Lær om gode kodeord

T1 – Sikkerhed

# Opgavens fokusområder

* + Du har kendskab til regler for sikker færdsel på nettet herunder best practice for kodeord

# Kort fortalt

I denne opgave skal du lære teorien bag gode kodeord, og efterfølgende opsætte en password-manager, som du kan bruge til at gemme dine kodeord i.

# Praktiske oplysninger

Du kan finde både programmet og plugins på <http://keepass.info>. Du kan finde vejledninger på wikipedia, programmets hjemmeside eller ved at søge på Youtube.

Hvis du ikke bryder dig om at gemme dine egne eksisterende koder i password manageren, så kan du vælge blot at oprette en smid-væk konto på et forum eller lignende, som du kasserer når opgaven er færdig.

# Opgave

## Del 1 – Tilegnelse og test af viden

1. Læs tegneserien [XKCD: Password Strength](https://xkcd.com/936/)
   1. Hvad er det tegneseriens forfatter ønsker at fortælle os med denne tegneserie?

At et password som Tro0ub4dor&3 er sværere at huske og lettere at knække end et password som correcthorsebatterystaple.

* 1. Skab 3 kodeord som lever op til de krav som opstilles i XKCD

Differencehopefulcrocodilesunshine, Thinkingdaydreamforgetfulantisocial, Technologicalmasterycomputersecurity

* 1. Kontrollér styrken af disse 3 kodeord på sitet [How Secure is my Password?](https://howsecureismypassword.net/)

Tro0ub4dor&3 = 45mil, correcthorsebatterystaple = 100 quadrillion, Differencehopefulcrocodilesunshine = 17 duodecillion, Thinkingdaydreamforgetfulantisocial = 900 duodecillion, Differencehopefulcrocodilesunshine = 49 quattuordecillion.

1. Se videoen [Ted Talk: Lorrie Faith Cranor: What’s wrong with your pa$$w0rd?](https://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd?language=en)
   1. Hvad er Lorris Faith Cranors budskab?

Når du laver dit password, sørg for at det er et længere password som ikke er alt for enkelt. Korte passwords med forskellige tegn er ofte dårlige og der er nogle tegn der bliver brugt mere end andre.

* 1. Hvor er hun uenig med XKCD?

Fordi hun lavede tests som viste at de fleste mennesker ikke var bedre til at huske lange ord sat sammen som tilfældige passwords og fordi de lange ord sat sammen var længere, tog det længere tid at type ind og derved lavede man flere fejl, når man skrev det ind.

* 1. Hvad bygger hun sin viden på?

Hun brugte Amazonmechanicalturk for at få nogle data sæt og så kunne hun også afprøve nogle svar imod passwords på et universitet.

1. Læs artiklen [Ars Technica: Anatomy of a hack: How crackers ransack passwords like “qeadzcwrsfxv1331”](https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/)
   1. Hvad er i følge artiklen det største problem med kodeord?

De værste passwords så ud til at være mellem 6-8 tegn da de let kunne blive kendt med ”brute force”. De længere passwords kunne blive kendt ved hjælp af mønstre fra f.eks. tidligere leaks af passwords.

* 1. Hvad er det som gør vores kodeord usikre?

De fleste laver et password som følger et mønster som hackere kan bruge til at ”brute force” som f.eks. et stort bogstav i starten, små bogstaver i midten og bogstaver/tegn i slutningen fordi det følger et mønster.

* 1. Hvordan skal et kodeord se ud for at være sikkert?

Mindst 11 tegn, både små og store bogstaver, numre og ikke er en del af et mønster.

1. Læs artiklen [Anatomy of a password disaster – Adobe’s giant-sized cryptographic blunder](https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/)
   1. Hvad betyder begreberne *hashed* og *salted*?

Hashed er en metode/algoritme som tager et string/password og ændrer værdierne ved hjælp af metoden/algoritmen.

Salted er hvor man tilføjer en string tilfældigt ind i ens password før man laver en hash. Så hvis 2 personer har det samme password, ville de have forskellige salts og derfor forskellige hashs

* 1. Hvad var hovedproblemet, som medførte at brugernes kodeord slap ud?

Hackere fik adgang til filer eller lign. fra Adobe som gemte følsomme informationer om Adobes brugere.

* 1. Hvordan kunne brugerne have beskyttet sig mod dette?

Bruge bedre passwords, sørge for at de ikke bruger det samme password andre steder og ændre nuværende password hos Adobe.

## Del 2 – Test af viden

Opstil 3 regler for gode kodeord, baseret på den viden du nu har tilegnet dig.

|  |  |
| --- | --- |
| Mine egne 3 regler, som alle mine kodeord skal overholde: | |
| Regel 1 | Benyt et langt password med numre, små og store bogstaver, specielle tegn. |
| Regel 2 | Sørg for at du ikke bruger det samme password flere steder. |
| Regel 3 | Sørg for at dit password ikke følger et mønster. |

## Del 3 – Test af kompetencer

Du skal nu installere password-manageren [Keepass](https://keepass.info/)

1. Læs dokumentation af programmet på Wikipedia og dets egen hjemmeside grundigt igennem.
2. Download programmet, og knyt det sammen med din browser ved at installere relevante plugins til Keepass og de rigtige extensions / addons til din browser
3. Prøv at gemme nogle af dine eksisterende koder i Keepass, og prøve at lade password manageren indtaste koderne for dig når du besøger de pågældende hjemmesider
4. Afprøv muligheder for at lade Keepass generere sikre koder, og prøv at ændre en af dine eksisterende koder til en ny, sikrere kode
5. Afprøv de forskellige muligheder i Keepass, så du er i stand til at anvende alle gængse funktioner
6. Gå på opdagelse i de mange plugins på <http://keepass.info> og afprøv de mest interessante på din egen installation

Vil denne password-manager ville kunne leve op til dine behov?

Ja, men dens interface er meget gammel in indviklet.

## Kriterie for færdiggørelse

Opgaveløsningen er færdig når du…

* Har læst eller set materialet i del 1 og besvaret de tilhørende spørgsmål
* Har udfyldt tabellen i del 2 med 3 gode kodeordsregler
* Har løst opgaverne i del 3

… eller når dagsplanen angiver en ny aktivitet.