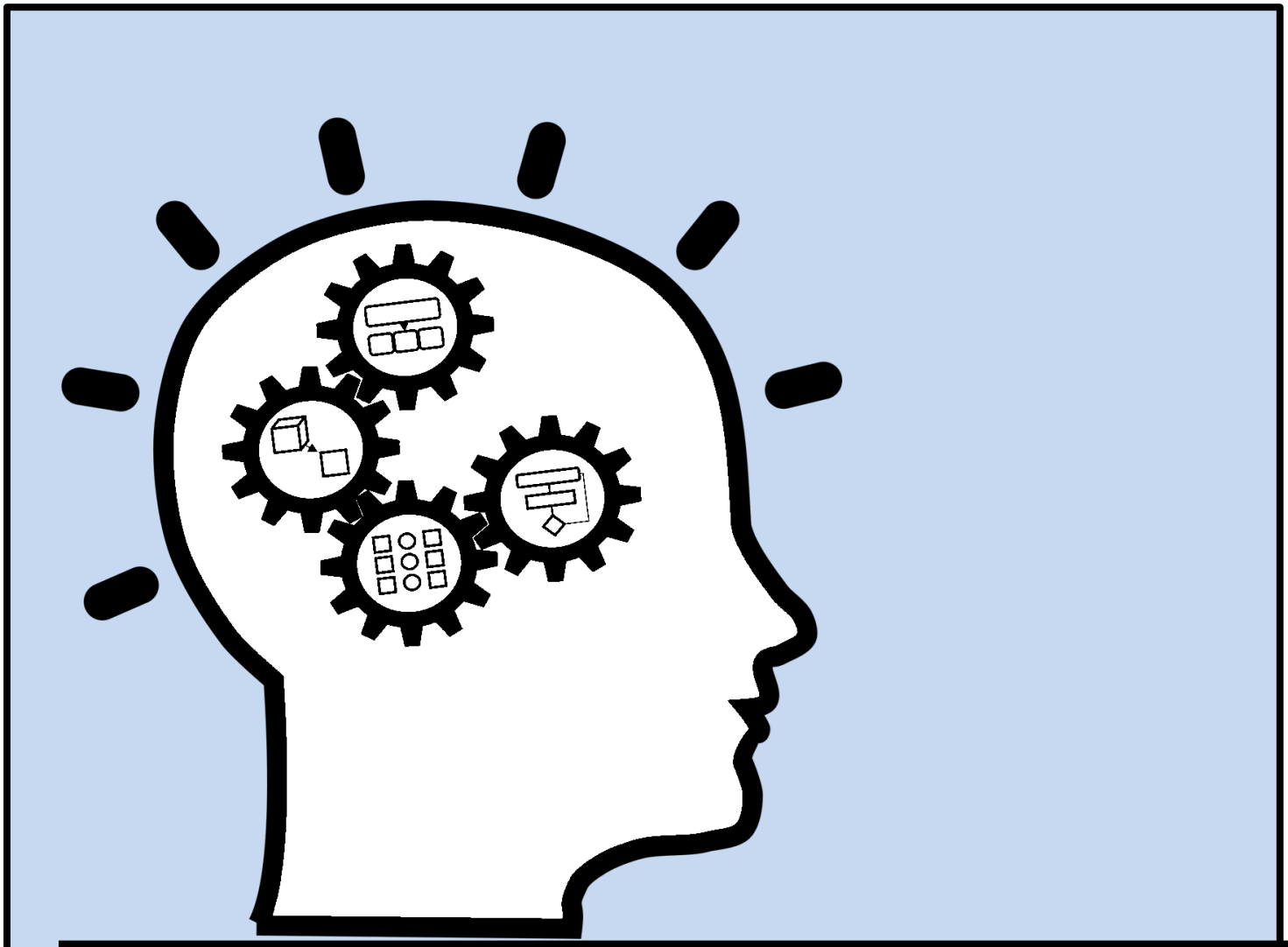


Computational Thinking Integration Guide for Secondary Education Teachers

Eksempelscenario

Version F.01

August 2022

CompuT
Computational Thinking at School
Erasmus+ KA201 Project: 2019-1-EL01-KA201-062883

Co-funded by the Erasmus+ Programme of the European Union

Computational Thinking Integration Guide for Secondary Education Teachers

Version F.01

Published by University of the Aegean – Laboratory of Learning Technology and Educational Engineering as deliverable of the “Computational Thinking at School” - “CompuT”, Erasmus+ KA201 project - Project Code: 2019-1-EL01-KA201-062883.

Authors:

Fesakis George, Prantsoudi Stavroula, Mavroudi Elisavet,
Volika Stamatia, Kefalas Ioannis

Learning Scripts edited by:

George Fesakis, Stavroula Prantsoudi, Elisavet Mavroudi, Konstantinos Zervas, Ioannis Kefalas, Georgia Papamargariti, Alexandra Papamargariti, Evangelia Stamatarou, Manuel Toro Casaucao, Kristine Feness, Monica Langeland, Sabine Lauw, Borghild Marie Opdahl, & Trude Sætveit

Learning Scripts Evaluations and Reflections by:

Anastasios Savas, Vasileios Kasapidis, Monica Langeland, Stavroula Prantsoudi,

August 2022

To cite this work:
Fesakis, G., Prantsoudi, S., Mavroudi, E., Volika, S., Kefalas, I. (2022). *Computational Thinking Integration Guide for Teachers* (5th ed.). Rhodes, Greece: University of the Aegean - LTEE Lab.

CompuT

Computational Thinking at School

Partners:

Directorate of Secondary Education in Dodecanese

University of the Aegean, Laboratory of Learning Technology and Educational Engineering (LTEE), Rhodes, Greece

2ο Upper Secondary School of Rhodes, "Kazoulleio", Rhodes, Greece

Secondary School of Gennadi, Rhodes, Greece

Secondary School of Zipari, Kos, Greece

CEP La Laguna, Tenerife, Spain

IES EL SOBRADILLO, Tenerife, Spain

Fyllingsdalen videregående skole, Bergen, Norway

Agrupamento de Escolas de São João da Talha, Lisbon, Portugal

Eksempelscenario 03: *Katter og hunder*

Del A. Generelle data	
A.1 Tittel:	***Katter og hunder***
A.2 Forfatter(e):	*Stavroula Prantsoudi , University of the Aegean*
A.3 Sammendrag/ Sammendrag:	*Smarte enheter, det vil si enheter som viser intelligens, omgir studenter i økende grad. Av denne grunn bør studenter forberedes på å bruke slik teknologi i sine fremtidige sosiale og profesjonelle liv. Disse enhetene bruker algoritmer som automatisk forbedres gjennom opplevelsen de bygger basert på eksempeldata. Algoritmene kan ta avgjørelser eller spådommer uten å være eksplisitt programmert til å gjøre det, og dette kalles Machine Learning (ML), en undergruppe av Artificial Intelligence (AI).* *Hensikten med dette scenariet er å introdusere elevene til de grunnleggende begrepene ML og AI. Etter en introduksjon til AI og grunnleggende AI-konsepter, blir studentene bedt om å bygge, trene og teste en maskinlæringsmodell. De diskuterer deretter AI-biasproblemet og prøver å finne årsaker og foreslå løsninger. For å utvide scenariet foreslås opprettelsen av en applikasjon ved hjelp av en ML-modell.* *Studentene forventes å bli kjent med grunnleggende konsepter for AI, lære å lage og bruke ML-modeller og øke bevisstheten deres om AI-etiske spørsmål, angående bruken av AI-applikasjoner i hverdagen, for eksempel algoritmisk skjevhet. De vil bli veiledet til å arbeide på en konstruktiv, samarbeidende måte, i grupper på 2, samtidig som de samhandler med hele klassen og læreren deres.* *Scenariet introduserer maskinlæringskonseptet og kan brukes i mange vitenskapelige felt og forskjellige fag, etter å ha blitt riktig modifisert.*
A.4 Nøkkelord:	*Maskinlæring, kunstig intelligens, bildegjenkjenning, AI-bias, programmering, Scratch*
A.5 versjon:	*Versjon 1*
A.6 Dato:	*20 /1 0 /202 1*
A.7 Opphavsrettslisens:	*Attribution ShareAlike CC BY-SA*
Del B. Læringsdata	
B.1 Karakter(er):	*Klasser 9-10 eller Alder: 14-15 år*
B.2 Emne(r):	***Datavitenskap***
B.3 Emne(r):	***Programmering, Maskinlæring, Bildegjenkjenning, Kunstig Intelligens, Algoritmisk skjevhet***

B.4 Computational Thinking Dimensjoner:

Algoritmisk tenkning (AL)	✓
Abstraksjon (AB)	✓
Generalisering (GE)	✓
Logisk resonnement (LR)	
Mønstertilpasning (PM)	✓
Problemnedbrytning (PD)	✓
Problemoversettelse (PT)	
Evaluering (EV)	✓
Representasjon (RE)	✓
Datainnsamling (DC)	✓
Datarepresentasjon (DR)	✓
Dataanalyse (DA)	✓
Modellering (MO)	
Simulering – (SIM)	
Automatisering (AUT)	
Sekvensering (SE)	
Testing (TE)	✓
Forstå mennesker – (UP) / Kunstig intelligens (AI)	✓

B.5 Computational Thinking-tilnærminger:

Triksing eksperimenterer og leker	✓
Å skape, designe og lage	✓
Feilsøking, finne og fikse feil	✓
Utholdende, fortsetter	✓
Samarbeid og samhandling	✓

B.6 Tematisk i sammenheng med CompuT-prosjektet:

Pedagogisk robotikk eller fysisk databehandling		
Computational Science-prosjekt	Modellering/Simulering	
	Bifokal modellering	
	Bruk av sensorer	
	Matematikk og CS	
	Annet: …	
Datavitenskapsprosjekt	✓	
Vitenskapens og teknologiens historie		
Digitalt spill, programvare eller mobilapp	✓	
Digitale humanistiske prosjekter	Digital historiefortelling	
	Interaktiv fiksjon	
	Tekstutvinning	
	Algoritmer i hverdagen	✓
	Annet: …	
Kunstig intelligens-prosjekter	✓	
Studiotilnærming – Future Classroom-prosjekter		
Unplugged erfaringsmessig eller ved hjelp av manipulasjoner		
Annet: ….		

B.7 Hensikt/mål med læringsscenarioet:	*Hensikten med læringsscenarioet er å gjøre elevene kjent med konseptet maskinlæring og kunstig intelligens generelt. Studentene er omgitt av enheter som bruker maskinlæring (chatbots, digitale plattformer, sosiale medieplattformer, beslutningsalgoritmer, prediksjonsalgoritmer osv.) og å utdanne dem i måten disse enhetene fungerer på er viktig for fremtidige samfunnsborgere. Etter å ha fullført scenariet, vil elevene ha fått forståelse for hvordan algoritmer bruker dataene de får til å ta avgjørelser og spådommer, og intelligensen som maskinene viser vil bli forklart og avslørt. De vil også være klar over de mange samfunnsmessige og etiske spørsmålene som reises på grunn av algoritmisk skjevhet.*	
B.8 Læringsutbytte/mål [1]:	*Følgende mål forventes å ha blitt oppnådd etter at scenariet er fullført:*	
	B.8.1 Kunnskap	● Studentene vet hvordan kunstig intelligens er innebygget i i systemer. ● Studentene vet hvordan maskinlæringsmodeller bygges og brukes til å definere atferden til maskiner og systemer. ● Studentene vet om betydningen av egne beslutninger om opplæring av modellene som algoritmene bruker.
	B.8.2 Ferdigheter	● Studentene kan trene en maskinlæringsmodell (ta avgjørelser om gruppene med data og kategorisere data i riktig gruppe). ● Studentene kan teste/evaluere en maskinlæringsmodell. ● Elever kan importere en maskinlæringsmodell til en algoritme. ● Studentene kan bygge en algoritme (som bruker en maskinlæringsmodell) for å ta beslutninger. ● Studentene kan endre en algoritme (som bruker en maskinlæringsmodell) for å ta avgjørelser.
	B.8.3 Holdnings-affektiv	● Elevene har utviklet samarbeidsevner. ● Studentene har fått kunnskap om maskinlæringskonsepter. ● Elevene har fått forståelse for hvordan maskiner og algoritmer i hverdagen bruker data til å handle intelligent (vise kunstig intelligens). ● Elevene har fått kunnskap om hvordan han/hun kan påvirke oppførselen til en algoritme ved å gi den visse data. ● Studentene har økt bevisstheten om problemer med algoritmiske skjevheter og metoder for å forhindre det.
B.9 Horisontale		

[1] For effektiv formulering av lærings-instruksjonsmål kan arbeidene til Mager , som krever definisjonen av observerbare handlinger og målbare kriterier for ytelsesevaluering under spesifikke forhold, være nyttige. Mager , F. (1975). Forberede instruksjonsmål. (2. utgave). Belmont, CA: Fearon. & Mager , F. (1997). Utarbeidelse av instruksjonsmål: Et kritisk verktøy i utviklingen av effektiv instruksjon. Atlanta: Senter for effektiv ytelse. Verbene kunne følge Blooms kunnskapstaksonomi, se for eksempel: https://tips.uark.edu/blooms-taxonomy-verb-chart/. Det er viktig å bruke høyere ordens tenkeverb. Anderson, LW, & Krathwohl, DR (2001). En taksonomi for læring, undervisning og vurdering, forkortet utgave. Boston, MA: Allyn og Bacon

kompetanser - ferdigheter i det 21. århundre:	**B.9.1 Lærings- og innovasjonsferdigheter:**	***Samarbeid** : elevene jobber i grupper på 2 og samarbeider* ***Kommunikasjon** : studentene skal kommunisere med andre grupper for å teste resultatene deres* ***Kritisk Tenkning** : elevene må tenke kritisk for å ta beslutninger om bildene og klassene de skal bruke for å trene modellene sine* ***Kreativitet** : elevene forventes å forbedre algoritmen sin ved å endre kostymer, lyder og uttrykk*
	B.9.2 Digitale ferdigheter:	***Informasjonskompetanse** : Elever evaluerer informasjon for å trene maskinlæringsmodellen deres* ***Informasjons- og kommunikasjonsteknologi (IKT) kompetanse** : studentene vil kunne trene en maskinlæringsmodell og bygge en algoritme i en populær programmeringsplattform (Scratch)* ***Digitalt medborgerskap** : studentene er klar over begrepet maskinlæring og måten det brukes på i ulike felt av hverdagen. De er også klar over problemet med AI-bias.*
	B.9.3 Karriere og livsferdigheter:	***Fleksibilitet og tilpasningsevne** : Studentene kan være fleksible og tilpasse dataene sine for å trene modellen deres til å reagere i nye tilfeller* ***Initiativ og selvledelse** : studentene skal ta avgjørelser selv, men også bidra til at gruppen kommer med et resultat* ***Sosialt og tverrkulturelt samspill** : elevene bør samhandle med andre grupper og teste resultatene deres* ***Produktivitet og ansvarlighet** : Studentene bør prøve å produsere det beste resultatet i løpet av den tiden som er gitt, og få algoritmen til å fungere for maksimalt antall tilfeller.*
B.10 Moderne undervisningsmetoder:	*Studentene jobber i grupper på 2 basert på et Collaborative Inquiry script. De forventes å lære ved å kode, på en prosjektbasert måte.*	
B.11 Integrasjon av CT i læreplanen:	*Scenariet, avhengig av maskinlæringsmodellen som brukes, kan kombineres med mange vitenskapsfelt når det gjelder tverrfaglighet. Den nåværende implementeringen kategoriserer bilder, slik at den kan brukes til å kategorisere dyr, bøker, resirkuleringsmateriale, kjøretøy, maskiner osv. for å kombinere med vitenskap, sosiologi, miljøundervisning, historie etc.* *En annen modell kan kategorisere tekst for å kombinere med språk og psykologi (f.eks. kategorisering av følelser i henhold til ordene som brukes). En modell som kategoriserer lyd kan også brukes til å kombinere med musikk, kunst, dans eller et hvilket som helst annet emne.*	
B.12 Forhold til læreplan og/eller standarder:	*Gresk nasjonal læreplan, klassetrinn 9-10, informatikk.* *Enhver annen alder og/eller fag i tverrfaglig implementering.*	
B.13. Forkunnskaper:	*Studentene må ha grunnleggende kunnskap om nettsøk og filbehandling. Scratch-programmering vil være nødvendig for implementeringen av utvidelsen.*	

<table>
<tr><td>B.14. Vanskelighetsgrad for scenariet:</td><td colspan="2">Medium</td></tr>
<tr><td>B.15. Sosial setting av scenariet:</td><td colspan="2">Par (2 elever), eller individuell</td></tr>
<tr><td>B.16 Sted for implementering:</td><td colspan="2">Datalab</td></tr>
<tr><td>B.17 Undervisningstid – Varighet:</td><td colspan="2">3 x 45' økter (eller 1x45' + 1x90')</td></tr>
<tr><td rowspan="4">B.18 Utdanningsmateriell, ressurser, instrumenter, verktøy og medier:</td><td>B.18.1 Programvare:</td><td>Scratch, nettleser
https://teachablemachine.withgoogle.com/
https://dancingwithai.media.mit.edu/
https://machinelearningforkids.co.uk/</td></tr>
<tr><td>B.18.2 Maskinvare:</td><td></td></tr>
<tr><td>B.18.3 Nettressurser:</td><td>https :// teachablemachine . med google . no /
https :// dancingwithai . media . mit . edu /
https://machinelearningforkids.co.uk/
Payne, BH & Breazeal, C. (2019). En læreplan for etikk for kunstig intelligens for ungdomsskoleelever . MIT Media Lab.</td></tr>
<tr><td>B.18.4 Konvensjonelt undervisningsmateriell :</td><td></td></tr>
<tr><td colspan="3"><u>Del C. Design for læringserfaring</u></td></tr>
<tr><td>C.1. Aktiviteter-Handling-Plot-Storyboard-sekvenstabell:</td><td colspan="2">
<table>
<tr><th>Fase 1.</th><th>Fasetittel : Introduksjon og utforskning</th><th></th></tr>
<tr><th>Aktivitet/Oppgave</th><th>Beskrivelse/Prosedyre</th><th>Varighet</th></tr>
<tr><td>A1.1 Oppvarming – Introduksjon til AI – AI-definisjonen</td><td>Læreren deler arbeidsark 1 og følger retningslinjene på det med klassen.

De diskuterer begrepet intelligens generelt, definisjonen av kunstig intelligens og dets tilstedeværelse i hverdagen. Elevene svarer på spørsmålene på arbeidsarket.
De ser på video https://www.youtube.com/watch?v=nASDYRkbQIY (Hva er kunstig intelligens? | The Royal Society) og diskuter om det.</td><td>1 5 min.</td></tr>
</table>
</td></tr>
</table>

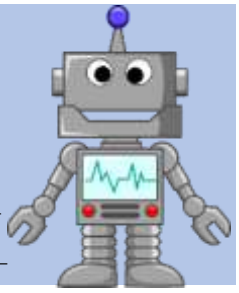
	A1.2 Anvendelser av AI	*Læreren veileder elevene til å liste opp anvendelser av AI og deres daglige bruk, han/hun veileder dem til å bruke noen av dem og foreslå andre, kategorisere dem basert på et konseptuelt kart og søke etter flere eksempler for hver kategori. Elevene ser også en video https://www.youtube.com/watch?v=3wLqsRLvV-c (Turing-testen: Kan en datamaskin bestå for et menneske?) og diskuterer den berømte Turing-testen.*	*3 0 min*
	Fase 2.	**Fasetittel: Utvikling og evaluering**	
	Aktivitet/Oppgave	**Beskrivelse/Prosedyre**	**Varighet**
	A2.1 AI-konsepter - maskinlæring og datainnsamling	*Læreren deler **arbeidsark 2** . Han/hun oppfordrer studentene til å lure på om det er en måte å lære en maskin å gjenkjenne **bilder** og skille mellom katter og hunder (Diskusjon). Basert på arbeidsarket samler elevene inn dataene de trenger for å bygge en modell av den grunn.*	*10 min _*
	A2.2 Bygg, tren og evaluer en maskinlæringsmodell	*Etter retningslinjene bygger elevene en maskinlæringsmodell i den foreslåtte plattformen https://teachablemachine.withgoogle.com/ . De trener, tester og evaluerer modellen sin og legger til nye eksempler/data om nødvendig.*	*30 min*
	A2.3 Vurdering	*Læreren deler vurderingsarket 2.1 og ber elevene svare på spørsmålene for å reflektere over byggingen av ML-modeller*	*5 min*
	Fase 3 .	**Fasetittel: AI-etiske spørsmål**	
	Aktivitet/Oppgave	**Beskrivelse/Prosedyre**	**Varighet**
	A3.1 Øke bevisstheten om AI-etiske spørsmål og bekjempe dem	*Læreren veileder en diskusjon om de etiske og samfunnsmessige spørsmålene som oppstår*	*45 min*

		ved bruk av AI. ***Arbeidsark 3*** *inneholder noen spørsmål og foreslåtte videoer for å starte en slik diskusjon. Læreren kan tilpasse innholdet i arbeidsarket (videoer og spørsmål) til hver klasse, alltid med sikte på å øke elevenes bevissthet om de kritiske spørsmålene om AI-etikk og sikkerhet.* *Varighet på økten og lengden på diskusjonen kan også tilpasses etter lærernes vilje.*	
C.2 Vurdering			
	C.2.1 Elevens tilbakemeldinger og refleksjon	*Studentene skal teste og evaluere sin ML-modell og sammenligne resultater i sanntid. De vil også fylle ut vurderingsarket.* *Modellene deres vil bli vurdert av klassekameratene og omvendt.*	
C.3 Lekser/ Arbeid med foreldre-familie	*Elevene kan bygge ML-modellene sine hjemme og teste dem med ekte data (som deres egne kjæledyr). De kan også diskutere med foreldrene og familien for å finne AI-applikasjoner de allerede bruker, og foreslå nye.* *Læreren kunne velge og tilordne en utvidelse til hvert team som lekser.*		
Del D. Informasjon til lærerne			
D.1 Tilpasning - Differensiering for inkludering av alle elever	*Konstruksjonen kan tilpasses til tilgjengelig undervisningstid. Det foreslås 3 økter á 45 min. I tilfelle dette ikke er mulig, foreslås det at lærerne implementerer scenariet i 1 økt på 45 min, og 1 økt på 90 min.* *Alle studenter i allmennutdanning kunne implementere scenariet uten begrensninger.*		

<table>
<tr><td>D.2 Forlengelse</td><td>En utvidelse av scenariet kan være bygging av en applikasjon i Scratch som benytter seg av en ML-modell. Arbeidsark 4 kan brukes av denne grunn, men ikke begrensende.
<table>
<tr><th>Faseforlengelse.</th><th>Fasetittel: Bruke intelligens til å bygge noe nyttig</th></tr>
<tr><td>AE.1 Bygg en applikasjon (en algoritme for å handle intelligent)
(35 min)</td><td>Læreren deler arbeidsark 4 og elevene følger retningslinjene. Elevene bygger en algoritme for å bygge inn en ML-modell de tidligere har laget.
De bruker https://machinelearningforkids.co.uk/-plattformen og Scratch-programmering. De blir bedt om å studere eksemplene og prøve å bygge en modell og en algoritme for å spille stein, papir, saks med datamaskinen.</td></tr>
<tr><td>AE.2 Evaluer algoritmen din (test applikasjonen din)
(10 min)</td><td>Etter at de har bygget applikasjonen, blir studentene bedt om å teste den og gjøre mulige endringer. De hjelper også til med å teste, evaluere og endre klassekameratenes søknader.</td></tr>
</table></td></tr>
<tr><td>D.3 Ressurser</td><td>https :// teachablemachine . med google . no /
https :// dancingwithai . media . mit . edu /
https://machinelearningforkids.co.uk/</td></tr>
<tr><td>D.4 Erfaring fra implementeringen av scenariet</td><td></td></tr>
<tr><td>D.5 Forhold til andre scenarier</td><td>Payne, BH & Breazeal, C. (2019). En læreplan for etikk for kunstig intelligens for ungdomsskoleelever . MIT Media Lab.</td></tr>
<tr><td>D.6 Anmeldelser av lærere</td><td></td></tr>
<tr><td>D.7 Vurdering av scenario</td><td>[1=Veldig dårlig – 5=Veldig bra]</td></tr>
<tr><td>D.8 Referanser</td><td>Payne, BH & Breazeal, C. (2019). En læreplan for etikk for kunstig intelligens for ungdomsskoleelever . MIT Media Lab.</td></tr>
<tr><td colspan="2">Del E. Vedlegg</td></tr>
<tr><td></td><td>Regneark 1, regneark 2, regneark 2.1, regneark 3, regneark 4</td></tr>
</table>

Maskinlæring _ Arbeidsark 1

Introduksjon til AI - AI-konsepter



Elevens navn(e): _____

Gruppenavn: _____

Dato: _____

I dag vil du lære om kunstig intelligens og hvor tilstede den er i vår hverdag.

A. Definisjon av AI

A. Svar kort på følgende spørsmål. Diskuter deretter svarene dine med klassekameratene dine og læreren din:

1. Hva er intelligens?

_____

_____

2. Når anses et menneske for å være intelligent?

_____

_____

3. Kan andre skapninger være intelligente? Hvordan vet du når det skjer?

_____

_____

4. Kan maskiner opptre intelligent? Hvilke maskiner kan gjøre det?

_____

_____

5. Hvordan tror du intelligent atferd kan oppnås med maskiner?

_____

_____

6. Hva er **kunstig intelligens** ?

_____

_____

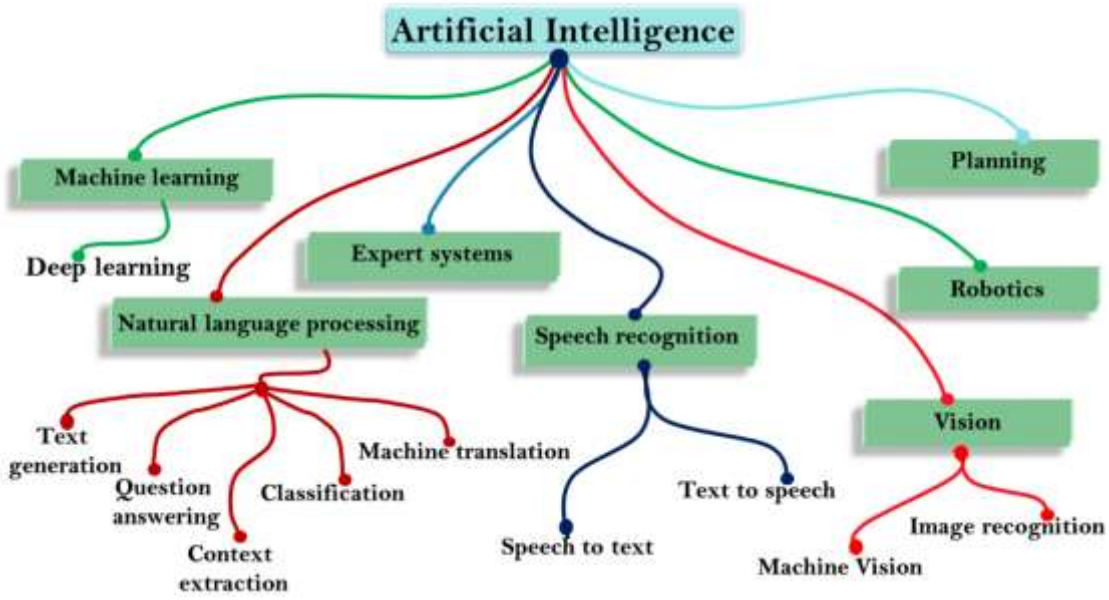
7. Se videoen på følgende lenke https://www.youtube.com/watch?v=nASDYRkbQIY (*Hva er kunstig intelligens?* | *The Royal Society*). Gå tilbake til svaret du ga på spørsmål 6 og diskuter det med klassekameratene og læreren.

B. Anvendelser av AI

B. Diskuter i hvilken grad følgende applikasjoner bruker AI.

a. En chat-bot
b. Søkemotorer
c. Autonome kjøretøy
d. Roboter
e. Sosiale medier
f. Et oversettelsessystem
g. Online annonser
h. Virtuelle assistenter (Siri, Alexa)

1. Bruk følgende applikasjoner og diskuter funksjonene deres med klassekameratene dine:
   a. Google Chromes tale til tekst
   b. WHO Health Alert chat-bot, https://www.who.int/
   c. Photomath - applikasjonen, https://photomath.com
2. Bruk følgende konseptuelle kart, søk på nettet for å finne et eksempel på en applikasjon i hverdagen, for hver kategori (gren) på kartet. Diskuter eksemplene du fant med klassekameratene dine og læreren din.



3. Se videoen på følgende link https://www.youtube.com/watch?v=3wLqsRLvV-c (Turing-testen: Kan en datamaskin erstatte et menneske?). Diskuter Turing-testen med klassekameratene og læreren din.
4. Er det noen risiko forårsaket av bruk av AI? Hvilke kan de være?

   _____

   _____
5. Foreslå måter å eliminere mulige farer (hvis noen) forårsaket av bruk av AI. Diskuter forslaget ditt med klassekameratene dine og læreren din.

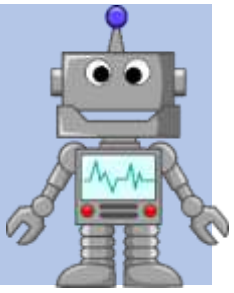
Godt jobbet!

Så langt har du lært om definisjonen av kunstig intelligens og dens bruk i hverdagen.

Deretter vil du lære om grunnleggende AI-konsepter og fokusere på maskinlæring.

Maskinlæring _ Arbeidsark 2

Bygg en AI-modell



Elevens navn(e): _____

Gruppenavn: _____

Dato: _____

I dag skal du lære en datamaskin å bestemme om et bilde viser en katt eller en hund.

Svar på følgende spørsmål for å varme opp:

A. Kan en datamaskin gjenkjenne dyr (**JA** eller **NEI)** ? _____

B. Hvis **JA** , hvordan skjer det?

_____

_____

C. Hvis **NEI** , kan vi lære en datamaskin å gjenkjenne dyr?

_____

_____

Datamaskiner tar avgjørelser ved hjelp av **algoritmer** og **data** som folk har gitt dem. Dette kalles **Machine Learning** .

Du vil nå lære en datamaskin å **klassifisere** katter og hunder ved å lage en **modell** .

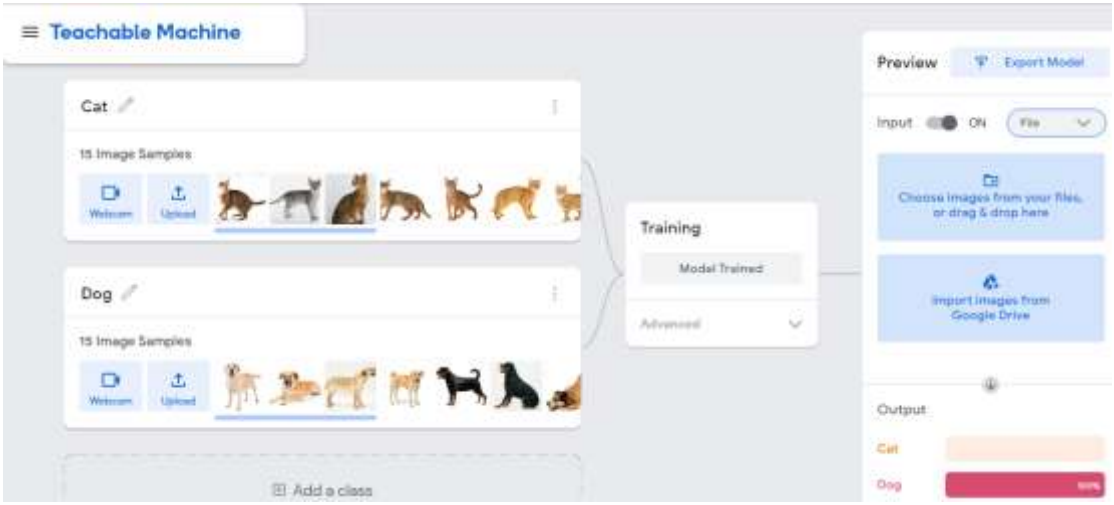
A. Bygg din modell

1. Lag to mapper på datamaskinen og gi dem navnet **Cats** og en annen som heter **Dogs** . Søk på nettet og samle bilder fra katter og hunder (minst 10-15 av hver kategori) og lagre dem i riktig mappe. Sørg for at det er variasjon og mangfold på bildene du valgte.
2. Åpne en nettleser og gå til https://teachablemachine.withgoogle.com/
3. Klikk på **"Kom i gang"** . Du vil opprette et nytt bildeprosjekt, så klikk videre den og velg **Standard bildemodell** i popup-vinduet.

4. Gi navn til de to klassene **Katt** og **Hund** og last opp bildene du har samlet i den aktuelle klassen.

B. Tren modellen din

1. Klikk på **Tren din modell** og vent. Datamaskinen trenger kanskje noen minutter for å trene modellen din. **Vær tålmodig!** Etter at opplæringen er fullført, skal modellen din se ut som den nedenfor:



2. For å **forhåndsvise** resultatene til modellen din, bruk de tilgjengelige alternativene til høyre (webkameraet eller en ny fil).
    a. På Cats-datasettet, hvilke forskjeller og likheter er det mellom kattene?
    b. Hvilke forskjeller og likheter er det mellom hundene i datasettet Dogs?
3. Tenk på tilfeller av dyr du kanskje ikke har inkludert i modellen din. Du kan alltid gå tilbake til modellen din, legge til eksempler og trene den på nytt.

C. Test modellen din

1. Opprett en ny mappe og samle inn noen **testdata** , for eksempel bilder av katter og hunder som du ikke har inkludert i eksemplene du brukte for å trene modellen. Samle også bilder av andre dyr (som løve, bjørn, rev, koala osv.). Lag et sett med testdata som ligner på det nedenfor:

2. Test bildene du har samlet på modellen din (importer eller dra og slipp hvert bilde). Maskinen vil fortelle deg hva den gjenkjenner, samt hvor sikker den er. (Du kan også slå på webkameraet og teste modellen med trykte bilder). Er **utgangen** riktig?
3. For hvert bilde av testdatasettet ditt, skriv ned resultatene som i tabellen nedenfor. Kan du forklare hvert resultat? Hvorfor tror modellen for eksempel at løven er en katt?

Bilde	Klasse	Selvtillit	Resultat
Løve	Katt	82 %	Feil

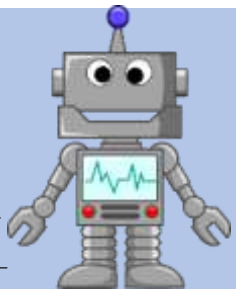
4. Be noen av klassekameratene dine hjelpe deg med å teste modellen din. Bytt ut testdatasettet med klassekameratene dine og test dataene deres på modellen din og omvendt. Er resultatene like? Hvorfor hvorfor ikke?
5. Er du fornøyd med svarene? Hvis ikke, ikke glem at du kan gå tilbake til modellen og legge til noen flere eksempler. Tren alltid modellen din igjen, etter at du har lagt til eksempler.
6. Hva synes du bør skje slik at modellen gjenkjenner andre dyr enn hunder og katter? Tror du du kan lage en modell som gjenkjenner ethvert dyr på planeten?
7. Klikk på **Last ned prosjekt som fil** og lagre prosjektet.

Godt jobbet!

Så langt har du trent datamaskinen din til å gjenkjenne bilder som katter eller hunder, og dermed har du trent en **maskinlæringsmodell** ved å mate den med eksempler. Du kan nå fortsette å lage noe mer morsomt og nyttig ved å bygge inn modellen din i en applikasjon.

Maskinlæring _ Arbeidsark 2.1

evaluering



Elevens navn(e): _____

Gruppenavn: _____

Dato: _____

Siden du har lært hvordan du bygger en maskinlæringsmodell, bør du nå kunne forutsi oppførselen til en modell basert på datasettene som brukes til opplæringen. Se på bildene og datasettene nedenfor og prøv å svare på følgende spørsmål:

1. En maskinlæringsmodell har blitt trent med følgende treningsdata:

Klasse	**Bilder**
Katt	

Hva tror du modellen vil resultere i hvis du importerer følgende bilde?

Hund ELLER **katt?**

2. En maskinlæringsmodell har blitt trent med følgende treningsdatasett:

Klasse	**Bilder**
Katt	
Hund	

Hvilken av følgende setning(er) er riktig, angående resultatene av modellen:

- **i.** Resultatene vil være mer presise for hundene
- **ii.** Resultatene vil være mer presise for kattene
- **iii.** Resultatene vil være like presise for hundene og kattene

3. Hvilket av følgende treningsdatasett vil gi mer presise resultater? Hvorfor ?

A .

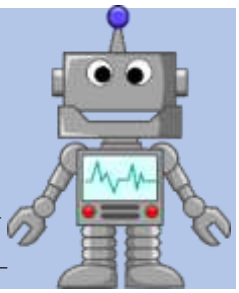
Katt	Hund
	

B.

Katt	Hund
	

Maskinlæring _ Arbeidsark 3

AI-etikk/sikkerhet



Elevens navn(e): _____

Gruppenavn: _____

Dato: _____

Kunstig intelligens (AI) har erobret våre liv og bruken av kunstig intelligens er nesten uunngåelig. Sammen med de mange fordelene, blir øker også bekymringer dag for dag. I dag vil du lære om de samfunnsmessige og etiske problemene som oppstår ved bruk av kunstig intelligens, de mulige farene og hvordan vi kan forholde oss til dem.

TIPS: Før du ser på hver av de følgende videoene, se på spørsmålene som følger 😉

Etikk og AI

Diskuter følgende spørsmål med klassekameraten din og læreren din:

1. Finnes det et kunstig intelligenssystem som vil fungere i alle tilfeller?
2. Tror du ML-systemer alltid er riktige/rettferdige?

Se følgende video: https://www.youtube.com/watch?v=tJQSyzBUAew (Ethics & AI: Equal Access and Algorithmic Bias)

3. Hva er de mulige farene ved å bruke AI? Hvordan kan de påvirke mennesker og samfunn?
4. Hva bør folk og/eller industrien gjøre for å unngå slike problemer?

Se følgende video: https://www.youtube.com/watch?v=BtgcuhQ0cks (Bias in AI is a Problem)

5. Hva er årsakene til skjevheter på algoritmer?
6. Kan du gi noen eksempler på algoritmer som kan ha vært partiske?
7. Hvordan kan slike funksjonsfeil forhindres?

Besøk https://www.ajl.org/ , nettstedet til Algorithmic Justice League-initieringen, et forsøk på en rettferdig og ansvarlig AI. Bla gjennom nettstedet for å:

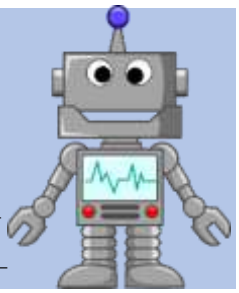
8. Nevn to eksempler der partisk AI påvirket virkelige menneskers liv.
9. Foreslå handlinger for bedre AI.

Gratulerer!

Du har offisielt blitt en AI-ekspert!

Maskinlæring _ Arbeidsark 4

AI-applikasjoner



Elevens navn(e): _____

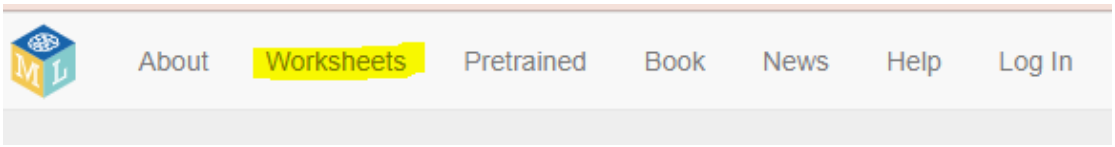
Gruppenavn: _____

Dato: _____

Etter at du er ferdig med **å trene modellen din**, er det på tide at du bruker den til å gjøre noe mer morsomt og brukervennlig. Du kan tenke på og lage hvilken som helst applikasjon som kan være nyttig i hverdagen din eller endre og bruke noen av de eksisterende.

Bygg en applikasjon

1. Besøk https://machinelearningforkids.co.uk/ , et annet nettsted hvor du kan bygge og trene en maskinlæringsmodell. Klikk på Regneark-menyen og bla gjennom de forskjellige maskinlæringsprosjektene. Er de ikke fantastiske?



2. Etter å ha bla gjennom de forskjellige prosjektene, velg **Rock, Paper, Scissors** og last ned regnearkene. Du vil bli guidet til å lage et program i Scratch for å spille spillet med datamaskinen.

3. Følg trinnene på regnearket for å lære en modell å gjenkjenne hånden din som stein, papir eller saks. Bruk deretter modellen og programmer en applikasjon i Scratch for å spille spillet med datamaskinen.

✓ Du kan alltid komme tilbake til modellen din for å legge til flere eksempler.

✓ Du kan bruke hvilket som helst prosjekteksempel du ønsker og endre det for å lage din egen applikasjon. Fremfor alt, se på den morsomme siden av AI.

Godt jobbet!

Du kan nå trene en maskinlæringsmodell og bygge en applikasjon for å bruke den.

Gratulerer!

Exemplar Scenario 04: *Cryptography*

Part A. General Data	
A.1 Title:	*Cryptography*
A.2 Author(s):	*Zervas Konstantinos, Fesakis Georgios - University of the Aegean*
A.3 Abstract/ Summary:	*The study of techniques used to secure communication, a major necessity these days, is called cryptography. Since ancient times, many cryptography methods have been used to protect communication. Students should be aware of these methods and techniques and be able to use them accordingly, when needed. This scenario is an introduction to the so-called symmetric cryptography methods such as Morse, Braille, and Caesar Cipher. It also introduces students to asymmetric cryptography based on the Public Key Encryption concept. Additionally, through various extensions, students may be given the chance to explore the enigma machine, the RSA algorithm, as well as the various applications of PKE. It intends to teach methods and practices of encrypting and decrypting messages, in both an unplugged and a simulated way through educational software, so that students may gain understanding and knowledge of the concept of cryptography.*
A.4 Keywords:	*Cryptography, encryption, decryption, symmetric/asymmetric cryptography, Caesar cipher, Morse, Braille, Enigma machine, (Public Key Encryption (PKE), RSA, Digital Signature, Certificate Authorities)*
A.5 Version:	*Version 1*
A.6 Date:	*05/11/2021*
A.7 Copyright license:	*Attribution ShareAlike CC BY-SA*
Part B. Learning Data	
B.1 Grade(s):	*Grades 8-10, or Age(s): 13-15 years old*
B.2 Subject(s):	*Computer Science*
B.3 Topic(s):	*Cryptography, security, encryption, decryption*

B.4 Computational Thinking Dimensions:

Algorithmic Thinking (AL)	
Abstraction (AB)	✓
Generalization (GE)	✓
Logical reasoning (LR)	✓
Pattern matching (PM)	✓
Problem decomposition (PD)	
Problem translation (PT)	
Evaluation (EV)	
Representation (RE)	✓
Data collection (DC)	
Data representation (DR)	
Data analysis (DA)	
Modeling (MO)	
Simulation – (SIM)	
Automation (AUT)	
Sequencing (SE)	
Testing (TE)	✓
Understanding People – (UP) /Artificial Intelligence (AI)	✓

B.5 Computational Thinking Approaches:

Tinkering experimenting & playing	✓
Creating, designing, and making	
Debugging, finding, and fixing errors	✓
Persevering, keeping going	
Collaborating, working together	✓

B.6 Thematic in the context of the CompuT Project:

Educational Robotics or Physical Computing		
Computational Science project	Modeling/Simulation	
	Bifocal modelling	
	Sensors use or making	
	Maths and CS	
	Other: …	
Data science project	✓	
History of science and technology	✓	
Digital game, software, or mobile app		
Digital humanities projects	Digital Storytelling	
	Interactive Fiction	
	Text mining	
	Algorithms in everyday life	✓
	Other: …	
Artificial Intelligence Projects		
Studio approach – Future Classroom projects		

	Unplugged experiential or using manipulatives	✓
	Other: ….	
B.7 Purpose/Aim of the learning scenario:	*The purpose of the scenario is to help students become familiar with the concept of cryptography and various methods of encrypting and decrypting messages. Students will then be able to protect their data by using various cryptographic methods to send and receive messages in the ever-evolving age of technology.*	
B.8 Learning outcomes/goals[2]:		
	B.8.1 Knowledge	*Students demonstrate understanding about cryptography.* *Students explain the need to encrypt and decrypt messages in this ever-evolving technological era.* *Students illustrate examples of online threats while conducting communication.* *Students compare some basic, widely used cryptography methods.*
	B.8.2 Skills	*Students can apply Morse signals to encrypt/decrypt a message.* *Students can make use of Braille signs to*

2 For effective formulation of learning-instructional goals Mager's work regarding the definition of observable actions and Measurable Criteria of performance evaluation under specific conditions, could be useful. Mager, F. (1975). Preparing Instructional Objectives. (2nd ed.). Belmont, CA: Fearon. & Mager, F. (1997). Preparing instructional objectives: A critical tool in the development of effective instruction. Atlanta: The Center for Effective Performance. The verbs could be in accordance to Bloom's knowledge taxonomy, see for example: https://tips.uark.edu/blooms-taxonomy-verb-chart/. It is important to use higher order thinking verbs. Anderson, L. W., & Krathwohl, D. R. (2001). A taxonomy for learning, teaching, and assessing, Abridged Edition. Boston, MA: Allyn and Bacon

		encrypt/decrypt a message. *Students can apply the Caesar cipher key to encrypt/decrypt a message.* *Students can experiment encrypting /decrypting a message using a simulation of Enigma machine.* *(If the extensions are implemented:* *Students can apply asymmetric methods for encrypting/decrypting messages (RSA, digital signatures).* *Students can create a new method to encrypt/decrypt a message to securely communicate with a friend.)*
	B.8.3 Attitudes-affective	*Students identify the need of protecting messages by encrypting them.* *Students have become conscious on security matters.* *Students can collaborate to find ways to securely communicate with their friends.*
B.9 Horizontal competences - 21st century skills:		
	B.9.1 Learning and innovation skills:	***Collaboration**: students work in groups of 2 and collaborate* ***Communication**: students will communicate with other groups to test their encrypted messages* ***Critical Thinking**: students need to think critically to make decisions on the ways they will encrypt their messages* ***Creativity**: students are expected to think of new methods to encrypt/decrypt their messages*
	B.9.2 Digital literacy skills:	***Information literacy**: students evaluate information in order to select the appropriate method for their encryption/decryption method* ***Digital citizenship**: students are aware of the concept of cryptography and the various ways it is used in fields of everyday life*
	B.9.3 Career and life skills:	***Flexibility and adaptability**: students should be flexible and adapt their encryption/decryption method according to the data given* ***Initiative and self-direction**: students should make decisions by themselves but also contribute to the group to come up with the result* ***Social and cross-cultural interaction**: students should interact with other groups and test their results*
B.10 Modern teaching methods:	*Collaborative learning*	

B.11 Integration of CT into the curriculum:	*Cryptography is an example of art combined with science, where Informatics has caused a radical transformation, with social implications for all citizens. The computational problem-solving method is clearly seen in the case of cryptanalysis.* *The scenario can be combined with many subjects depending on the message to be handled each time.*	
B.12 Relation to curriculum and/or standards:	*Greek National Curriculum, Grades 8-10, Computer Science Curriculum*	
B.13. Prerequisite knowledge:	*No prior knowledge needed to successfully implement the current scenario.*	
B.14. Difficulty Level of the Scenario:	*Intermediate*	
B.15. Social setting of the scenario:	*Individual or pair (2 students)*	
B.16 Place of implementation:	*Classroom or Computer Lab*	
B.17 Teaching time – Duration:	*4 x 45' sessions*	
B.18 Educational material, resources, instruments, tools, and media:	**B.18.1 Software:**	For the extensions' purposes: https://travistidwell.com/jsencrypt/demo/, https://www.devglan.com/onlinetools/rsa-encryption-decryption https://8gwifi.org/rsafunctions.jsp https://www.cryptool.org/en/
	B.18.2 Hardware:	
	B.18.3 Online resources:	*Youtube videos*
	B.18.4 Conventional educational material:	

Part C. Learning Experience Design

C.1. Activities-Action-Plot-Storyboard sequence table:

Phase 1.	***Introduction and exploration: Morse code, steganography***	
Activity/Task	**Description/Procedure**	**Duration**
A1.1 The need of cryptography – Warm up	*The teacher discusses the need of protecting personal data from others in various instances of everyday life (e.g. transfer of private data like usernames and passwords, credit card credentials etc.) The danger of unauthorised access to*	*10 minutes*

		this data is discussed with the students and they are asked to propose methods to protect their data from third parties. • *Which personal data would you like to protect?* • *Who do you think would want to steal your data?* • *Can you think of a way to protect your communication from third parties?* *They come up with the idea of cryptography.* *They discuss its use since ancient times.*	
	A1.2 Cryptography methods: The Morse code and steganography	*Students are divided in groups of 2.* *They are introduced to Morse code and steganography.* ***Worksheet 1*** *is shared to them, and the Morse code is discussed. Students are asked to encrypt a message using the Morse code and decrypt one using the same technique. They are also asked to decrypt a message from a picture (steganography).*	*35 minutes*
	Phase 2.	**Exploration: Braille code**	
	Activity/Task	**Description/Procedure**	**Duration**
	A2.1 Warm up – linking to earlier discussed	*Teacher and students deepen the discussion on encryption and decryption and the teacher asks them if they can think of other ways to encrypt their messages.* *Then he/she proposes the Braille code and discusses whether it could be used as a cryptography method*	*10 minutes*
	A2.2 Exploration – Braille code	*Teacher shares* ***Worksheet 2*** *and asks students to collaborate and encrypt/decrypt messages using the Braille code.*	*35 minutes*
	Phase 3.	**Exploration: Caesar cipher**	
	Activity/Task	**Description/Procedure**	**Duration**
	A3.1 Warm up –	*Students are introduced to*	*10 minutes*

	linking to earlier discussed	*the Caesar cipher encryption method and the way it is used.* *An introduction to the method can be found here:* https://www.youtube.com/watch?v=sMOZf4GN3oc&feature=emb_title *The teacher can project a way of using it and discuss it with the students.*	
	A3.2 Exploration – Caesar cipher	*The teacher shares* ***Worksheet 3*** *and introduces students to the Caesar cipher method.* *Students are asked to collaborate to encrypt and decrypt messages using Caesar cipher.*	*25 minutes*
	A3.3 Discussing the weaknesses of symmetric cryptography	*The teacher and students discuss the symmetric encryption methods they have used so far to understand that the methods can be deciphered, especially with the use of computers.*	*10 minutes*
	Phase 4.	***Asymmetric Cryptography Diffie-Hellman Key Exchange-RSA***	
	Activity/Task	**Description/Procedure**	**Duration**
	A4.1 Warm up – linking to earlier discussed	*The teacher summarizes the course of the lesson so far and reminds students that the main problem of cryptography is the sending of a message from a transmitter to a receiver without being able to be caught-received by a third party interfering with the route of the message. It is also pointed out that the main weakness of symmetric cryptography methods is the secure sending of the key between transmitter and receiver without being perceived by third parties. Students are informed that symmetric cryptographic problems have been addressed with public key cryptographic methods since*	*15 minutes*

		the 1970s. The teacher connects Public Key Encryption (PKE) to pre-existing knowledge by presenting examples such as secure messaging (email), information transmission over the Internet (Secure http - https) and digital signatures. It is suggested that the relevant video: The Internet: Encryption & Public Keys (Code.org), https://www.youtube.com/watch?v=ZghMPWGXexs is viewed.	
	A4.2 2 Exploration-Diffie-Hellman Key Exchange algorithm and PKE	*Students are briefly informed that the PKE method was first published in 1976 by Whitfield Diffie and Martin Hellman, although it is known from an earlier time in the state secret service. The teacher shares **Worksheet 5** and introduces students to Diffie-Hellman Key Exchange algorithm.* *Depending on the readiness of the class, the algorithm can only be shortly demonstrated, or the students can also proceed with the study of the mathematical background of the method, included in the worksheet.* ***Worksheet 6** demonstrates the PKE asymmetric cryptography algorithm method with CrypTool software. Students test the PKE process and try out the method with each other. They can also use different free tools and web pages to create key pairs for encryption-decryption.*	*30 minutes*
C.2 Assessment			
	C.2.1 Student's feedback and reflection	*Students create public and private RSA keys and then exchange encrypted*	

		messages and try to decrypt them. If they are able to complete the process, the student is considered to have gained knowledge of the method.
C.3 Homework/ Work with parents-family	*Students are asked to apply the RSA method: key generation, encryption/decryption and exchange of messages with their parents using different online tools and simulation software.*	
Part D. Information for the Teachers		
D.1 Adaptation - Differentiation for inclusion of all students	*All students should be able to implement the scenario.*	
D.2 Extension	**D.2.1. Enigma machine** ***Worksheet 4:*** *The teacher introduces the use of machines for encryption with the example of the Enigma machine. These machines were extremely difficult to decipher either by humans or by other machines. Alan Turing's attempt to figure out the way the Enigma machine encodes messages, paved the way for the development of computer science.* *Initially how the Enigma machine works is demonstrated and explained with the help of video.* *Next, students practice two Enigma machine simulations:* *1. Firstly, a simple simulation made with paper that simulates the machine with one rotor.* *2. Secondly a simulation with the CrypTool educational software.* *Students are asked to collaborate to encrypt and decrypt messages using Enigma machine simulations.* *Suggested videos:* *https://www.youtube.com/watch?v=-mdSvGUd0_c* *https://www.youtube.com/watch?v=ASfAPOiq_eQ* **D.2.2. Educational game** *A game can be organized for the students to consolidate the encryption methods. Indicative examples:* 1. *Students are divided into A. The Cryptographers and B. The Hackers. The cryptographers choose a message and a method and hackers try to break their "code" by decrypting the messages. Cryptography methods practiced by students are used.* 2. *Students invent a hidden treasure mystery game. Specifically, a series of instructions for accessing the hidden treasure are encrypted and made accessible with QR-Codes placed in different places. Players must decrypt the QR-Code message to find out where the next one is (the first one is given). For decryption they can use paper-pencil, their programs and cryptool.org. The treasure may be the web address of the movie*	

	"imitation game". *3. The students can build an escape room. The escape from which will require the decryption of instructions.* **D.2.3. Reflecting on Cryptography** *Students could:* – *study and discuss the applications of the RSA method. Observe how intractable data security problems are exploited (e.g. calculating large prime numbers).* – *discuss and research cryptography and privacy* – *study cryptography policies and laws. What is the position of the citizens?* ***D.2.4. The biography of A. Turing (movie "imitation game")*** *Students can watch the movie "imitation game" which refers to Alan Turing's biography and his efforts to decipher the algorithm on which the Enigma machine is based. Following this students discuss issues of encryption. Additionally themes which extend from this for example history, language, peace education, human rights and sex education may then be explored in co-operation with other subjects such as art, history, biology and other subjects as inter-thematic projects.* ***D.2.5. Mathematical Background of RSA Method*** *Students are introduced to the method 's mathematical background.* ***Worksheet 8*** *illustrates the method with small prime numbers. Students can practice, finding prime numbers mathematically compute private and public keys and encrypt-decrypt messages with the RSA method.* *Mathematical knowledge of powers and mod operation are prerequisites.* *This scenario-extension can be combined with Maths (calculations of powers and application of mod rules).* ***D.2.6. Digital Signatures*** *The teacher connects PKE through examples of secure messaging (email), information transmission over the Internet (Secure http - https) and digital signatures. The digital signature of documents or messages made using the hidden key for encryption and the public key for decryption is also displayed. The problem of pretense and identification is raised, and the role of certification authorities is introduced.* ***Worksheet 7*** *helps students to explore the Digital Signature procedure and practice the signing-verification phase with CrypTool software.*
D.3 Resources	*Youtube*
D.4 Experience deriving from the	

implementation of the scenario	
D.5 Relations to other scenarios	
D.6 Reviews by teachers	
D.7 Assessment of the scenario	*[1=Very Bad – 5=Very Good]*
D.8 References	Grimm, R., Kempe, T., Löhr, A., & Scholle, O. (2015). *Informatik*. (Schöningh-Schulbuch, 1. Auflage, 4. Druck). Paderborn: Schöningh. *Spioncamp (2019).Bergische Universität Wuppertal, retrieved* from *https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf*
Part E. Annexes	
	Worksheet 1 *Worksheet 2* *Worksheet 3* *Worksheet 4* *Worksheet 5* *Worksheet 6* *Worksheet 7* *Worksheet 8*

CRYPTOGRAPHY

Worksheet 1

Student name(s): _____

Group name: _____ Date: _____

Cryptography is the practice of using techniques to securely communicate on the Internet, when trying to exchange private messages. With cryptography you can **encrypt** your messages to avoid third parties from having access to them. The receiver will have to **decrypt** your message to read it.

1. Think of a **message** you would like to send to a friend of yours and write it down:

_____

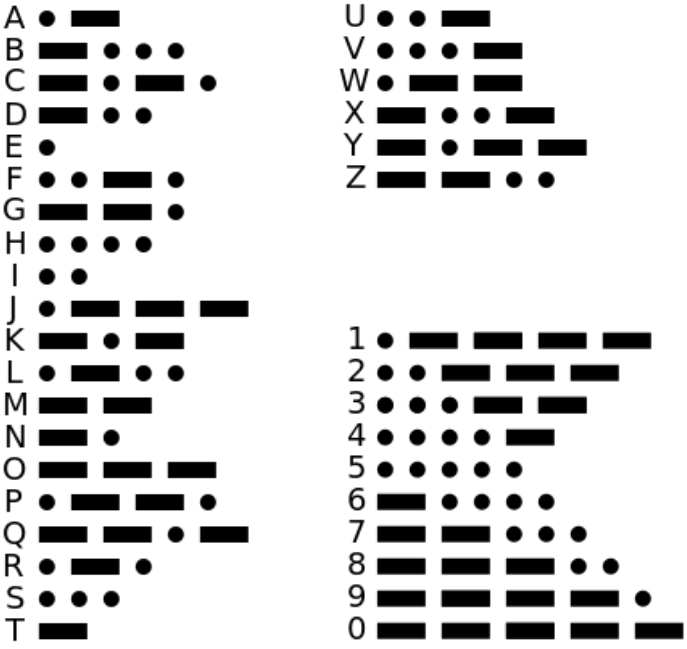
What do you think you should do to **encrypt** your message, so that nobody else understands it? Write down your encrypted message:

_____

What does your friend need to know so that he/she can **decrypt** your message?

_____

In 1832, before the invention of telephones, American Samuel Morse invented a device called the **Morse telegraph**, which was used to transmit messages over long distances. A network of cables was gradually established throughout the country. The cables did not transmit sound but electrical pulses of long or short duration, according to the table below.



Between letters there was a brief pause and between words a longer one. Light signals could also be used for the transmission of Morse code.

2. Based on the table above, can you understand the following message?

-.-. --- -- .--. ..- - . .-.

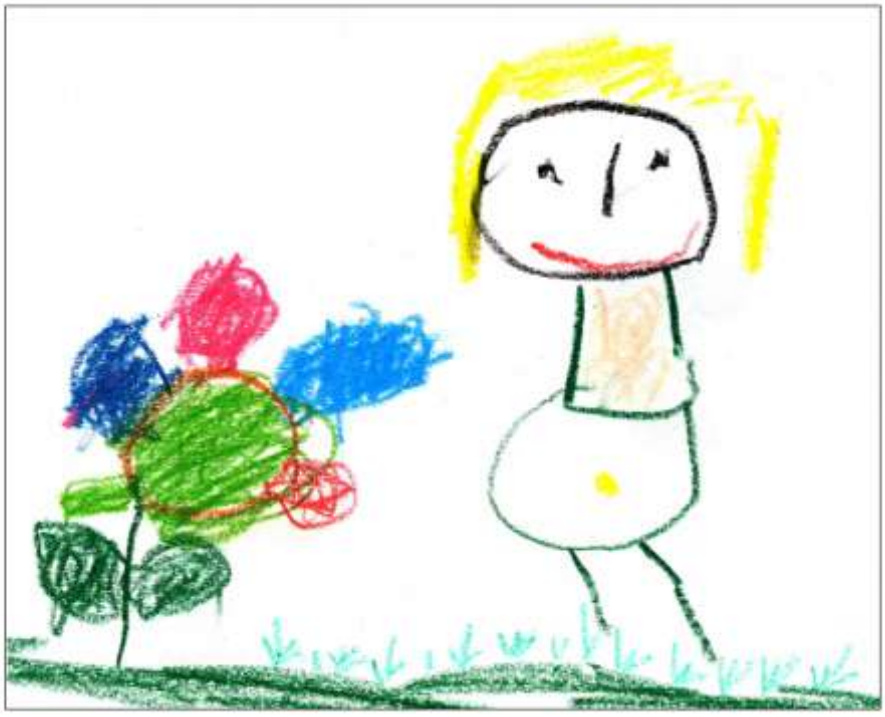
_____

3. What is the Morse signal for **SOS**? (This is the international help signal.)

_____

4. In groups of two, try to send a message to another group of your classmates by flashing a lens to represent Morse signals.

Another way to transmit messages is by hiding them in media, e. g. in pictures. This method is called **steganography**. If you look at the picture below, you may not notice that there is a message hidden in it. But the picture contains a message in Morse code. The long and short stems of the grass are the dashes and dots respectively, while each tuft is a letter.



Spioncamp (2019).Bergische Universität Wuppertal, retrieved from *https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf*

5. Can you find the secret message? _____

6. How would you draw a picture to encrypt a message for your friend?

Well done!

CRYPTOGRAPHY

Worksheet 2

Student name(s): _____

Group name: _____ Date: _____

BRAILLE CODE

Louis **Braille** was born in France in 1808 and went blind after an accident at the age of 3. At the age of 14 he developed a font which blind people can read. The font consists of raised points that someone can feel with one's fingers. The Braille signs are depicted in Table1.

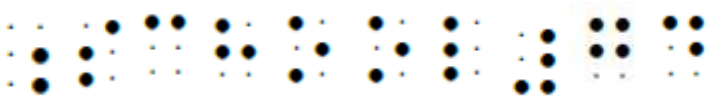
Table 1. Braille signs

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
1	2	3	4	5	6	7	8	9	0			

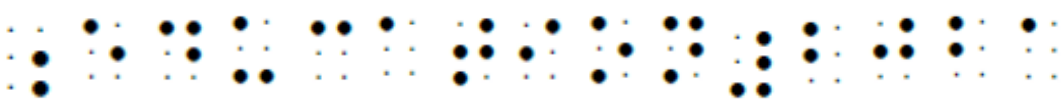
Words and numbers are discerned by using different signs before them. With these signs the reader knows if what follows is a word, or a number:

 when a **word** follows, or  when a **number** follows.

For example:

 is the code for **School 74**.

1. Can you decrypt the following message?



_____

2. Using the tip of your pencil, try to code your name and age by puncturing on the form below.

Use the Braille signs table to see which sign corresponds to each letter.

Ask your classmate to read what you wrote with his/her eyes closed, by touch.

GOOD JOB!

CRYPTOGRAPHY

Worksheet 3

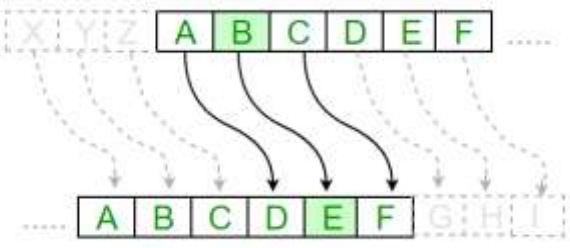
Student name(s): _____

Group name: _____ Date: _____

CAESAR CIPHER

Caesar cipher (or Caesar code) is one of the most famous and easy encryption systems, used by Julius Caesar (100-44 B.C.) for his private messages. According to this method, each letter of a message is substituted by another letter, some fixed number of positions down the alphabet. The number of positions is defined by the **key**, or **Caesar shift**, e. g. left shift of 3 or right shift of 4 etc.

Method: First, you will have to choose a number from 1 to 26, which you will have to share with the receiver. This is called the **key** and the receiver will use it to decrypt your message.



Then you need to write the alphabet in two lines: first the letters from A to Z and then each letter replaced, beginning from the letter in the position right after the key.

For example, in the case where the key is 4, letter A will be replaced by E (the letter after the 4th one), letter B will be replaced by F and so on. The first four letters (ABCD) follow right after Z.

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

1. Based on the above, if you use Caesar cipher key 4, the word **ANNA** will be encrypted to **ERRE**. Can you encrypt the following message using the above method (Caesar cipher key 4)?

CRYPTOGRAPHY **IS** **FANTASTIC**:

_____

2. Based on the above, can you also decrypt the following message?

GSQTYXIVW VSGO:

_____

Variation:

The method presented can easily be broken, so a variation of it was found. The sender and receiver will have to agree on a **key word**, for example the word **DODEKANISOS** (an island complex in Greece). The key word is written in the beginning of the alphabet (same letters are not repeated). Then you replace each of the other letters with the rest of the letters of the alphabet, beginning from the last letter of the key word. See the example below:

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

This table will be used for coding and decoding.

3. Based on the above variation, if you use the Caesar cipher key **DODEKANISOS**, can you now encrypt the following message?

CRYPTOGRAPHY **IS** **FANTASTIC**:

_____

4. Also based on the above, can you now decrypt the following message?

GSQTYXIVW VSGO:

_____

5. Do you notice any difference?

ACTIVITY:

In groups of two, agree on a key word and create the corresponding table below using Caesar cipher:

	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
Replaced by																										

Send an encrypted message to each other. Did you decrypt the message you received correctly?

You now can encrypt and decrypt messages using the Caesar cipher method!

Homework: Why not try to make your own cipher disk?

Well done!

ENIGMA CRYPTOGRAPHY MACHINE
Worksheet 4

Student name(s): _____

Group name: _____ Date: _____

Enigma cryptography machine

The "Enigma" machine was invented in 1923 by the German engineer Arthur Scherbius. Its name comes from the Greek word "enigma". This machine was originally used for commercial purposes, it was commercially available before World War II but it was modified into many variants and used to encrypt German army orders in World War II. Historical accounts confer that Alan Turing, an employee of the English counterintelligence, managed to break the code. “The imitation game” is a movie which refers to these events and the tragic fate of Turing.

Encryption/Decryption Method

Next a simplified simulation of the engine is presented. It consists of two wheels, an internal and an external one. The internal wheel rotates while the external wheel stays fixed.

Prerequisite: Both Sender and recipient must possess the machine!

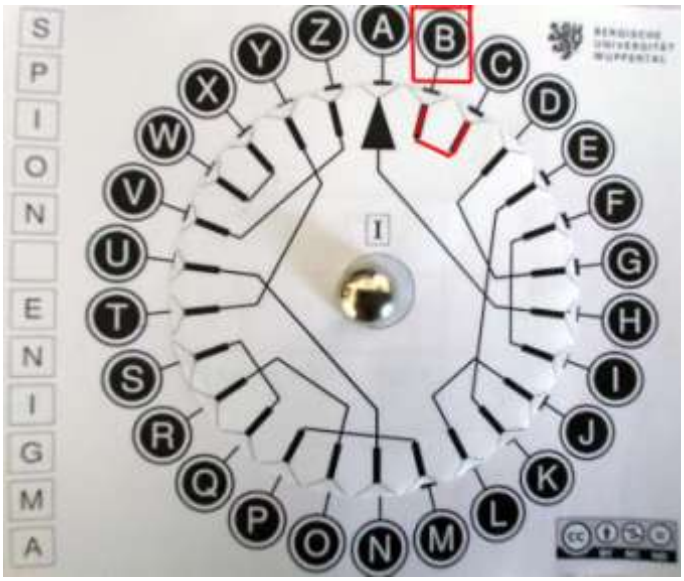
Encryption instructions:

- Place the arrow to point it towards the key.
- Then locate the letter of message you want to encrypt.
- Follow the link. This is the first encrypted letter.
- Then turn the arrow to the right so that it points to one letter down (pointing to the next letter of the key clockwise).
- Follow the link. This is the second encrypted letter.
- Do the same for all the letters in the message to be encrypted. Do not forget to rotate the arrow one letter down each time in a clockwise direction.

Example

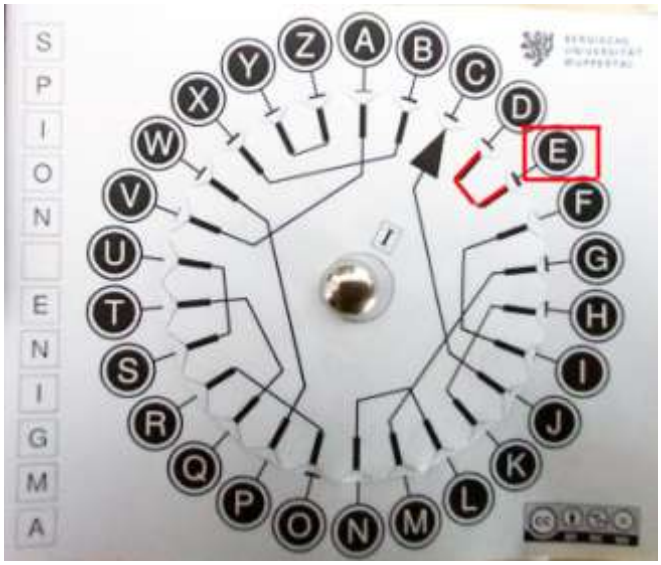
1. A key letter has been agreed upon. For example «A». The big arrow of the internal wheel should point to the key letter, that is letter «A».

2. If for example we want to encrypt the word «BYE»
3. The large arrow on the inner wheel must indicate the key, i.e. «A».
4. To encrypt the first letter B, look at its mapping. The letter B corresponds to the letter C. C is therefore the first encrypted letter.



5. To encrypt the next letter, turn the large arrow one position down clockwise. It should now point to B.

6. To encrypt the letter Y notice that Y is connected to X. The second encrypted letter is therefore X.
7. Turn the arrow one more position clockwise. It should now point to the letter C.



8. To encrypt the letter E notice that E is connected to D. The third encrypted letter is therefore D.

Following the procedure described above, the word **BYE** was encrypted in the ciphertext **CXD**.

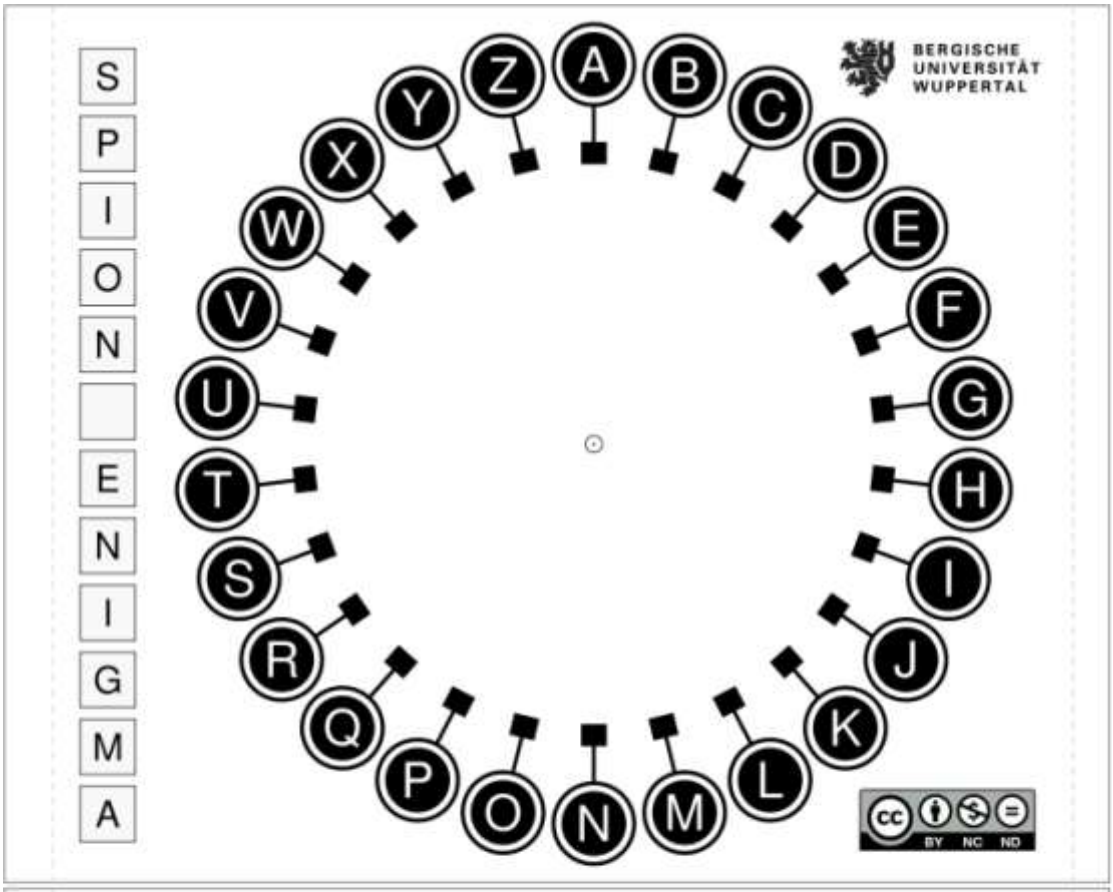
Decryption instructions:

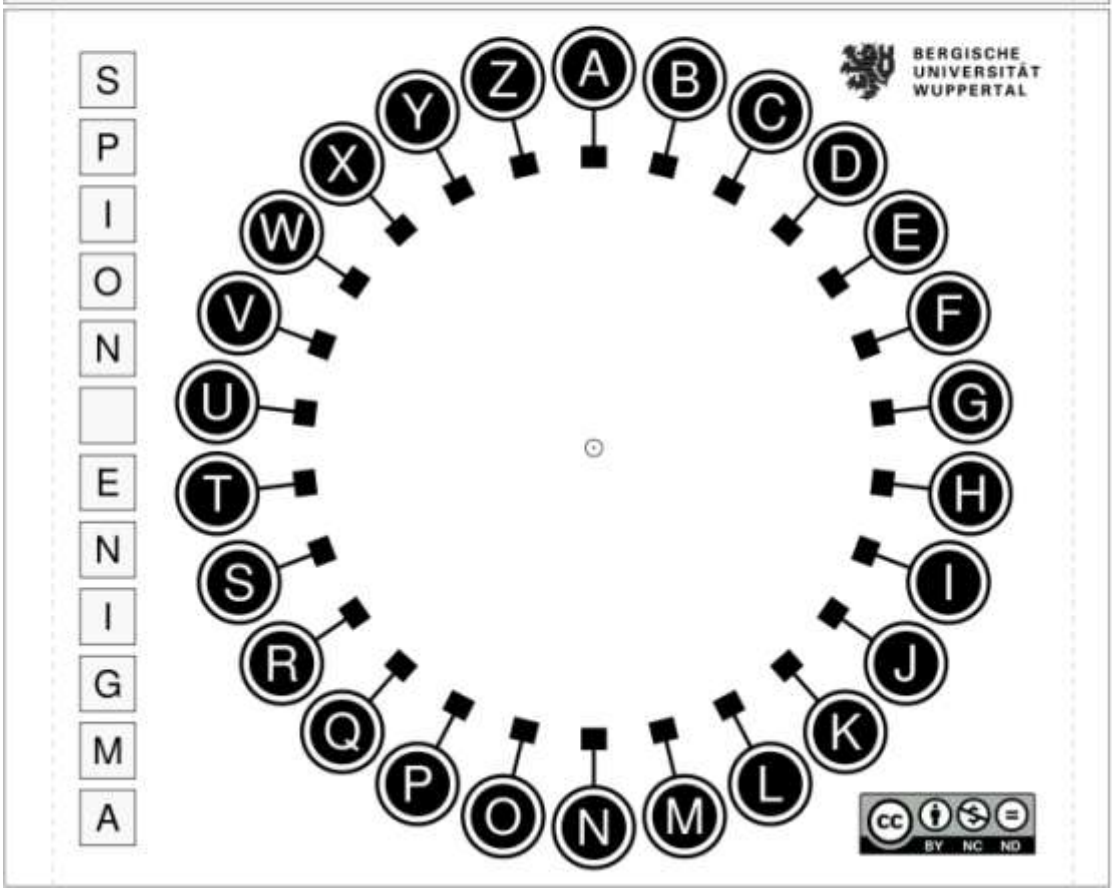
- Place the arrow pointing to the letter that is the key.
- Then locate the letter you want to decrypt.
- Follow the link. This is the first letter of the encrypted message.
- Then turn the arrow one letter down (pointing towards the next letter of the key) clockwise.
- Follow the link. This is the second encrypted letter.
- Do the same for all the letters in the message. Do not forget to rotate the arrow one letter at a time in a clockwise direction.

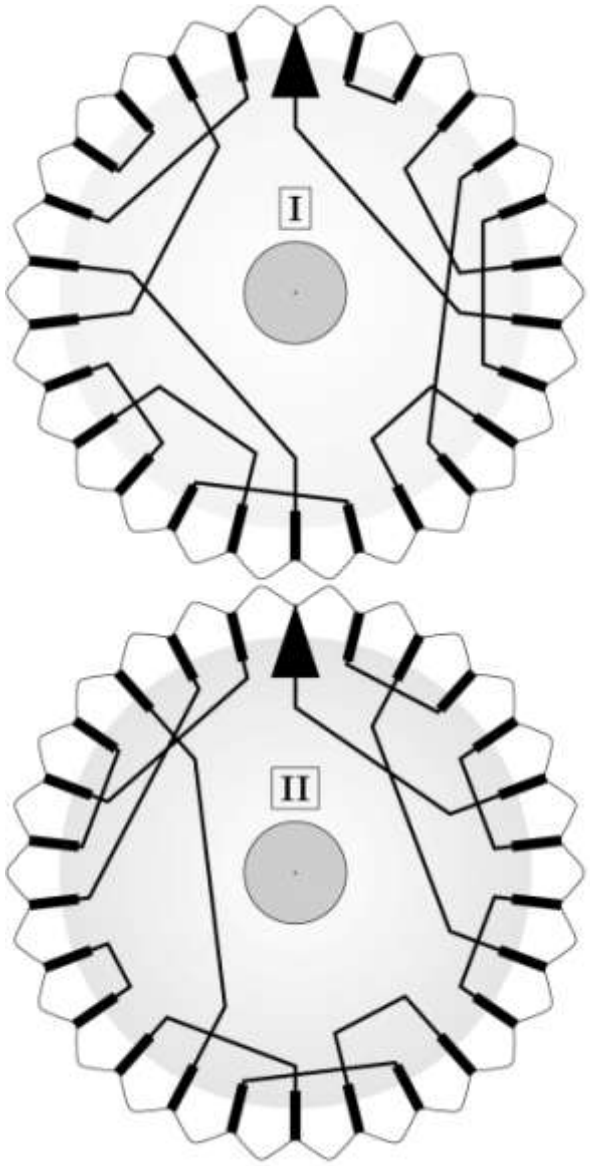
Construction of rotor

Print the two rotor discs.
Use a CD / DVD holder. In this case, cut the inner grey circle.

Alternatively use a  (blister drawing pin)


SPION ENIGMA
BERGISCHE UNIVERSITÄT WUPPERTAL
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
BY NC ND


SPION ENIGMA
BERGISCHE UNIVERSITÄT WUPPERTAL
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
BY NC ND



Spioncamp (2019).Bergische Universität Wuppertal, retrieved from *https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf*

Extension of Worksheet 4

Activity 1

Simulation with C*rypTool*

The Enigma Machine itself uses three such rotors which are in fact cylinders. For an introduction to the operation of the Enigma Machine watch the two videos suggested here.

https://www.youtube.com/watch?v=-mdSvGUd0_c

https://www.youtube.com/watch?v=ASfAPOiq_eQ

Let's try an example of simulation that is close to reality.

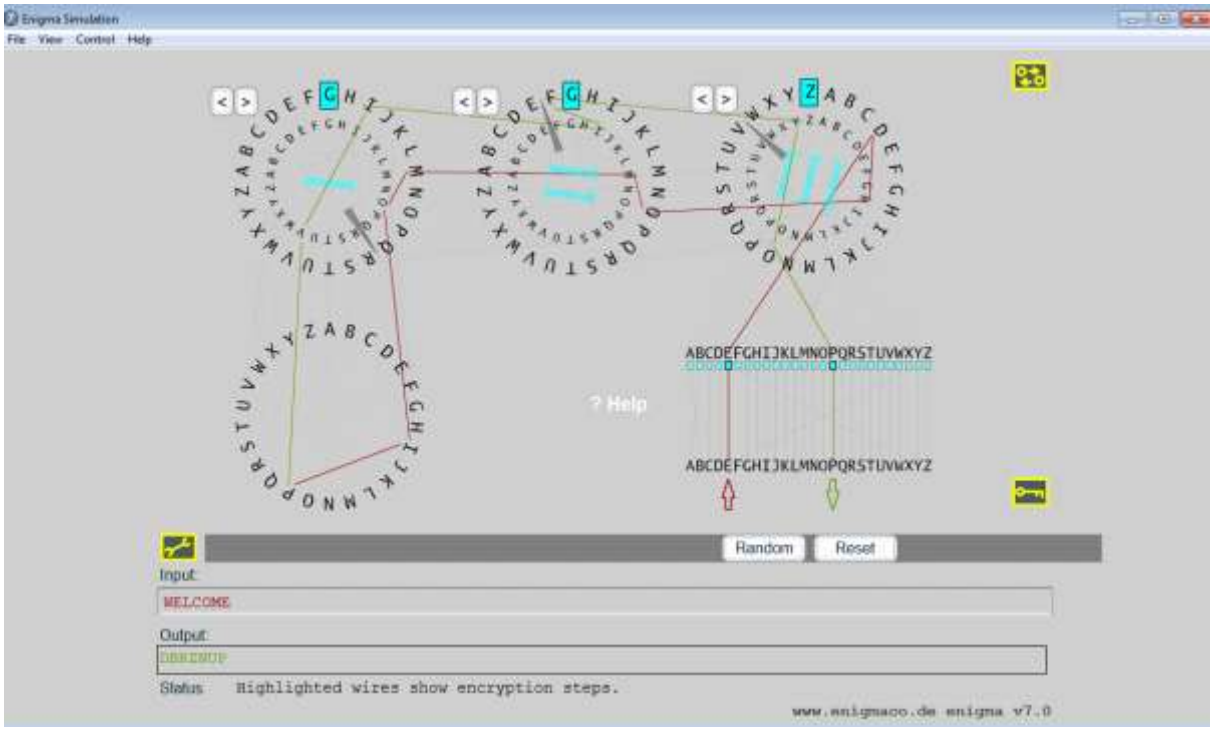
Download the simulation-tool cryptool1.4.41
https://www.cryptool.org/de/cryptool1

From the www.cryptool-online.org site.

Open the menu and choose *Individ. Procedures/Visualisation of algorithms /Enigma*

How can I encrypt a plain text?

- The first step is to make up a key. In this case, a key consists of two parts.
- The second step is to decide which pairs of letters should be exchanged or trans- positioned in the plugboard, e.g. A to B and also F to X. Notice that rotor settings at the beginning of the text entry, must be chosen for all three rotors e.g. F-E-S.
- The third step is to "RESET" the whole machine to the "initial state" by clicking on "RESET". The machine is now ready to encrypt the first sample.
- The fourth step is to drag the small yellow circle underneath A to B and release the mouse button. Thus, A and B have been exchanged. Please exchange F and X in that same way.
- The fifth step is to set the mentioned rotor settings by pressing the buttons "<" or ">" above each specific rotor. Each click of the mouse puts a rotor one position forward in the indicated direction.
- Finally, the word "welcome" is typed in. The line "Output:" should show the ciphertext i.e."DBRZNUP". The encrypted text looks completely different compared to the original, the only similarity is the same number of letters.



Activity 2

Encrypting –Decrypting with Simulator of Enigma-machine (CryptTool)

Students are divided into two groups: an encryption and a decryption group Using Cryptool software each group respectively encrypts or decrypts messages after having initially agreed on the values that the rotors will have and two letter transpositions.

Cut around the edges of the three text boxes below.

Secret memorandum for encrypting and decrypting groups

1. Set the rotor values (A-Z, English alphabet)

   rotor 1=

   rotor 2=

   rotor3=

2. Set the letter alternation

   … →…

To be kept top secret

Instructions for the encrypting group

Open CrypTool *(Individ. Procedures/Visualisation of algorithms /Enigma*).

Set the rotors as agreed

Set the letter transpostions

Enter the text for encrypting

Send the encrypted text to your decrypting group

Instructions for the decrypting group

Open CrypTool *(Individ. Procedures/Visualisation of algorithms /Enigma*).

Set the rotors as agreed

Set the letter transpositions

Enter the text for decrypting

Check the decrypted message

Asymmetric Encryption: Diffie- Hellman algorithm
Worksheet 5

Student name(s): _____

Group name: _____ Date: _____

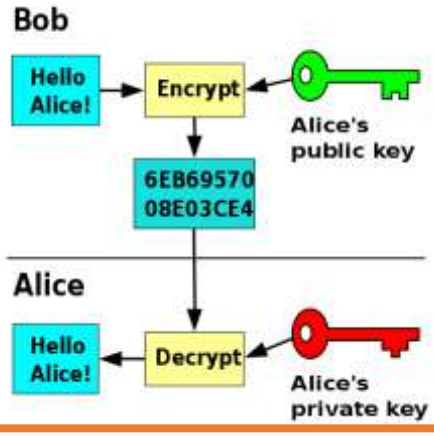
Diffie- Hellman algorithm

Method

Cryptography flourished when it became possible for the sender to encrypt the message with a secret key, send another public key to the recipient, and allow the recipient to decrypt the message using only the public key. Any third party who has access to the public key cannot decrypt the message!!! This is why such a process was called **asymmetric encryption**: But is such a thing possible?

For many years it was considered impossible to exchange a key that even if a third party knew it, it could not decode the encrypted message. In 1976 Martin Hellman, Whitfield Diffie and Ralph Merke developed the Diffie-Hellman algorithm which allows two parties to agree on a key, which even a third party would not know how to decrypt the message.

The diagram below (wikimedia.org) illustrates the steps for sending a message. Two different keys for encryption and decryption are used. Each user freely provides his public key to be sent encrypted messages that only he can decrypt with his secret-private key.



Let's explain it with an example: Bob and Alice agree to use a key number. A third party Ismene can obtain (by eavesdropping !!!) the public key number. Bob and Alice use the key to encode and decode messages which are then exchanged, not secretly, Ismene can see them, but she cannot encrypt them.

Bob and Alice apparently agree at first to use a **prime** number p. They must also agree on a **natural** number, say c. You should c <p.

Bob then chooses a positive integer α (less than p) which he keeps secret.

Alice also chooses a positive integer β (less than p) which she keeps secret.

Bob and Alice can calculate the **key** "**K"** based on the formulas given in the table below. Ismene could know p, c, A and B but cannot calculate the key K because she does not know α and β.

Private space	**Public space**	**Private space**
Bob 	Ismene 	Alice 
choose α, α<p	determine p και c	choose β, β<p
compute $A=c^{\alpha}$ mod p		compute $B=c^{\beta}$ mod p
	A →	
B ←	B →	A
compute $K=B^{\alpha}$ mod p		compute $K=A^{\beta}$ mod p

Reference: Spioncamp (2019).Bergische Universität Wuppertal, retrieved from *https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf*

Here is an example with numbers

Private space	**Public space**	**Private space**
Bob 	Ismene 	Alice 
	p=17 και c=5	
choose α, με α<p		choose β, β<p
α=4		β=7
compute $A=c^{\alpha}$ mod p		compute $B=c^{\beta}$ mod p
$A=5^4$ mod 17		$B=5^7$ mod 17
A= 625 mod 17		B= 78.125 mod 17
A=13	A →	B=10
B ←	B →	A
compute $K=B^{\alpha}$ mod p		compute $K=A^{\beta}$ mod p

$K=10^4$ mod 17 K=10.000 mod 17 **K=4**		$K=13^7$ mod 17 K=62.748.517 mod 17 **K=4**

The key that Bob and Alice will use is 4. This key can be used to encrypt and decrypt messages.

You can use the Windows calculator in scientific view to calculate powers and divisions with mod.

Question: Is it possible for Ismene to find the key K?

Answer: Yes by trying combinations of numbers from 0 to p.

In case p is small, as here, finding the key is easy. But if the numbers to be chosen are large then it is impossible even with the fastest computers available to find the key through number testing.

Activity 1

Compute key K applying Diffie- Hellman algorithm for numbers p=7 και c=4

Private space	**Public space**	**Private space**
Bob 	Ismene 	Alice 
	p=7 και c=4	
choose α, α<p		choose β, β<p
α=…		β=…
compute $A=c^{\alpha}$ mod p		compute $B=c^{\beta}$ mod p
A=…….		B=……..
A= …….		B= …….
A=…….	A	B=……...
B	B	A
compute $K=B^{\alpha}$ mod p		compute $K=A^{\beta}$ mod p
K=……..		K=…….
K=……..		K=……
K=…..		**K=……**

Asymmetric Encryption: PKE (RSA) Procedure
Worksheet 6

Student name(s): _____

Group name: _____ Date: _____

Activity 1

The operation of the RSA algorithm will be demonstrated in two parts with CrypTool:

a. The generation of an RSA key,

b. The encryption and decryption of messages

According to RSA, encrypted communication between two parties requires:

1. a public key, which consists of a pair of numbers (N, e)

2. a private key, which also consists of a pair of numbers and which remain secret (N, d)

Generation of RSA keys

To create an RSA key select **Individual Procedures \ RSA Cryptosystem \ RSA Demonstration**.

For the RSA key, two different prime numbers, p and q are needed.

Enter two prime numbers into the fields **Prime number p** and **Prime number q**, or generate two random prime numbers, p and q.

As an example we wish to generate a random 256-bit RSA key. To do this, click on the **Generate prime numbers…** button. Similarly to menu selection **Indiv. Procedures \ RSA Demonstration \ Generate Prime Numbers…**, a dialog box opens in which to generate prime numbers p and q. For prime number p, choose 2^127+2^126 as the **lower limit** and 2^128 as the **upper limit**, and activate for the value range the radio button, **Both are equal**. When you click on **Generate prime numbers**, two prime numbers p and q of bit length between 127.5 and 128 are generated. When p and q are multiplied together, the result is RSA modulus N of bit length greater than 2*127.5 = 255, i.e. a 256-bit RSA key.

Prime numbers can be generated as often as you like. If you click on the **Apply primes** pushbutton, prime numbers p and q are passed to the RSA dialog. At the same time RSA modulus N is calculated, also the Euler phi function phi(N).

The next step is to determine the public RSA key e, a number that is coprime to phi(N). Sometimes it is not easy to find such a number. For this reason we offer a small tip: the number e = 2^16+1 = 65537 (= 10000000000000001 binary) is in practice always coprime to phi(N).

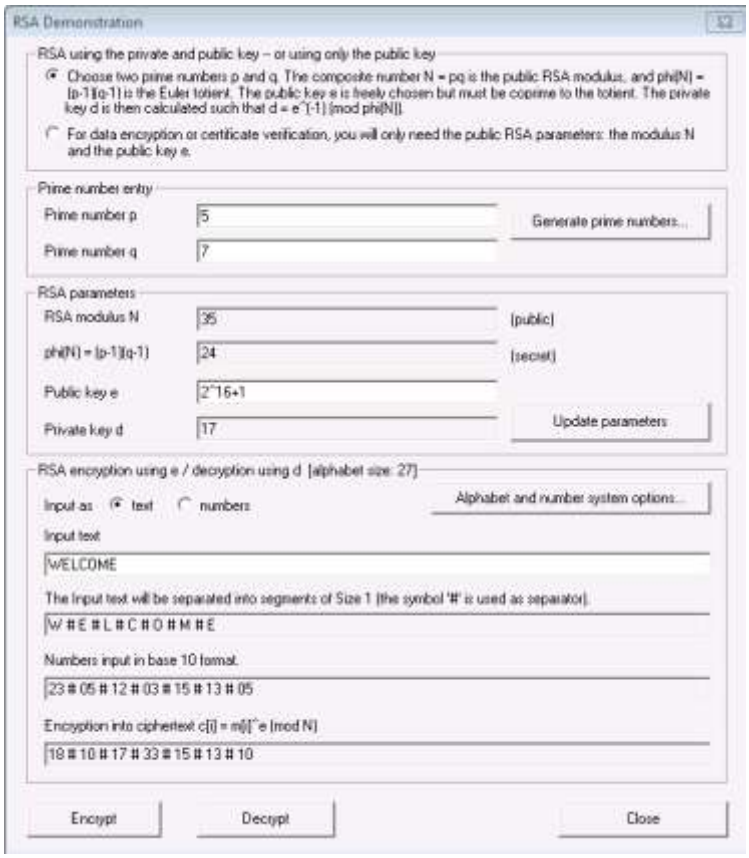
Click on the **Update parameters** pushbutton, and the secret RSA key d will then be calculated from the number e.

You can now encrypt and decrypt messages.

2. Encryption or decryption of messages using the RSA key pair

Once you have generated the RSA key, you can encrypt and decrypt messages.

You can view an example below:



Activity 2

Students are divided into two groups (one group encrypts, the other decrypts).

Step 1
Activity for both groups: the creation of public and private key pairs.

Step 2

The Encryption group encrypts a message.

Step 3
The encrypted message is sent to the decryption group

Step 4
The decryption group decrypts the encrypted message

Activity 3

The operation of the RSA algorithm will be demonstrated alternatively in other simulation software:

- *https://travistidwell.com/jsencrypt/demo/,*
- *https://www.devglan.com/online-tools/rsa-encryption-decryption*
- *https://8gwifi.org/rsafunctions.jsp*

Students can:

1. Create RSA keys
2. Encrypt/Decrypt and exchange messages

Asymmetric Encryption: Digital Signature – Worksheet 7

Student name(s): _____

Group name: _____ Date: _____

Method

Create and verify digital signature

The use of the digital signature involves two procedures: the creation of the signature and its verification. Below, the actions of the sender and the recipient are described step by step in order to facilitate understanding of the digital creation and verification signature mechanism.

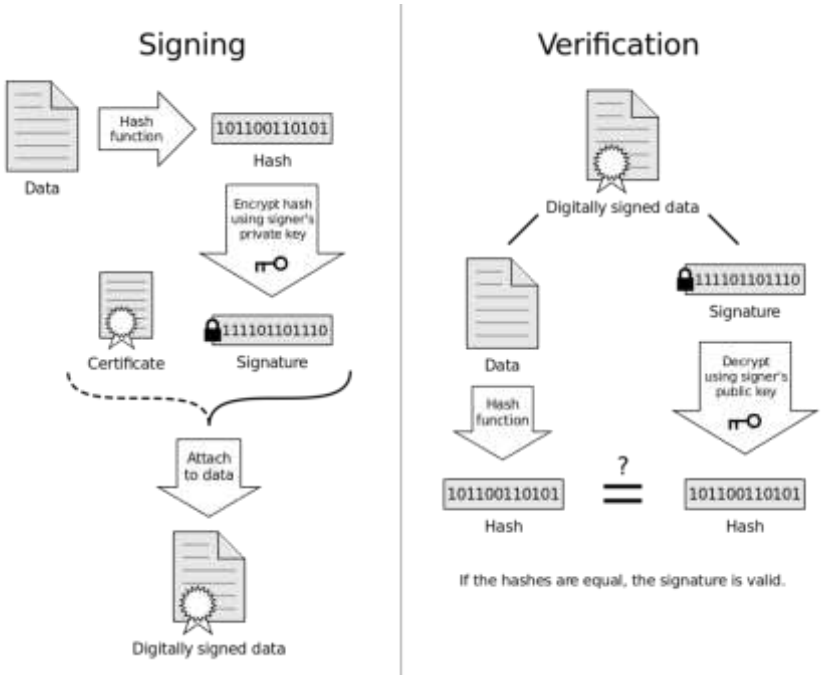
Sender

1. The sender using a hash algorithm (one way hash) creates the summary of the message (message digest) to be sent. A series of digits of a certain length will be generated regardless of the size of the message.
2. The sender encrypts the above using the private key. The digital signature is thus produced and consists of a series of digits.
3. The encrypted summary (digital signature) is attached to the text and the digitally signed message is transmitted over the network (note that message can be encrypted by its sender with the use of the public key).

Recipient

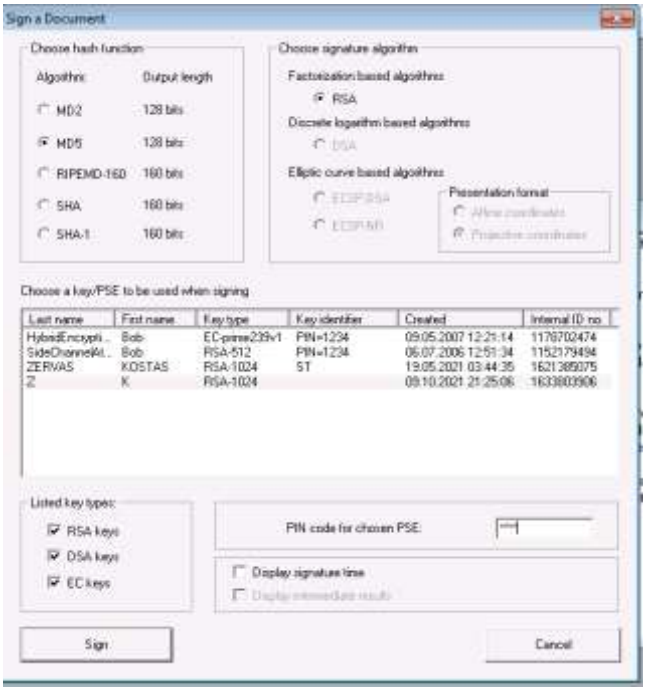
1. The recipient separates the digital signature from the message.
2. The recipient creates the message summary by applying the same hash algorithm as the sender to the message received.
3. The digital signature is decrypted using the sender's public key and a digital signature summary is produced.
4. The message and digital summaries are compared and if they are found to be the same, it means that the message received by the recipient is intact. If on the other hand they are found to be different, then the message sent has been subjected to change.

The diagram below illustrates the signing process (digital signature)



Activity: Practicing the Digital Signature process with CrypTool.

1. The public key pair is created from the menu: Digital signature/PKI/Generate keys (additionally PIN is required)
2. Next the text for encryption is typed in or the file to be encrypted is uploaded.
3. Digital Signatures/Sign Document command is then chosen. It is necessary to specify
    a. The Hash function algorithm (MD2, MD5 etc)
    b. The signature algorithm (RSA etc)
    c. The public key pair
4. Sign



5. Save the produced file and send to recipients. This file contains
    a. The signature
    b. The content to be sent

The team that will receive the file containing the signature and the content can confirm the signature (which guarantees that the text has reached intact), choosing Digital /signature/PKI/Verify Signature

Asymmetric Encryption: RSA Procedure- Mathematical Background

Worksheet 8

Student name(s): _____

Group name: _____ Date: _____

Method

The table below shows the RSA procedure (prerequisite knowledge: prime numbers, powers)

1	Choose two prime numbers p and q	p=3 και q=11
2	Compute N=p*q	N=3*11=33
3	Compute r=(p-1)*(q-1)	r=(3-1)*(11-1)=2*10=20
4	Choose a number e in such a way that e and r have no common divisor	e=7 e=5 r=20 have no common divisor
5	Determine number d such as e*d mod r=1	d=23 7*23 mod 20=161 mod 20=1
6	Publish N and e, keep secret d	Public key (N,e)=(33, 7) Private key (N, d)=(33, 23)
7	Encrypt message M: Compute $C=M^e$ mod N	For example **M=2** $C=2^7$ mod 33=128 mod 33 =29
8	Decrypt C Compute $M=C^d$ mod N	Decrypt C=29 $M=29^{23}$ mod 33=2 **M=2**

The philosophy of the algorithm is that calculations in one direction are easy, but much more difficult in another direction. The RSA method is based on the mathematical fact that it is easy to calculate the product of two prime numbers, but it is very difficult to factorize this product, that is, to find the factors from which it is formed. In this case (if we limit ourselves to small numbers, it is possible with tests to calculate the private key d with tests).

But when the numbers are large, the order of 200-300 digits is extremely time-consuming even with the fastest computers to calculate d. It is "computationally impossible" to calculate it. The factorization of small numbers, for example in our example of 33, is easy. We find "by hand that 33" is produced by multiplying 3 by 11.

There are also applications that can factorize numbers, such as the one given in the link *https://www.mathpapa.com/factoring-calculator/*

1	Choose two prime numbers p and q	p= και q=
2	Compute N=p*q	N=
3	Compute r=(p-1)*(q-1)	r=
4	Choose a number e in such a way that e and r have no common divisor	e=
5	Determine number d such as e*d mod r=1	d=
6	Publish N and e, keep secret d	Public key (N,e)= Private key (N, d)=
7	Encrypt message M: Compute $C=M^e$ mod N	For example **M=2**
8	Decrypt C Compute $M=C^d$ mod N	Decrypt C

Activity: Mathematical Background of RSA Method

Choose two prime numbers p and q and then apply RSA Method.

You can use the Windows calculator in scientific view to calculate powers and divisions with mod or apply mod rules.

Mod rules

(x+y) mod b = x mod b +y mod b

$(x*y) \bmod b = x \bmod b * y \bmod b$

This makes it easy to calculate powers modulo a number

$(x^{y+z}) \bmod b = (x^y * x^z) \bmod b = (x^y \bmod b * x^z \bmod b) \bmod b$

References

Grimm, R., Kempe, T., Löhr, A., & Scholle, O. (2016). *Informatik*. (Schöningh-Schulbuch, 1. Auflage, 4. Druck). Paderborn: Schöningh (p. 280-284)

UNIVERSITY OF THE AEGEAN

LTEE lab
University of the Aegean
ltee.aegean.gr

CompuT

Computational Thinking at School

Erasmus+ KA201 Project: 2019-1-EL01-KA201-062883