

Øving 5: Strengbehandling, datoer og matriser

Svend Andreas Horgen, IDI Kalvskinneth, NTNU
Lærestoffet er utviklet for emnet IINI3003 Webprogrammering med PHP

Oppgave 1 - Noen kontrollspørsmål

Svar for eksempel i en tekstfil:

- Hva er datofunksjoner?
- Anta at vi ønsker å skrive ut informasjon om hvilken dag det er i dag. Hvorfor fungerer ikke denne setningen som forventet?

```
echo date("I dag er det den d. M") . "<br>";
```

Oppgave 2 - Enkel behandling av dato

En side skal vise teksten «God morgen» dersom det er morgen, «God ettermiddag» dersom det er ettermiddag, og «God kveld» dersom det er kveld.

- Bruk datofunksjoner til å løse dette problemet.
- Utvid slik at teksten vises i grønn skrift dersom det i tillegg er søndag.

Oppgave 3 - Reklame

Et nettsted har en toppseksjon med reklameannonser i form av bilder, og ønsker å la en tilfeldig annonse vises på hver side. To brukere som kommer til samme side, kan altså bli presentert for ulike bilder, og etter å ha navigert gjennom flere sider vil de trolig ha sett mange forskjellige annonser. Anta at det er ti bilder totalt. Bruk funksjoner for dato/tidspunkt til å velge et tilfeldig bilde. MERK: Det er veldig mange måter å finne tilfeldige tall/bilder på. Tenk gjerne kreativt rundt hvordan ulike datofunksjoner kan brukes til å plukke ut et bilde tilfeldig. I en "normal" situasjon ville du trolig brukt Random-funksjonen og ikke datofunksjoner. Målet med denne oppgaven er **ikke** å få så tilfeldig uttrekk som mulig, men å øve på datofunksjoner.

XTRA (frivillig): Oppgave 4 - Brukernavn og passord

I kodesnutt 6.4 i boka ble det vist hvordan `md5()` kunne brukes til å lage forslag til passord. Her er sitat fra boka:

```
<?php
    $utgpunkt = "Det er en fin dag i dag";
    echo "$utgpunkt <p>";

    //lager en hashet streng
    $hashet_streng = md5($utgpunkt);
    $strengLengde = strlen($hashet_streng);
    echo "Etter md5 har vi fått denne strengen ";
    echo " <b>$hashet_streng</b> som er en <b>$strengLengde</b>";
    echo "   tegn lang streng av heksadesimale tall<br>";

    $passordLengde = 8;
    //setter startverdi til et tilfeldig sted i strengen, men ikke
    //for nær slutten for å sikre at det blir 8 tegn i passordet
    $start = rand(0, ($strengLengde - $passordLengde - 1));

    //lager selve passordet
    $passordet = substr($hashet_streng, $start, $passordLengde);
    echo "Passordet som foreslås er:<b> $passordet</b>";
?>
```

Det ble også nevnt at strategien ikke er optimal.

- Modifiser løsningen slik at en kan velge hvor langt passordet skal være.
- Gjør forbedringer til løsningen slik at de genererte passordene blir vanskeligere å gjette for uvedkommende.
- Går det an å lage passord som har stor grad av tilfeldighet, uten å bruke `md5()`? Gi et eksempel.
- Lag et skjema som lar brukeren registrere opplysninger om seg selv. Et passende brukernavn som har elementer av både fornavnet og etternavnet, skal produseres i det en knapp trykkes. Hva er faremomentet ved å la en slik løsning lage brukernavn og passord til for eksempel hundre nye studenter/elever ved en skole?

XTRA (frivillig): Oppgave 5 - Krypteringsoppgaven i boka

Her er oppgave 6-4 fra boka (limt inn som skjermbilde slik at de som ikke har bok kan løse den). Du kan lære mye av denne oppgaven.

Kryptering er et interessant og aktuelt fagfelt i websammenheng. Allerede for flere tusen år siden var det vanlig å benytte kryptering for å sikre at ikke meldinger kunne tolkes av fienden. Cæsars metode bygde på substitusjon i form av forskyvning. Alle forekomster av «a» ble erstattet med «d», «b» ble erstattet med «e» og så videre. Bare den som kjente mønsteret, klarte å reversere prosessen og slik dekode meldingen til meningsfull tekst.

- Lag en funksjon som krypterer en melding ved å endre alle tegn ved forskyvning. Du skal ikke bruke noen innebygde krypteringsfunksjoner til denne oppgaven, men vil trolig få bruk for funksjonene `ord()` og `chr()`. Lag gjerne funksjonen så fleksibel at antall tegn som skal forskyves (nøkkelen), mottas som argument.
- Hva må til for å håndtere bokstaver på slutten av alfabetet, slik at disse forskyves til starten av alfabetet? (Hint: Se modulo-operatoren avsnitt 2.3.3.)
- Lag også en funksjon som dekrypterer en tekststreng som er kryptert.
- Er det mulig å lage en funksjon som kan brukes til å både dekryptere og kryptere?

Her er en annen metode for å kryptere en beskjed som gjør bruk av matriser på en interessant måte. Beskjeden er for eksempel:

"Hovedstaden i Norge er Oslo!"

Stegene i krypteringen er å legge hvert tegn inn i en matrise rad for rad. I dette tilfellet brukes fem kolonner i matrisen, men dette kan varieres:

```
H o v e d
s t a d e
n   i   N
o r g e
e r   O s
l o !
```

Ved å lese tegnene kolonne for kolonne kan en ny tekststreng bygges opp. Resultatet er den krypterte meldingen:

"Hsnoelot rrovaig! ed eO deN s "

Merk at mellomrom også er tegn.

- Lag en funksjon som krypterer innkommende tekst i henhold til denne strategien.
- Lag en funksjon som dekrypterer en slik tekst.
- Lag et skjema som lar brukeren skrive inn ønsket melding, velge en av krypteringsmetodene du har lagd, og deretter får den krypterte strengen skrevet ut på skjerm.