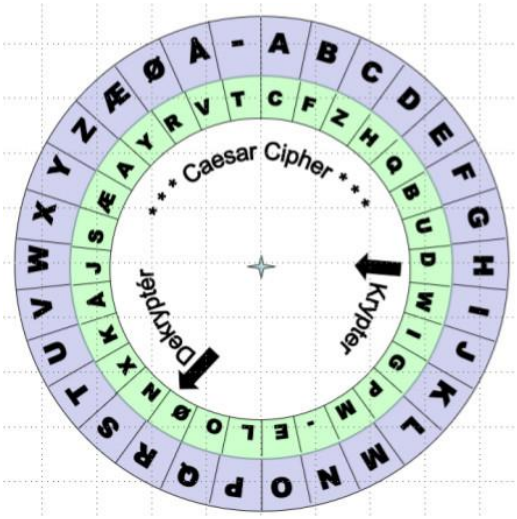
**Universitetet i Oslo**
**IN2120 Informasjonssikkerhet**
**Høst 2024**
**Teoretiske oppgaver**

# *Teori 2 (Del 2): Kryptografi*




## Oppgave 1: Cæsar-chiffer

Anta en substitusjons-chifferalgoritme som ligner Caesar-algorithmen, men der bokstavene i den innerste sirkelen er omstokket. Bokstavene kan ha en vilkårlig rekkefølge, der figuren til høyre viser et eksempel. Rekkefølgen av tegnene i det omstokkede alfabetet på den inder sirkelen utgjør nøkkelen. Det er til sammen 30 tegn, som består av 29 bokstaver og bindestrek '-'.

a. Gi et enkelt matematisk uttrykk for hvor mange forskjellige nøkler denne chifferalgoritmen har, og finn tallsvaret med en kalkulator, f.eks. online: https://www.calculatorsoup.com/calculators/discretemathematics/factorials.php
b. Hva er nøkkelstørrelsen for 30 tegn uttrykt i antall bits? Vurder om nøkkelstørrelsen er tilstrekkelig for å motstå uttømmende søk i hele nøkkelrommet.
c. Hva hadde nøkkelstørrelsen vært om alfabetet hadde hatt 34 tegn? Er nøkkelstørrelsen tilstrekkelig for å motstå uttømmende søk gjennom hele nøkkelrommet? Forklar svaret.
d. Kan algorithmen motstå statistisk kryptanalyse? Forklar svaret.
e. Forklar kort hvordan man kan kryptanalysere en chiffertekst som er kryptert med denne chifferalgorithmen.

## Oppgave 2: Digital signatur

Alice ønsker å sende melding *M* med digital signatur *S*(*M*) til Bob. De har hverandres offentlige nøkler, og har blitt enige om en kryptografisk hash-funksjon Hash og en signatur-algoritme som opererer i signeringsmodus Sig (tilsvarende dekrypteringsmodus D) eller i valideringsmodus Val (tilsvarer krypteringsmodus E).

a. Beskriv trinnene Alice må følge for å sende *M*.
b. Beskriv trinnene som mottaker Bob må følge for å validere autentisiteten av *M*.
c. Forklar hvordan den digitale signaturen beviser for Bob at den mottatte meldingen er autentisk, og forklar hvordan også enhver tredjepart, ikke bare Bob, kan bli overbevist om at meldingen er autentisk. Hva kalles egenskapen?
d. Hvilke plausible grunner kan avsender Alice gi for å nekte å ha sendt den signert meldingen selv om den har hennes signatur? Hva sier det om begrepet 'ubenektelighet'?
e. Diskuter den semantiske tolkningen av "digitalt signert melding", som kan bety: I) at jeg Alice er enig i innholdet av meldingen, eller II) Alice sendte meldingen uten nødvendigvis å være enige i innholdet?

## Oppgave 3: Strømchiffer

Anta at en binær additiv strømchiffer-algoritme (som bruker en pseudotilfeldig nøkkelstreng eller en engangsnøkkel (One-Time-Pad)) har blitt brukt til å kryptere en elektronisk pengetransaksjon. Anta at det ikke brukes andre kryptografiske mekanismer. Forklar hvordan en angriper kan endre overføringsbeløpet uten å vite noe om nøkkelen som brukes (du kan anta at angriperen vet formatet på klartekstmelding som brukes ved overføring av pengene.)

## Oppgave 4: Fremoverhemmelighold

Kryptering av data med asymmetriske algoritmer er upraktisk fordi det gir for stor belastning med beregning. I praksis brukes en kombinasjon av både symmetrisk og asymmetrisk kryptering, der en symmetrisk nøkkel utveksles mellom avsender og mottager ved hjelp av en asymmetrisk metode, og den symmetriske nøkkelen benyttes for selve kryteringen av data.

a. Hva er fremoverhemmelighold (Forward Secrecy) (noen gang kalt perfekt fremoverhemmelighold) for sikkerhetsprotokoller?
b. Anta at Alice og Bob etablerer økter der de krypterer data med en hemmelig symmetrisk øktnøkkel som Alice hver gang sender til Bob kryptert med Bobs offentlige nøkkel. Gir dette fremoverhemmelighold? Forklar hvorfor/hvorfor ikke.
c. Hva er en typisk metode for å oppnå fremoverhemmelighold? Nevn en prominent sikkerhetsprotokoll som støtter fremoverhemmelighold.

## Oppgave 5

Diffie-Hellman-algoritmen for nøkkelgenerering og utveksling lar to parter opprette en felles hemmelig nøkkel over en usikker kanal.

a. Forklar med formell notasjon trinnene i Diffie-Key-algoritmen.
b. Forklar hvorfor Diffie-Hellman-algoritmen i seg selv ikke gir gjensidig autentisering av partene, og hva som kan gjøres i tillegg for å oppnå autentisitet.

## Oppgave 6: Symmetrisk kryptering

Alice ønsker å sende melding $M$ til Bob, uten at Eve observere den. Alice og Bob har blitt enige om å bruke en symmetrisk kryptoalgoritme som kan brukes til kryptering med funskjonen E eller dekryptering med funskjonen D. Nøkkelutveksling er allerede gjort, slik at de har felles nøkkel $K$ for den spesifikke krypteringsalgoritmen. De er også enige om å bruke en sikker krypteringsmodus for bruk av algoritmen (f.eks. CTR-modus), men detaljer om krypteringsmodus er uvesentlig for denne oppgaven.

a. Beskriv trinnene Alice må følge for å kryptere $M$ og sende chifferteksten til Bob.
b. Beskriv trinnene som Bob må følge for å dekryptere den mottatte chiffertekst $C$.

## Oppgave 7: Hashfunksjoner

Hashfunksjoner brukes ofte til å verifisere meldingsintegritet.

a. Oppgi fire fundamentale krav til kryptografiske hash-funksjoner.
b. Hva er forskjellen mellom de to variantene av kollisjonsresistens?
c. Bruk Internett til å finne en SHA-2 demo webside. Du finner en interaktiv webside laget av Geraint Luff som kan finnes på: http://geraintluff.GitHub.io/sha256/
   Undersøk hash-funksjons egenskaper ved å beregne SHA-2 hash for følgende:
   (i) ta ut $100 fra min konto
   (II) ta ut $1000 fra min konto
   (III) ta ut $100 fra din konto
   (IV) (du kan prøve å lage hashe for både lengre og kortere meldinger)

## Oppgave 8: Meldingsautentisering

Alice ønsker å sende en melding *M* med en meldingsautentiseringskode *MAC*(*M*) til Bob. Alice og Bob deler en hemmelig nøkkel *K*, og har blitt enige om å bruke en bestemt nøkkelstyrt hashfunksjon Hash(*M*, *K*) som tar inndataparametere *M* og *K* for å produsere *MAC*(*M*).

a. Beskriv trinnene Alice må følge for å sende *M* med meldingsautentisering.
b. Beskriv trinnene som mottaker Bob må følge for å validere autentisiteten til *M*.
c. Forklar hvordan en *MAC* beviser for Bob at den mottatt melding er autentisk, og hvorfor Bob **ikke er istand** til å bevise overfor en tredjepart at meldingen er autentisk.

## Oppgave 9: Bruk av kryptografi

a. For hvilke datatilstander (lagring, overføring, prosessering) kan kryptografi brukes til å beskytte informasjon? Hvordan kan kryptografi beskytte data under prosessering?
b. Hvilke sikkerhetsmål/tjenester kan støttes av kryptografi?

## Oppgave 10: Postkvantekrypto

Kvantecomputing har potensiale til å knekke de fleste standardiserte asymmetriske kryptografiske algoritmer. Kvanteresistente kryptoalgoritmer kalles PQC (Post-Quantum Crypto) fordi de skal være sikre selv etter at store kvantecomputere er tilgjengelige på markedet.

a. Hvilke tre PQC-algoritmer ble publisert som utkast til NIST-standarder i august 2024?
b. Hvilken type nye PQC-algoritmer ønsker NIST fremdeles å velge?