Ordliste 2

Dette er et forsøk på å gi forklaringer til ord og uttrykk som brukes i forbindelse med tekst og tall (og litt datakommunikasjon og kryptering) i kurset INF1040 høsten 2004. En del av nøkkelordene er *ikke* brukt i kurset INF1040, men er ord som man kan støte på i annen faglitteratur på dette nivået, eller som tilhører allmenndannelsen for en MatNat-student.

Understreket ord er forklart et annet sted i ordlisten

2er-komplement (2-complement)
Prinsipp for representasjon av negative heltall. 2er-komplementet beregnes ved å invertere alle bitene i heltallsrepresentasjonen og deretter legge til 1. Representasjonsformen gjør at samme logikk kan brukes for addisjon med negative tall som med positive tall.

ASCII
Universell standard for koding og representasjon av tegn. Forkortelse for "American Standard Code for Information Interchange". Bruker 7 biter per tegn, og har dermed plass til 128 tegn/kodepunkter. Omfatter ikke særnorske bokstaver som Æ Ø Å æ ø å.

asymmetrisk kryptering (asymmetric cryptography)
Kryptering der vi bruker et nøkkelpar, en nøkkel for å kryptere og en annen, tilhørende nøkkel for å dekryptere.

Basic Multilingual Plane – BMP
Den delen av UNICODE-tegnsettet som har kodepunkt mindre eller lik 0xFFFFFFFF. Bemerk at noen av bitmønstrene er reservert for surrogatpar og derfor ikke kan brukes for kodepunkter.

bias (bias)
En konstant som legges til en mengde med tall for å forskyve tallområdet. Brukes oftest for å forskyve et tallområde fra [-n, +n] til [0, 2n] ved hjelp av en bias n, slik at alle tall blir positive og dermed enklere å representere.

bit (bit)
Kortform for "binary digit", binærsiffer, dvs. et siffer som kan ha bare to verdier, vanligvis visualisert som 0 og 1.
I den statistiske informasjonsteorien brukes bit som enhet for informasjonsmengde. [Norsk dataordbok]

Byte (byte)
En streng på 8 biter som behandles som en enhet.

diakritisk markering (diacritic)
Et tegn som ikke er ment å stå alene, men som knyttes til et annet tegn for å modifisere dette. Eksempler på diakritiske markeringer er ulike typer aksenter.

DTD (DTD)
Document Type Definition. Spesifiserer hva som er gyldig struktur i et XML-dokument, spesielt hvilke XML-markeringer som skal brukes, hvilke attributter som er tillatt, og hvordan XML-elementene skal kunne nøstes. Avløses etter hvert av XML-skjema.

eksponent (exponent)
Tallord som bestemmer den potens det underforståtte grunntall skal opphøyes i før multiplikasjon med fasttallsdelen. [Norsk dataordbok, ISO]

flytende tall/flytetall (floating point number)
Tall som er angitt i et flytetallsystem, dvs. et system for tallrepresentasjon der et reelt tall er representert av to tallord og er lik produktet av det ene tallordet, mantissen, og en potens av et underforstått grunntall med en eksponent som representeres av det andre tallordet.
[Norsk dataordbok, ISO]

glyf (glyph)
Visuell fremvisning av et tegn. A **A** *A* er tre ulike glyfer for det samme tegnet.

heksadesimal (hexadesimal)
Om fast grunntallsystem med grunntall 16. Sifrene som brukes, er 0-9 og A-F.
[Norsk dataordbok, ISO]
For å vise at et tall er på heksadesimal form, setter vi gjerne 0x foran selve tallet.

heltall (integer)
ett av tallene null, pluss en, minus en, pluss to, ...
[Norsk dataordbok, ISO

kodepunkt (codepoint)
En entydig numerisk verdi knyttet til et tegn. Knytningen angis i kodetabeller. Den numeriske verdien angis gjerne på heksadesimal form, som lett lar seg konvertere til en tilsvarende verdi på binær form.

Kodetabell (code table)
En tabell som viser knytningen mellom tegn og kodepunkter. Eksempler på slike kodetabeller er ASCII-tabellen og UNICODE-tabellen.

lag (layer)
I datanettarkitektur: Gruppe tjenester, funksjoner og protokoller som er fullstendige fra et begrepsmessig synspunkt, som er en av et sett med hierarkisk oppbygde grupper i henhold til en lagdelt referansemodell (som f.eks. TCP/IP-"stakken" og den nå historiske OSI-modellen).
[Norsk dataordbok, ISO, modifisert]
Et lag kan be om tjenester fra det underliggende laget og yter tjenester til det overliggende laget. Grensesnittene mellom lagene er standardisert. Et velkjent eksempel på et slikt lag er IP-laget i TCP/IP-"stakken".

linklag (link layer)
Et lag (i nettverksprotokoller) som har som oppgave å transportere data fra en node i nettverket til en nabonode.

nøyaktighet (accuracy)
1: Kvalitetsmål for frihet fra feil.
2: Kvantitativt mål for størrelsen av feil (høy verdi svarer til liten feil).
[Norsk dataordbok, ISO]
Et uttrykk for avviket mellom en virkelig verdi og den verdien vi greier å måle.

mantisse (matissa)
Den delen av en flyttallsrepresentasjon som multiplisert med en potens av grunntallet gir det tallet som er representert (bortsett fra fortegn) [Norsk dataordbok, ISO]

nettverkslag (network layer)
Et lag (i nettverksprotokoller) som har som oppgave å ta i mot data og ut fra adressen til endesystemet bestemme til hvilken node dataene bør videresendes for etter hvert å kunne nå endesystemet. Benytter tjenester fra det underliggende linklaget. Eksempel på protokoller: IP

offentlig nøkkel (public key)
Krypteringsnøkkel brukt i asymmetrisk kryptering, knyttet til en bestemt juridisk person og offentlig kjent. Del av et nøkkelpar, den andre nøkkelen er den private nøkkelen.

oktal (octal)
Om fast grunntallsystem med grunntall 8. Sifrene som brukes, er 0-7.
[Norsk dataordbok, ISO

one-time-pad
Krypteringsnøkkel brukt i symmetrisk kryptering, minst like lang som bitmønsteret som skal krypteres. Forutsettes brukt bare én gang, og gir da 100% sikkerhet.

overføringskapasitet (transfer capacity)
Det antall biter som kan overføres gjennom en datakommunikasjonskanal i løpet av en tidsenhet. Oppgis i biter per sekund.

overløp (overflow)
Oppstår når en aritmetisk operasjon gir et resultat utenfor det representerbare tallområdet.

posisjonstallsystem (postional numeration system)
Tallsystem der et reelt tall representeres av et ordnet tegnsett på en slik måte at bidraget fra et tegn avhenger av både dets posisjon og dets verdi.

presisjon (precision)
Evnen til å skille mellom verdier som er nesten like.
[Norsk dataordbok, ISO]
Særlig aktuelt for flytende tall, der presisjonen er avhengig av antall biter i representasjonen av mantissen.

privat nøkkel (private key)
Krypteringsnøkkel brukt i asymmetrisk kryptering, knyttet til en bestemt juridisk person og bare kjent av denne. Del av et nøkkelpar, den andre nøkkelen er den offentlige nøkkelen.

protokoll (protocol)
Sett med regler som fastlegger hvordan enheter bestående av maskin og programvare kan gjennomføre datakommunikasjon.
[Norsk dataordbok, ISO, modifisert]

signalhastighet (signaling speed)
Hvor fort et signal forplanter seg gjennom et samband. Måles i meter per sekund, m/s. I trådløse samband er signalhastigheten lik lyshastigheten, dvs. $3 * 10^8$ m/s. I trådbundne samband er signalhastigheten omlag 2/3 av lyshastigheten, dvs. $2 * 10^8$ m/s

steganografi (steganography)
Egentlig "hemmelig skrift", brukt om å skjule en melding i en annen melding, kalt *dekke*. Bilder blir ofte brukt som dekke fordi de inneholder mange biter og fordi endringer er vanskelige å observere.

stilark (Style Sheet)
Et stilark inneholder spesifikasjoner for utseendet på en nettside, som for eksempel fonter, farger på tekster og bakgrunner og plassering av tekster og bilder. Stilark betegnes ofte som CSS (Cascading Style Sheet) fordi stiler kan angis på flere nivåer og det finnes presendensregler som bestemmer hvilken spesifikasjon som skal brukes i hvert enkelt tilfelle. Standardisert av W3C.

streng (string)
Endimensjonal sekvens av tegn.
[Norsk dataordbok, ISO, noe modifisert]

surrogatpar (surrogate pair)
i UNICODE: Et par av 16-bits verdier mellom henholdsvis 0xD800 – 0xDBFF (high surrogate) og 0xDC00 – 0xDFFF (low surrogate). Disse verdiene brukes for å beregne et kodepunkt S i de 16 planene over Basic Multilingual Plane (BMP). Formelen som brukes er S = (high – 0xD800) * 0x0400 + (low – 0xDC00) + 0x10000. På denne måten kan alle kodepunktene representeres i BMP, men noen av disse representasjonene vil være på 32 biter. Verdier i området 0xD800 – 0xDFFF kan derfor ikke brukes som kodepunkter.

symmetrisk kryptering (symmetric cryptography)
Kryptering der vi bruker samme nøkkel både for å kryptere og dekryptere.

tallord (numeral)
Diskret representasjon av et tall. En streng som representerer et tall. Eks.: 3, trettitre, 33 og XXXIII.
[Norsk dataordbok, ISO]

tegn (character)
Den minste komponent som har semantisk verdi i et skrevet språk; betegner den abstrakte betydningen/formen, ikke en spesifikk visualisering (se også glyf). I kodetabeller må imidlertid tegn visualiseres i form av glyfer for å gjøre tabellene forståelige for brukeren.
[etter www.unicode.org/glossary/]

transportlag (transport layer)
Et lag (i nettverksprotokoller) som har som oppgave å transportere data fra endesystem til endesystem. Benytter tjenester fra det underliggende nettverkslaget. Eksempler på protokoller: TCP, UDP

UNICODE
Standard for koding og representasjon av tegn, med plass for over 1 million kodepunkter – se www.unicode .org. Kodepunktene kan representeres på ulike måter, de viktigste er UTF-32, UTF-16 og UTF-8. Unicode-standardiseringsorganisasjonen samarbeider med ISO, som har en parallell standard ISO 10646.

UTF-32
UNICODE representasjon som bruker 32 biter (4 bytes) for et kodepunkt. Kodepunktet representeres direkte. Siden kodepunktene i gjeldende standard kan representeres med 21 biter, fylles opp med ledende 0-biter til 32 biter.

UTF-16
UNICODE representasjon som bruker 16 biter (2 bytes) for et kodepunkt. Kodepunkter i Basic Multilingual Plain representeres direkte. For å kunne representere kodepunkter utenfor Basic Multilingual Plain, er en del av dette (2 områder på 4*256) avsatt for surrogatpar. Disse områdene inneholder altså ikke vanlige kodepunkter.

UTF-8
UNICODE representasjon som bruker fra 8 til 32 biter (1 til 4 bytes) for et kodepunkt. Kodepunkter som er felles med ASCII representeres direkte etter innsetting av et ledende 0-bit. Andre kodepunkter representeres på formen
1...10x..x 10xxxxxx ... 10xxxxxx, der antall 1-biter i første byte angir hvor mange bytes som brukes for representasjonen, og xxxxxxxx inneholder bitene for verdien av kodepunktet.

XHTML
Standard utarbeidet av W3C for markering (”tagging”) av tekster som skal vises fram av en nettleser. Bygger på XML. Hvilke XML-markeringer etc. som er tillatt er spesifisert i dokumenttypedefinisjoner utarbeidet av W3C.

XML-dokument (XML document)
Fil som inneholder en tekst bestående av XML-elementer, samt innledende <?xml ...> og eventuell dokumenttypedeklarasjon.

XML-dokument, gyldig (valid XML-document)
Et XML-dokument som er velformet, og som tilfredsstiller kravene spesifisert i en dokumenttypedefinisjon eller et XML-skjema som XML-dokumentet henviser til gjennom en dokumenttypedeklarasjon.

XML-dokument, velformet (well-formed XML-document)
Et XML-dokument der strukturen som dannes av XML-elementer avgrenset av start- og sluttmarkeringer danner en sammenhengende trestruktur med én rot.

XML – Extensible Markup Language
Standard utarbeidet av W3C for markering (”tagging”) av tekster for å kunne legge inn opplysninger om teksten. Se også XML-markering.

XML-element (XML element)
Den delen av et XML-dokument som omsluttes av en startmarkering og den tilhørende sluttmarkering.

XML-markering (XML tag)
Streng som settes inn i et XML-dokument for å legge inn opplysninger om teksten. Strengen begynner alltid med < og avsluttes med >. XML-markeringer opptrer alltid i par, en startmarkering og en sluttmarkering. Sluttmarkeringen skal bestå av samme streng som startmarkeringen, bortsett fra at tegnet / skal skytes inn som andre tegn i strengen. Eksempel: <dette_er_en_XML-markering> markert tekst </dette_er_en_XML-markering>. Startmarkeringen kan inneholde attributter med verdier: <dette_er_en_XML-markering attributtnavn="verdi", ...>. Hvis det ikke finnes noen markert tekst, kan startmarkering og sluttmarkering kombineres i én streng (legg merke til plasseringen av /-tegnet):
<dette_er_en_kombinert_start_og_sluttmarkering/>.

XML-skjema (XML Schema)
Spesifiserer hva som er gyldig struktur i et XML-dokument, spesielt hvilke XML-markeringer som skal brukes, hvilke attributter som er tillatt, og hvordan XML-elementene skal kunne nøstes. Erstatter etter hvert DTD.

(XSLT = Extensible Style Sheet Language Translator)
Program som kan transformere en tekst på grunnlag av regler spesifisert i en XSLT-fil. Brukes ofte for å transformere et XML-dokument til en XHTML-fil som kan vises fram av en nettleser.