TEKNOLOGIFORSTÅELSE SOM FAG – UDSKOLING

7. KLASSE

Kryptering, kommunikation og data i klassen og samfundet (1:3)

Teknologiforståelse i folkeskolen

KØBENHAVNS PROFESSIONS HØJSKOLE | LÆREMIDDEL.DK | VIA University College | UCN | RAMBØLL

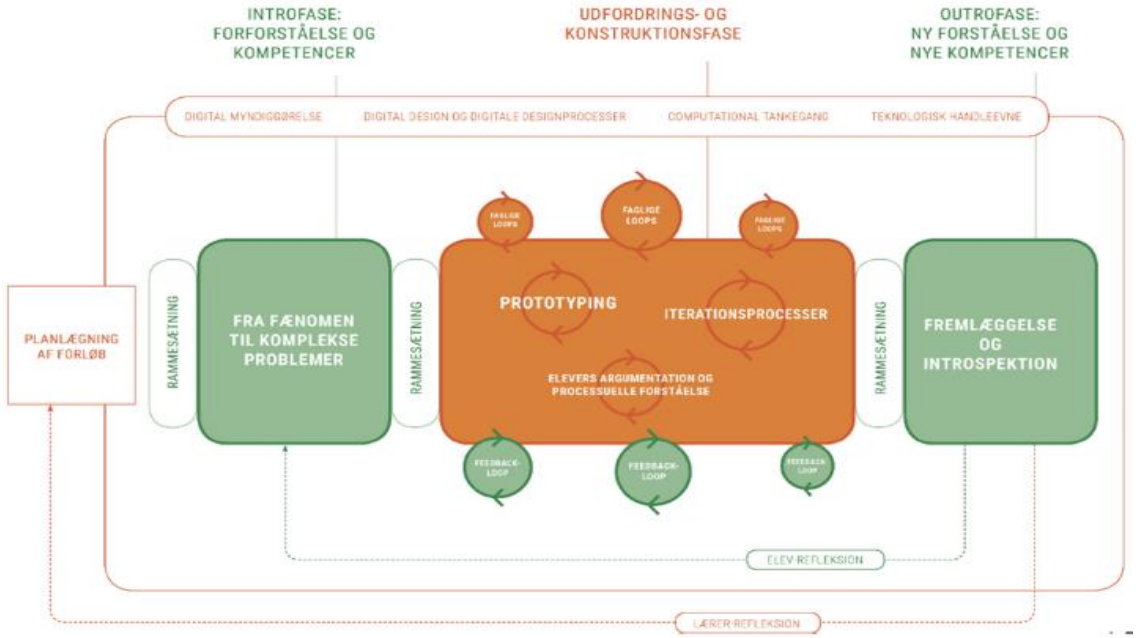
Teknologiforståelse i folkeskolen

Indholdsfortegnelse

1. Forløbsbeskrivelse

Forløbet er bygget op over det didaktiske format for prototyperne med en introducerende del, en mere undersøgende/eksperimenterende del og en outro-del med opsamlinger og evalueringer, se figur 1.

Figur 1: Didaktisk prototypeformat



1.1 Overordnet beskrivelse – tre sammenhængende forløb

Et vigtigt aspekt af elevernes alsidige udvikling er at arbejde med elevernes oplevelse af handlekraft og refleksion over egen situation – i skolen, i hverdagen og senere i samfundet.

En del af hverdagens udfordringer i et digitaliseret samfund er at kunne forholde sig til den udbredte indsamling og deling af data, vi som borgere er en del af. For at kunne være aktive og kritiske borgere, har vi derfor brug for viden om data og brug for færdigheder i at indsamle og analysere data. Vi har brug for viden om, hvordan digitale artefakter indsamler data om os, og hvordan vi selv kan indsamle og benytte data. Men vi har også brug for viden om betydningen af den øgede overvågning og viden om, hvordan vi sikrer egne data, fx gennem kryptering.

Tre forløb om kryptering, kommunikation og data i klassen og samfundet

I disse forløb vil eleverne gennem tre forskellige aktiviteter udvikle faglige kompetencer og opnå færdigheder og viden til at forstå muligheder og konsekvenser i teknologier omkring os, når vi bruger dem til at sende informationer til hinanden. Eleverne skal gennem forløbene arbejde med teknologifagets fagbegreber, og der lægges i arbejdet med forløbene vægt på, at der bevidst arbejdes med at udvikle et nyt fælles sprog i klassen.

Forløbene er planlagt i følgende rækkefølge:

Tabel 1: Forløbsoversigt

TITEL	INDHOLD	KOMPETENCEMÅL
Kryptering (8 lektioner)	I dette forløb sættes scenen med et historisk tilbageblik på datalogiens historie og kryptering under anden verdenskrig med filmen The Imitation Game. Herefter arbejder eleverne praktisk med koder og kryptering.	Digital myndiggørelse: ■ Teknologianalyse ■ Formålsanalyse ■ Konsekvensvurdering Computationel tankegang: ■ Data Teknologisk handleevne: ■ Netværk ■ Sikkerhed
Krypteret kommunikation (10 lektioner)	Eleverne arbejder undersøgende med eksisterende, krypterede teknologier og eleverne giver et bud på en sikker app til en fiktiv journalist, der har brug for høj grad af sikkerhed.	Digital myndiggørelse ■ Teknologianalyse ■ Formålsanalyse ■ Konsekvensvurdering ■ Redesign Computationel tankegang: ■ Data Teknologisk handleevne: ■ Netværk ■ Sikkerhed
Tingenes internet (Internet of Things) (22 lektioner)	Efter at have introduceret eleverne til nogle af udfordringerne ved kommunikation gennem apps og sociale medier, arbejder eleverne i denne del med at designe en model for indsamling af data i klassen med henblik på at øge læring og trivsel.	Digital design og designprocesser ■ Rammesættelse ■ Idegenerering ■ Konstruktion ■ Argumentation og introspektion Computationel tankegang: ■ Data Teknologisk handleevne: ■ Netværk ■ Sikkerhed

Der er en indbyrdes sammenhæng mellem de tre forløb, som på forskellig vis tager udgangspunkt i elevernes hverdag og globale problematikker.

1.2 Resumé: Kryptering

I dette forløb om kryptering arbejder eleverne med velkendte fænomener som galgeleg og krydsord for at forstå principper bag kryptering. I forhold til det digitale genstandsfelt arbejder eleverne med analyse og vurdering af frit tilgængelige apps. Der arbejdes med komplekse problemstillinger som kryptering, som gennem forløbets indsnævring har fået karakter af tamed problems, som eleverne kan arbejde med og komme med forskellige løsninger på.

Det betyder imidlertid, at læreren har en stor opgave i forhold til at bevare det teknologiske genstandsfelt og bringe elevernes refleksioner tilbage til de individuelle, lokale og samfundsmæssige perspektiver.

I forløbet sættes scenen med et historisk tilbageblik på datalogiens historie og kryptering under anden verdenskrig med filmen The Imitation Game. Herefter arbejder eleverne praktisk med koder og kryptering. Kryptering er en væsentlig del af sikringen mod overvågning, som eleverne arbejder med i næste forløb.

Der er god hjælp at hente for læreren i denne artikel og video fra videnskab.dk:
https://videnskab.dk/teknologi/video-foredrag-sadan-blev-tyskernes-enigma-kryptering-knaekket.

Dette forløb lægger op til næste forløb om overvågning, hvor vi bruger app'en Signal som eksempel. Derfor starter vi med at se nærmere på denne og andre kommunikationsapps i dette forløb. Signal fungerer lidt som et online forum eller en sms-app. Signals opgave er at kryptere meddelelserne, så andre ikke får fat i dem, og den er derfor meget benyttet af fx journalister, som har stort behov for at kunne kommunikere uden myndigheder eller andre kan følge med.

Signal er udgivet af virksomheden Open WhisperSystem og er open source. Det betyder, at alle kan få adgang til koderne og hjælpe til med at gøre app'en så sikker som muligt. Signal er gratis at bruge og kræver ikke abonnement. Der er ingen reklamer og, ifølge Open WhisperSystem, ingen overvågning af brugerne. Open source er betegnelsen for software, hvor man har adgang til koden og mulighed for selv at ændre i koderne og skabe et nyt og bedre program.

Produkt:

I udfordring 1 arbejder eleverne individuelt med at udarbejde koder, som afprøves i gruppen, evt. i par. Der gives eksempler på koder og ombytningstavler i systemet atbash, cæsar og i morse. Eleverne skal løse en simpel kode for at tjekke egen forståelse. Herefter konstruerer de egne koder ud fra samme ombytningstavle og konstruerer endelig selv egne ombytningstavler.

I udfordring 2 arbejdes videre med information fra filmen the Imitation Game, hvor eksperter i krydsord bliver til eksperter i kodebrydning. Eleverne skal i denne opgave se nærmere på, hvordan koder kan brydes

gennem viden om sproget. Eleverne får en liste over danske bogstavers hyppighed stillet til rådighed og laver deres egen undersøgelse af bogstavers hyppighed i deres egen galgeleg.

I opgaven agerer gruppen afprøvningslaboratorium og opgaverne fordeles mellem gruppens deltagere:
- En elev står for at udvælge ord og gennemføre galgelegen (går evt. på skift)
- En elev sørger for at alle ord samles i et regneark
- Resten af gruppen deltager i galgelegen

Optælling af ord kan ske i par, eller enkeltvis, i et fælles, delt regneark. Herefter arbejder gruppen sammen om at udarbejde regler for løsning af galgelegsopgaver. Reglerne afprøves i fællesskab i gruppen og gruppernes resultater samles i klassen.

1.3 Rammer og praktiske forhold

1.3.1 Varighed

8 lektioner svarende til ca. 4 uger - afhængigt af brugen af faglige loops.
- Introduktion: 1 lektion
- Film: 3 lektioner
- Udarbejde koder: 1 lektioner
- Krydsord/galgeleg: 2 lektioner
- Præsentation, opsamling: 1 lektion

1.3.2 Materialer

Der vil under forløbet være brug for følgende ressourcer:
- Filmen The imitation game (evt. fra CFU)
- Videnskab.dk (2012), *Sådan blev tyskernes Enigma-kryptering knækket* (videoforedrag).
  - https://videnskab.dk/teknologi/video-foredrag-sadan-blev-tyskernes-enigma-kryptering-knaekket.
- Data over danske bogstavers hyppighed hentet fra: https://dsn.dk/nyt/nyt-fra-sprognaevnet/numre/argang-1968-1984/marts-1970-pdf.
- Kopier af eventuelle koder, morsenøgler mm.
- Adgang til regneark
- Materialer til at lave kravsspecifikation, evt. med illustration
- Computer med adgang til internettet

1.3.3 Lokaler

Forløbet vil kunne gennemføres i et almindeligt klasselokale med mulighed for at vise film fra fx CFU ved hjælp af projekter med lyd, eller tilsvarende.

2. Mål og faglige begreber

Der arbejdes i dette forløb primært med kryptering og teknologifaglige begreber som digital myndiggørelse, teknologianalyse, formålsanalyse, konsekvensvurdering, data, netværk og sikkerhed.

KOMPETENCE-OMRÅDER	DIGITAL MYNDIGGØRELSE	COMPUTATIONEL TANKEGANG	TEKNOLOGISK HANDLEEVNE
Kompetencemål (efter 9. klassetrin)	Eleven kan handle med dømmekraft i komplekse situationer, der vedrører digitale artefakters betydning for individ, fællesskab og samfund.	Eleven kan reflektere over og anvende computationel tankegang på problemstillinger fra omverdenen.	Eleven kan vurdere, vælge og på kvalificeret vis anvende digitale teknologier i autentiske situationer.
Færdigheds- og vidensmål	Teknologianalyse ■ Eleven kan vurdere egne og andres digitale artefakter ift. artefaktets komposition. ■ Eleven har viden om modeller til analyse af digitale artefakters komposition.	Data ■ Eleven kan behandle, vurdere og visualisere data reflekteret ved hjælp af digital teknologi. ■ Eleven har viden om kriterier for datakvalitet.	Netværk ■ Eleven kan vurdere muligheder og begrænsninger ved udveksling af data i digitale netværk. ■ Eleven har viden om den grundlæggende opbygning og virkemåde af digitale netværk.
	Formålsanalyse ■ Eleven kan vurdere digitale artefakter gennem afkodning af et artefakts formål og intentionalitet. ■ Eleven har viden om formål og intentionalitet udtrykt gennem designet af digitale artefakter.		Sikkerhed ■ Eleven kan handle sikkert og hensigtsmæssigt i interaktionen med digitale teknologier og digitale artefakter. ■ Eleven har viden om sikkerhedsmæssige aspekter ved færden i den digitale verden.
	Konsekvensvurdering ■ Eleven kan kritisk reflektere over digitale artefakters betydning for		

	individ, fællesskaber og samfund ■ Eleven har viden om digitale artefakters betydning for individ, fællesskaber og samfund		

3. Forløbsnær del

3.1 Introfase: Forforståelse og kompetencer

3.1.1 Kort rids af fasen

Eleven arbejder med kommunikation og digitale kommunikationsværktøjer, med henblik på at udvikle kompetencer til at udvælge den rette teknologi til et autentiske scenarie. Der vil i dette forløb lægges særlig vægt på sikker og hensigtsmæssig kommunikation på nettet.

Gennem forløbet arbejder eleverne med teknologianalyse og vurderer tre kommunikationsapps. Målet med analysen er at udvikle kompetencer til afkodning af artefakters funktion og formål, som de kommer til udtryk gennem designet. Dette arbejde munder ud i elevernes arbejde med konkrete eksempler på redesign i form af kravsspecifikationer til en ny kommunikationsapp. Fokus for elevernes arbejde vil være på funktionen i den aktuelle situation, hvor sikker og privat kommunikation er afgørende.

Gennem arbejde med koder og kryptering trænes elevernes algoritmiske tænkning og eleverne stifter bekendtskab med, hvordan databaser med informationer, fx om bogstavernes hyppighed, ligger bag forskellige teknologier.

Der arbejdes med begreber som *kryptering*, *kommunikation*, *Open Source* og *overvågning*. Det anbefales at arbejdet begynder med fælles snak i klassen om de centrale begreber, hvor elevernes erfaringer og viden bringes i spil, inden appen Signal bruges som eksempel til at udfolde begreberne og deres betydning for individ og samfund.

3.1.2 Komplekst problemfelt

Data flyder rundt mellem os og de digitale artefakter omkring os. Men hvordan kan disse data sikres gennem kryptering og hvordan omsættes disse behov til en brugbar kommunikationsapp, der fx kan benyttes af journalister i verdens brændpunkter?

3.1.3 Problemstilling

Hvordan kan vi lave vores egne koder, der kan kryptere meddelelser og hvordan kan vi bruge vores viden til at lave strategier for at bryde andres koder? Hvilke data samler og videregiver almindelige kommunikationsapps, og hvilke har vi brug for at kryptere?

3.1.4 Iscenesættelse/scenarie

For at introducere problemfeltet til eleverne anbefales filmen The Imitation Game, der er tilgængelig på mitCFU. Her får eleverne gennem en narrativ ramme om Alan Turings liv en indsigt i kryptering af koder under 2. verdenskrig.

Efter filmen beskriver eleverne i fællesskab russernes Enigma og Turings maskine.

BEMÆRK at filmen strækker sig over næsten 3 lektioner.

3.2 Udfordrings- og konstruktionsfase

I denne del arbejder eleverne undersøgende.

De præsenteres for simple, monoalfabetiske ombytningstavler (Atbash, Cæsar og morse) og bruger disse tavler til at løse to simple koder.

Herefter bruger eleverne deres viden om monoalfabetiske ombytningstavler til selv at skabe koder og afprøve dem på hinanden. Alt efter klassens sammensætning kan der være behov for, at der samles op efter hver af delopgaverne. I denne opsamling benyttes begreberne monoalfabetisk ombytningstavle, kryptering og hemmelig nøgle, hvor det er relevant. Derudover gives løbende feedback af læreren gennem elevernes arbejde.

Det anbefales, at eleverne arbejder i grupper.

3.2.1 Konkret udfordring 1: Løs koder

Ombytningstavle i Atbash

Atbash er et gammet hebraisk kodesystem. Det er monoalfabetisk, fordi hvert bogstav bliver udskiftet med et andet. Bogstaverne i Atbash bliver erstattet af et i samme afstand fra den modsatte ende af alfabetet. Det første bogstav, B, bliver altså erstattet af det sidste bogstav, Å, og så videre. Du kan se hele ombytningstavlen herunder:

Tabel 2: Ombytningstavle - Atbash

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
Å	Ø	Æ	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Kan du, ved at bruge ombytningstavlen, læse denne tekst:

JILUPW HÅL QYZ JUR ÅJ WLIPZRCWWY ZÅJÅROWUYP

Ombytningstavle i Cæsar

En anden ombytningstavle er udviklet af Julius Cæsar. Her er alfabetet ikke spejlvendt som i Atbash, men flyttet X-antal pladser til venstre, fx 3 som her: A er blevet til D og N er blevet Q og så videre.

Tabel 3: Ombytningstavle - Cæsar

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Æ	Ø	Å	A	B	C

Kan du, ved at bruge ombytningstavlen, læse denne tekst:

DUWKXU VFKHUELXV EØJJHGH HQLJPD

Morse

På samme måde har man i mange år brugt morse til at sende beskeder med lys, som siden kunne læses ved hjælp af en morsenøgle. Nøglen læses oppefra og ned. Hvide felter er en prik, grå felter en streg. Mest brugte bogstaver (på engelsk) er kortest. Et E er altså en prik, mens et V er prik-prik-prik-streg (med denne simple nøgle skrives Å som AA).

Tabel 4: Morsenøglen

E								T							
I				A				N				M			
S				U				R				W			
H	V	F		L	Æ	P	J	B	X	C	Y	Z	Q	Ø	

Afprøv selv morsenøglen ved at sende meddelelser til hinanden. I kan enten bruge lyset fra en mobiltelefon eller aftale at en finger er en prik, mens to fingre er en streg. På den måde kan I signalere til hinanden i klasse uden brug af digitale teknologier.

Lektionen afsluttes ved, at eleverne laver egne koder, som de bruger til at sende beskeder til hinanden. En anden gruppe "opsnapper" beskeden og skal forsøge at bryde koden.

3.2.2 Konkret udfordring 2: Galgeleg

I Alan Turings team sad også kodelæsere, der var udvalgt, fordi de var dygtige til at løse kryds og tværs. Men hvorfor egentlig? Hvis man tit har spillet galgeleg, eller løst kryds og tværs, så ved man, at nogle bogstaver er mere hyppige end andre, og at nogle kombinationer er mere sandsynlige end andre. Det kan man udnytte, hvis man vil være hurtig til at løse den slags ordopgaver eller bryde koder, der bygger på monoalfabetiske ombytningstavler.

Vi skal nu prøve at blive dygtigere til at lege galgeleg.

Tabel 5: Data over danske bogstavers hyppighed

Kilde: https://www.dsn.dk/nyt/nyt-fra-sprognaevnet/numre/argang-1968-1984/marts-1970-pdf
I tabellen ovenfor kan du se en tabel over danske bogstavers hyppighed. Som du kan se, bruger vi E mest, og W, Z, Z og Q mindst.

Du skal nu lave dit eget datasæt: spil en omgang Galgeleg i klassen. Aftal et emne, fx ordsprog eller danske dyr. Aftal om både ord og sætninger er tilladte. Valget af emner kan have stor betydning for udfaldet. Lav derfor øvelsen med forskellige emner.

Alle ord skrives ned og bruges til at lave jeres egen registrering af, hvilke bogstaver der bruges hyppigst. Data samles i et regneark. Optælling kan fx ske ved at markere hele teksten og søge på forekomsten af et bogstav (altså hvor mange gange, et bogstav findes i teksten).

SÆTNINGER FRA GALGELEG, ORDSPROG
Tab og vind med samme sind
Gammel kærlighed ruster ikke
Små gryder har også ører
Tyv tror hver mand stjæler

OPTÆLLING AF BOGSTAVER

A	5
B	1
C	0
D	6
E	9
…	…

Men vi kan også gøre vores analyse mere præcis:

- Hvilke bogstaver følger fx typisk efter et E? Eller efter et R?
- Hvilke bogstaver står typisk før et E og før et R?

I kan udvide med flere af de mest hyppige bogstaver. Når I har samlet jeres data, kan I samle nogle simple regler for galgeleg.

Kan jeres regler gøre jer bedre til at spille galge? Afprøv spillet igen i gruppen og afprøv jeres system.

3.2.3 Faglige loops

- Til udfordring 1: Hvor har man brugt det hebraiske kodesystem Atbash, hvem var Cæsar, og hvor kunne han have haft brug for et kodesystem?
- Til udfordring 2: Hvad dækker begrebet hyppighed?

3.2.4 Feedbackloops

- Efter filmen:
  - Beskriv med egne ord, hvad Enigma-maskinen kunne, som man ikke ville kunne opnå uden Enigma.
  - Forklar hvorfor det var så vigtigt, at man opfangede nogle enkelte ord, man kunne tyde.
  - Beskriv med egne ord, hvorfor der var brug for så stor en maskine for at kunne bryde koderne?

- Til udfordring 1:
  - Hvad er kodernes i Atbash og Cæsar største sårbarhed?
  - Hvordan ville I kunne gøre koderne og ombytningstavlerne i Atbash og Cæsar sværere at bryde?
- Til udfordring 2:
  - Kan I komme med konkrete eksempler på, hvordan hyppigheden for bogstaver på dansk må være forskellig fra fx engelsk? Hvorfor har rækkefølgen betydning?

3.3 Outrofase: Ny forståelse og nye kompetencer

Som afslutning afprøver grupperne deres regler på en anden gruppe. Herefter præsenterer grupperne sine resultater for hinanden og løsningerne vurderes i forhold til, hvor effektive de har vist sig i afprøvningen.

4. Perspektivering

4.1 Evaluering

Under evalueringen lægges der vægt på, om eleverne i forbindelse med præsentationerne kan benytte centrale begreber som algoritmer, hyppighed og databaser. Endelig lægges der vægt på, at eleverne frit kan samtale om begreber som *kryptering*, *kommunikation*, *Open Source* og *overvågning*.

4.2 Progression

Den indsamlede viden bringes videre til det næste forløb om overvågning.

4.3 Differentieringsmuligheder

- Til udfordring 1: Nogle elever vil være fortrolige med arbejdet med koder, mens det for andre elever vil være første gang. Disse elever kan med fordel arbejde videre med denne del i længere tid.
- Til udfordring 2: Der kan være stor forskel på bogstavers hyppighed alt efter emne. Læreren kan med fordel stilladsere grupperne valg af emner til galgelegen for at sikre mere brugbare resultater, fx ved at arbejde med ordsprog.

4.4 Særlige opmærksomhedspunkter

Dette forløb kræver ikke særlige tekniske forudsætninger eller særligt udstyr.