Kryptografiopgaver

september, 2025

➡️ De fleste øvelser udføres sammen med en anden, hvor i bytter ciffertekst, og dechifrerer hinandens besked.

➡️Du skal dokumentere øvelserne i et dokument til din portfolio.

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

Eksempel på løsning
Eman har klartekst: Hello world
Kryptotekst: Uryyb jbeyq
Algoritme: ROT-13

Modtaget fra min medstuderende:
Kryptotekst: xbqrbeq
Klartekst: Kodeord

2. Vigenére

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

3. Steganografi

Steganografi: Find beskeden i det kattebillede, som du kan finde på dette link:
https://gist.github.com/andracs/c2b6a7ae6efb179043b6728e312222ac

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

4. (Ekstraopgave) Enigma og Bomba

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

Moderne kryptografi

1. Symmetrisk kryptering

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

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.

b. *RSA Signer* din besked med din egen private key, send til din makker. Din makker skal *RSA Verify* med din public key.

c. Spoiler alert: Løsning hint a - Løsning hint b - Mulig løsning

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

Prøv Base64 og Base32

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.)

5. Hashing

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

d. Send dem til din makker.

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

f. Gentag evt. med at beregne hashen af en fil

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.

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/)

8. Hashcat

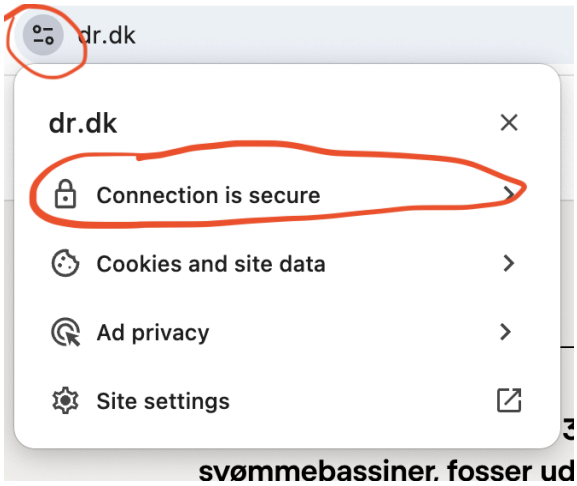
Prøv at cracke en MD4 hashet password med Hashcat i din kali. Du kan bruge disse instrukser:
https://gist.github.com/andracs/e15967fc55d4b7f74011ee525d0f8b69

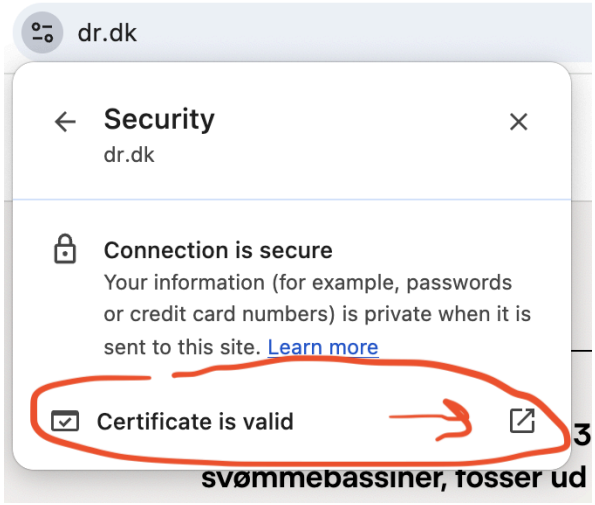
9. Crack et passwordbeskyttet zip-fil
Efterprøv denne øvelse i Kali, hvor du laver en passwordbeskyttet zip-fil, og du cracker den bagefter.

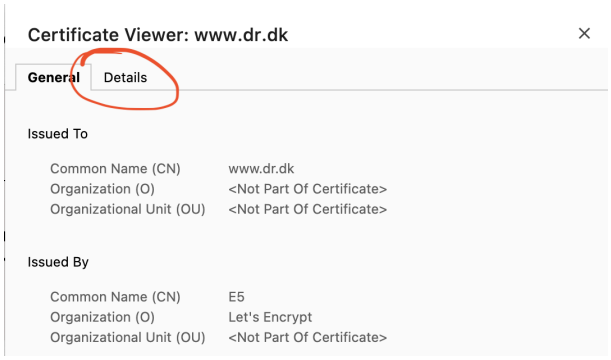
Anvendt kryptografi

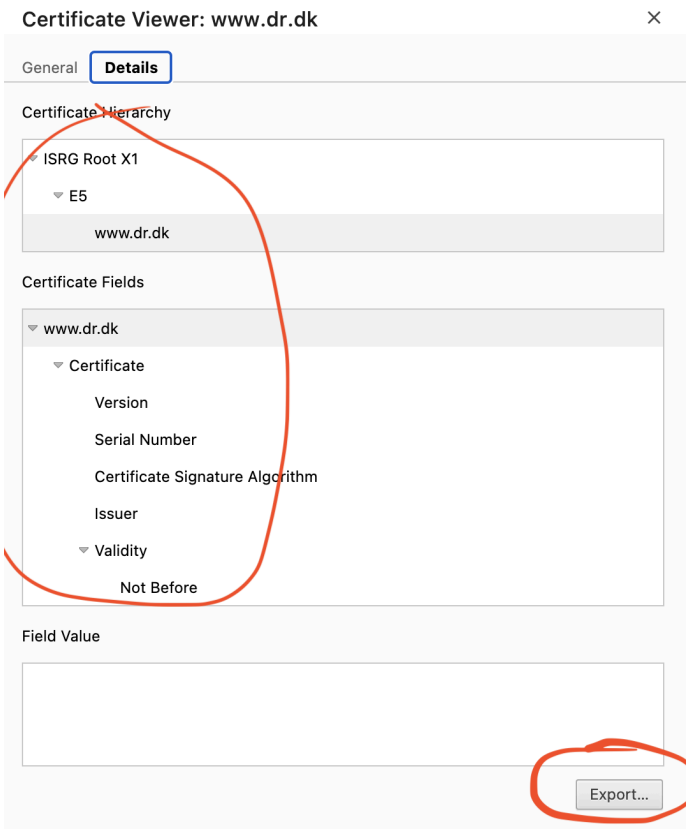
1. TLS certifikater i browsere

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?

4. Pcrypt

Undersøg Pcrypt, som er en lokal virksomhed, der tilbyder kryptografi. Måske en praktikplads?

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".

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?"

Memoriser svaret.

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

8. Læs artiklen og beskriv det i 6 bullet points (no AI)
https://samsik.dk/cybersikkerhed/temaer/overgangen-til-kvantesikker-kryptografi/

9. Blockchain fra bunden
(Ekstra) Diskuter, hvordan I ville kunne udvikle blockchain fra bunden. Beskriv de væsentligste steps i et par sætninger.
(Ekstra ekstra) Lav en dummyudgave af denne blockchain.