rounds' set to 80. The 'Input' field contains 'Hej'. The 'Output' pane shows the hex output: `c816d61e71445ee2cf10b29342f9e16d`.

Alend Nezar Mustafa Ismail

Din makker skal vha. hashværdien verificere, at beskeden er ægte.

The screenshot shows a web application interface for MD5 encryption and decryption. At the top, there is a redacted input field containing the text "a58fc871f5f68e4146474ac1e2f07419". To the right of this is another redacted output field showing the result of the decryption: "a58fc871f5f68e4146474ac1e2f07419 : Hello". Below these fields are two dark blue buttons labeled "Encrypt" and "Decrypt".

Md5 Encrypt & Decrypt

This screenshot is similar to the one above, showing MD5 encryption and decryption. The input field contains "8b1a9953c4611296a827abf8c47804d7" and the output field shows "8b1a9953c4611296a827abf8c47804d7 : Hello". It includes a promotional banner for a monthly VPN service: "Monthly VPN For Only \$3.49 ! No long-term contract, cancel anytime !" with a cartoon character icon.

SHA1 Encrypt & Decrypt

This screenshot shows SHA1 encryption and decryption. The input field contains "f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0" and the output field shows "f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0 : Hello". It includes a promotional banner for a monthly VPN service: "Monthly VPN For Only \$3.49 ! No long-term contract, cancel anytime !" with a cartoon character icon.

This screenshot shows SHA1 encryption and decryption. The input field contains "3615f80c9d293ed7402687f94b22d58e529b8cc7916f8fac7fd df7fb5af4cf777d3d795a7a00a16bf7e7f3fb9561ee9baae48 Oda9fe7a18769e71886b03f315" and the output field shows "bf7e7f3fb9561ee9baae480da9fe7a18769e71886b03f315 : Hello". There is no promotional banner present in this version.

e. [Gentag evt. med at beregne hashen af en fil](#)

[2] CHOOSE YOUR HASH FUNCTION

| | |
|-----------------------------------------------------|----------------------------------------------|
| <input checked="" type="checkbox"/> > MD5 128-bit | <input type="checkbox"/> > SHA-1 160-bit |
| <input type="checkbox"/> > SHA-256 256-bit | <input type="checkbox"/> > SHA-384 384-bit |
| <input type="checkbox"/> > SHA-512 512-bit | <input type="checkbox"/> > BLAKE2b 512-bit |

[3] LAUNCH THE HASHING PROCESS

 [\[CALCULATE HASH\]](#)

OUTPUT: [COPY] [GENERATE REPORT]

ALGORITHM: **MD5**

HASH: **cc8fe4ead550dd63fcf8f6d028b46b03**

FILE: **Birthday.tsx** SIZE: **0.00 MB**

TIMESTAMP: **2025-12-03T12:10:41.477Z**

✓ Enjoying this free tool?

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.

Alend Nezar Mustafa Ismail

Fra mig til medstuderende.

The screenshot shows the Hashcat interface. At the top, it says "Last build: 4 months ago - Version 10 is here! Read about the new features [here](#)". On the right, there are "Options" and "About / Support" buttons. The main area has tabs for "Recipe" and "Input". Under "Input", the word "hello" is typed. Below that is an "Output" section containing the hash "5d41402abc4b2a76b9719d911017c592". There are also "Raw Bytes" and "LF (di)" buttons at the bottom of the output section.

Jeg skal cracke medstuderende kode.

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

48bb6e862e54f2a795ffc4e541caed4d



[Crack Hashes](#)

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

| Hash | Type | Result |
|----------------------------------|------|--------|
| 48bb6e862e54f2a795ffc4e541caed4d | md5 | easy |

Color Codes: Green: Exact match, Yellow: Partial match, Red: 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/>)

Alend Nezar Mustafa Ismail

Laver key pair

```
Generate ECDSA Key Pair
Elliptic Curve P-256 Output Format PEM

sec 0  ⌂ 1  Tr Raw Bytes ↵ LF (detected)
Output ✎
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAoYIKoZIzj0DAQcDQgAEgSIBGTmEjUE0ucdrwYKC5wIdztis
QXP/aA/zEDMoSWURwS3zDs/Sxxv1rHNK84s8fH3Vi+rkqZFZMy6ccK9iw==
-----END PUBLIC KEY-----

-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG0wawIBA0Qgy2746ngsdjpCKxOM
Kn3Ynz02G3vnBl0uJ3hWFxiTsh1ShRANCAASB1gEZOYNSNQ065x2vBgoLnAh302LB
c/9oD/M0MyhJZRHEJnf40z9LHG/Wsc0rzizyEfwdL6uSpkVlbLpxyT2L
-----END PRIVATE KEY-----
```

Jeg signer beskeden.

```
Recipe
Generate ECDSA Key Pair
Elliptic Curve P-256 Output Format PEM

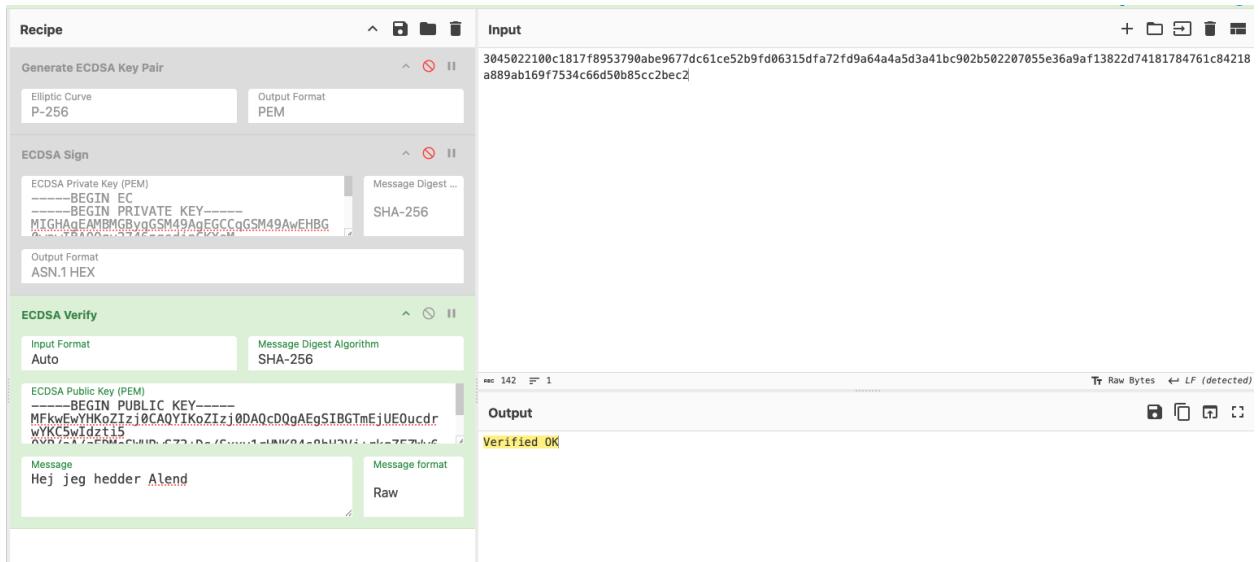
ECDSA Sign
ECDSA Private Key (PEM)
-----BEGIN EC-----
-----BEGIN PRIVATE KEY-----
MIGHAgEAMBMGByqGSM49AgEGCCqGSM49AwEHBG
-----END PRIVATE KEY-----
-----END EC-----
Message Digest ...
SHA-256
Output Format ASN.1 HEX

Input
Hej jeg hedder Alend

sec 20  ⌂ 1  Tr Raw Bytes ↵ LF (detected)
Output ✎
3045022100c1817f8953790abe9677dc61ce52b9fd06315dfa72fd9a64a4a5d3a41bc902b502207055e36a9af13822d74181784761c84218
a889ab169f7534c66d50b85cc2bec2
```

Alend Nezar Mustafa Ismail

Jeg verifier beskeden

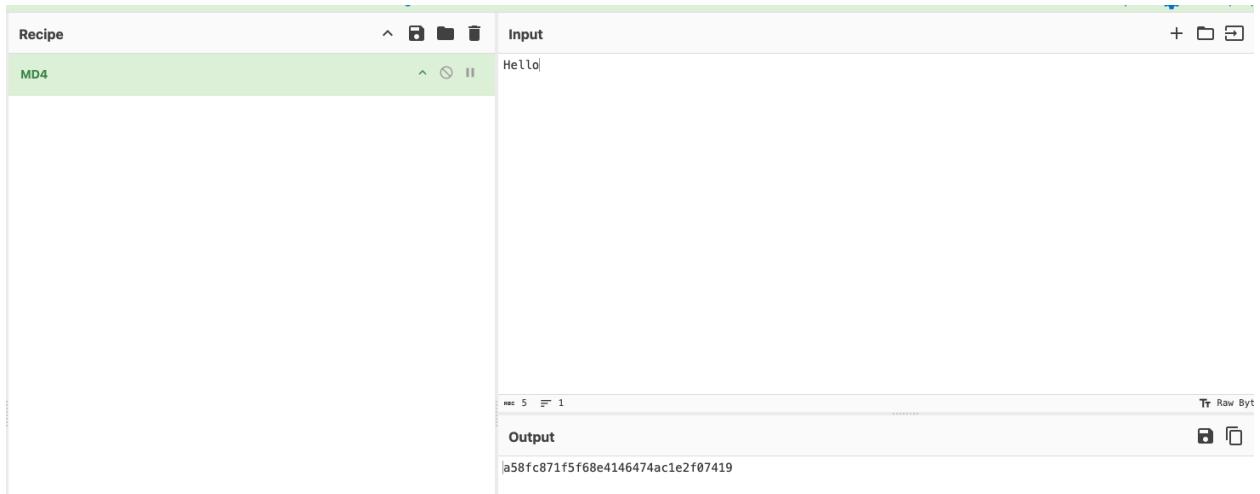


8. Hashcat

Prøv at cracke en MD4 hashet password med Hashcat i din kali. Du kan bruge disse instrukser:

<https://gist.github.com/andracs/e15967fc55d4b7f74011ee525d0f8b69>

Jeg starter med at lave en MD5 kode.



Her kan den cracked kode ses som er Hello

```
a58fc871f5f68e4146474ac1e2f07419:Hello

Session.....: hashcat
Status.....: Cracked
Hash.Mode....: 900 (MD4)
Hash.Target....: a58fc871f5f68e4146474ac1e2f07419
Time.Started....: Wed Dec 3 12:25:56 2025 (3 secs)
Time.Estimated ... : Wed Dec 3 12:25:59 2025 (0 secs)
Kernel.Feature ... : Pure Kernel
Guess.Mask.....: ?a?a?a?a?a [5]
Guess.Queue.....: 2/5 (40.00%)
Speed.#1.....: 47797.9 kH/s (1.77ms) @ Accel:256 Loops:95 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 162944000/7737809375 (2.11%)
Rejected.....: 0/162944000 (0.00%)
Restore.Point....: 1714176/81450625 (2.10%)
Restore.Sub.#1 ... : Salt:0 Amplifier:0-95 Iteration:0-95
Candidate.Engine.: Device Generator
Candidates.#1....: s{s}d → <ani

Started: Wed Dec 3 12:25:52 2025
Stopped: Wed Dec 3 12:26:01 2025
```

9. Crack et passwordbeskyttet zip-fil

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

```
└─(kali㉿kali)-[~]
$ mkdir 6.10

└─(kali㉿kali)-[~]
$ cd 6.10

└─(kali㉿kali)-[~/6.10]
$ touch one two three

└─(kali㉿kali)-[~/6.10]
$ 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]
$ fcrackzip -u -D -p '/home/kali/Desktop/crack.txt' numbers.zip

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

Anvendt kryptografi

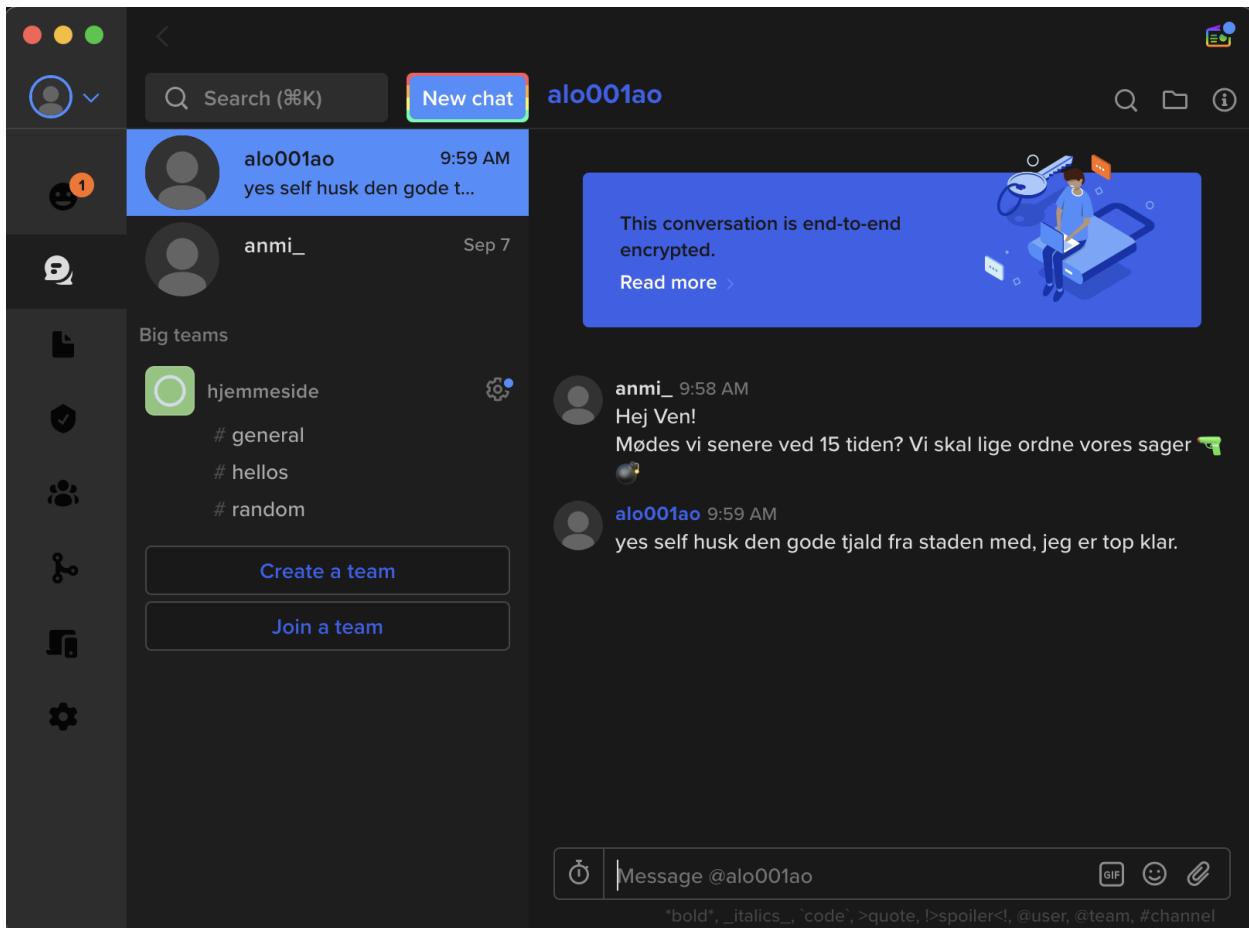
1. TLS certifikater i browsere

Besøg en tilfældig hjemmeside, og undersøg, hvilket certifikat den bruger for HTTPs (TLS.) Sådan kan man gøre det i Chrome (se billeder →)



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

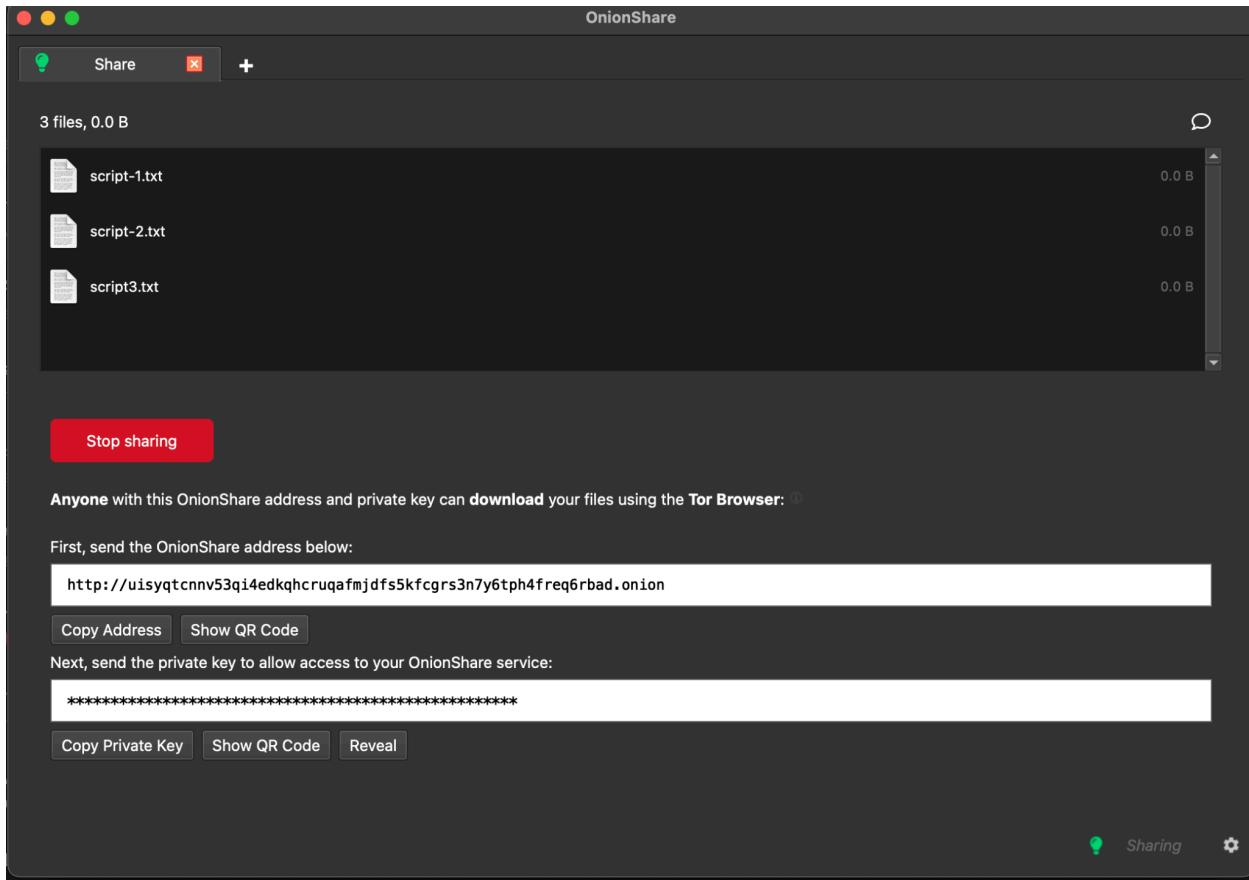
Send en fil til din makker sikkert med [OnionShare](#). Hvordan er det anderledes end Keybase?

OnionShare: Deler filer anonymt via Tor med et midlertidigt .onion-link. Ingen konto, ingen server – direkte fra din computer.

Keybase: Bruger krypteret chat/filoverførsel gennem en konto på deres platform. Hurtigere, men ikke anonymt og afhænger af Keybases servere.

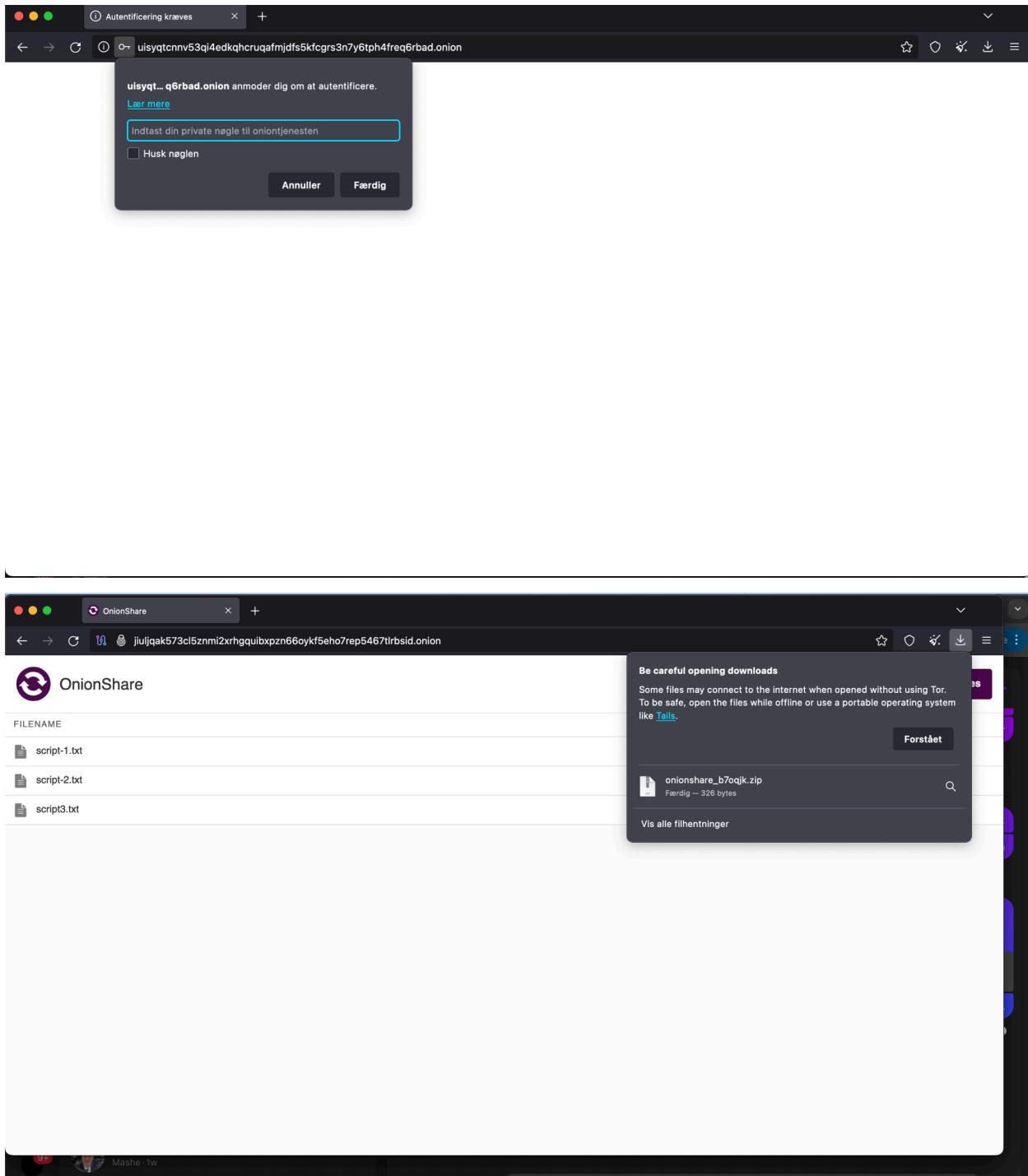
Alend Nezar Mustafa Ismail

Jeg sender filer til medstuderende:



Jeg modtager filer fra medstuderende.

Alend Nezar Mustafa Ismail



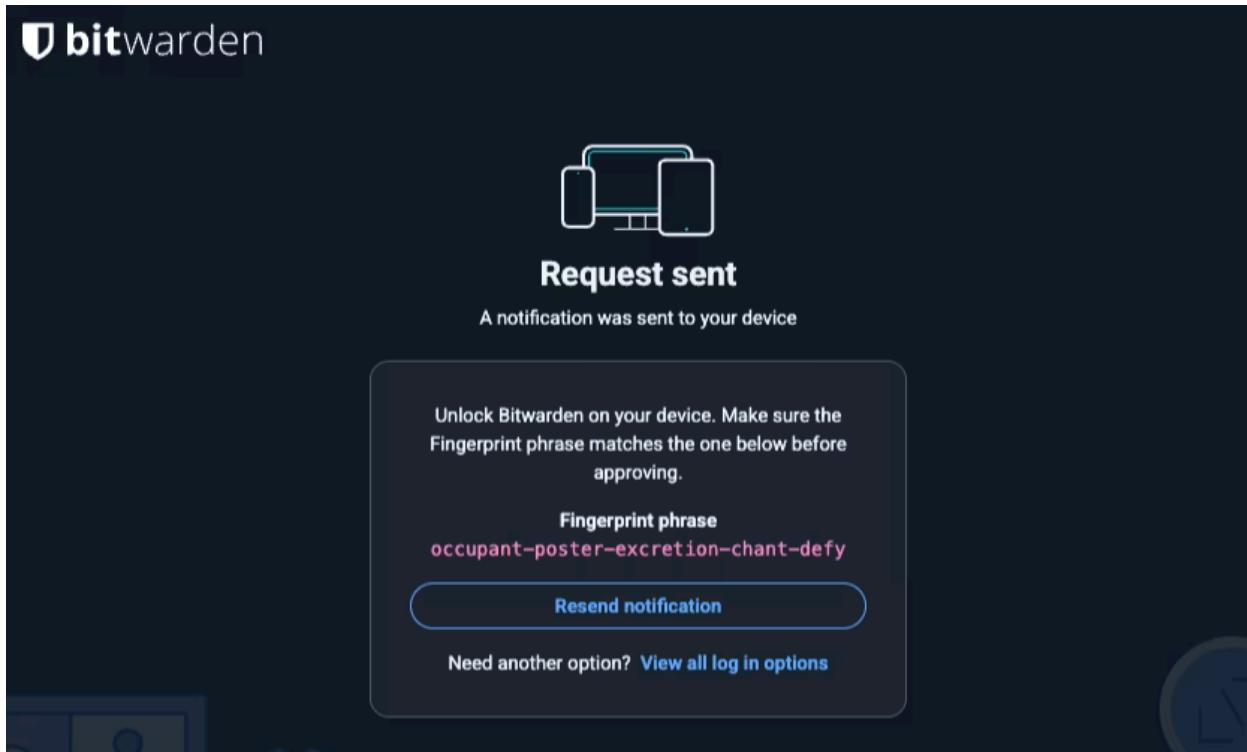
4. Pcrypt

Undersøg [Pcrypt](#), som er en lokal virksomhed, der tilbyder kryptografi.
Måske en praktikplads?
Det kunne være en god mulighed for praktik.

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 fandt bitwarden, som er en open source password manager. Den fungere virkelig godt



6. Kryptografi i din software

Web Crypto API er tilgængeligt i alle webbrowsere, og kan bruges til at kryptere og hashe med. I denne opgave skal du undersøge, hvad Web Crypto API er for noget.

1. Besøg <https://copilot.cloud.microsoft/>
2. Spørg “Hvad er Web Crypto API, og hvad kan den bruges til? Forklar til en bachelorstuderende i it-sikkerhed.”
3. Sprøg også: “Kan du give et eksempel på brug?”

Alend Nezar Mustafa Ismail

Memoriser svaret.

I dag —

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

 Copilot 

Web Crypto API er en standardiseret JavaScript API, som giver webapplikationer adgang til kryptografiske funktioner direkte i browseren – uden at skulle bruge eksterne biblioteker. Den er designet til at være sikker, effektiv og nem at bruge i moderne webapplikationer.

Hvad er det?

Web Crypto API er en del af W3C-specifikationen og implementeres i de fleste moderne browsere. Den giver udviklere mulighed for at udføre kryptografiske operationer som:

- **Hashing** (fx SHA-256)
- **Symmetrisk kryptering og dekryptering** (fx AES)
- **Asymmetrisk kryptering og signering** (fx RSA, ECDSA)
- **Generering af nøgler** (til både symmetrisk og asymmetrisk kryptografi)

7. Sikker e-mail?

E-mail-protokollerne er desværre skabt uden indbygget sikkerhed i tidernes morgen. Derfor er der ikke et enkelt svar på, hvordan man kan sende en sikker e-mail. I denne opgave skal du afprøve mulighederne for at sende sikker e-mail. Spør copilot om:

- hvordan kan jeg sende sikker mail fra gmail (eller hotmail eller andet, erstat med din egen mailudbyder)

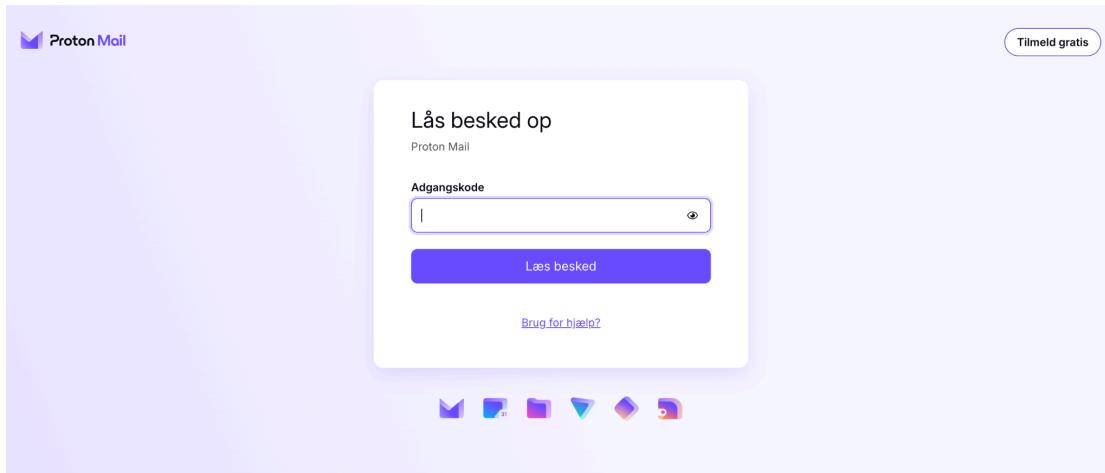
Man kan bruge PGP. Jeg eller modtageren opretter hver vores nøglepar. Jeg krypterer mailen med modtagerens offentlige nøgle. Modtageren dekrypterer med sin private nøgle, det kan integreres via browser plugins som mailvelope

- hvordan kan jeg sende sikker mail fra office 365 (din edumail på skolen)

Alend Nezar Mustafa Ismail

Man kan bruge Office Message Encryption, som kan sendes krypteret direkte fra outlook. Tryk på Options -> Encrypt eller Permissions -> do not Forward. Så modtageren en sikker portal til at læse mailen, selvom de ikke bruger office 365

Jeg vælger at bruge Proton Mail til at sende en sikkermail



Proton

You have received an encrypted email from
[REDACTED]

[Learn more about password-protected emails](#)

Expiry date

Thursday December 25th 2025 at 17:38:37 GMT

Password hint

None

[Unlock message](#)

Please contact the sender if you have any trouble opening this email.

Want to send secure messages? Protect your privacy with a free [Proton account](#).

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

<https://www.cfcs.dk/da/temasider/overgangen-til-kvantesikker-kryptografi/>

- Kvantecomputere truer klassisk kryptografi
- Tidshorisonten er usikker
- Indsaml nu – dekryptér senere-angreb
- Standardisering af kvantesikre algoritmer er i gang
- Digitale signaturer og identitet
- Smalle eller ældre systemer kræver særlig opmærksomhed

9. Blockchain fra bunden

(Ekstra) Diskuter, hvordan I ville udvikle blockchain fra bunden.

Beskriv de væsentligste steps i et par sætninger.

(Ekstra ekstra) Lav en dummyudgave af denne blockchain.

Index: 0 Data: Genesis Block Hash:

5e23892343061f4b11d847eee2dace1ad27f5563f681f6a5ac5b6c9fec3e4ab Index:

1 Data: Transaktion: Alend sender 5 BTC til Alperen Previous Hash:

5e23892343061f4b11d847eee2dace1ad27f5563f681f6a5ac5b6c9fec3e4ab Hash:

c1615ee41dc65097035e5f99cea3f2aa4cb553fa6ff9e0245ba3b496338daf78 ...

Er blockchainen gyldig? True