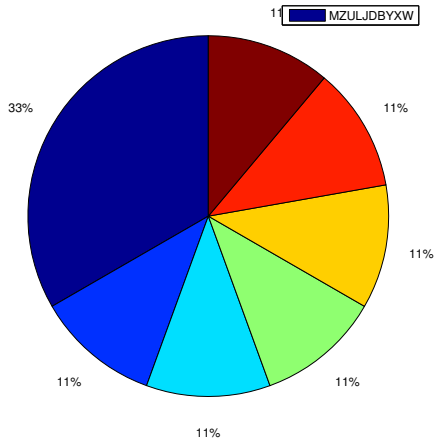
DN1212, Numeriska metoder och grundläggande programmering
– Laboration 3 –
Kryptering

Denna uppgift behandlar hantering av text som data.

Kryptografi har blivit en del av vår vardag även om vi inte tänker så mycket på det. När du loggar in på din personliga banksida eller pratar i mobiltelefonen sker kommunikationen krypterat. När man använder kryptering konverterar man en klartext till en kryptotext med hjälp av en krypteringsmetod och vanligen dessutom en krypteringsnyckel. Att konvertera tillbaka kallas att dekryptera. Om man inte känner till krypteringsmetod eller nyckel måste man gissa för att återfinna klartexten. Att göra det systematiskt kallas att forcera kryptotexten.

I denna laboration ska du skriva ett program som forcerar en krypterad text där vi vet krypteringsmetoden men själva måste hitta nyckeln och sedan dekryptera texten. Ditt program ska läsa och dekryptera en text på engelska som finns på fil. På kursens hemsida (länkad under "Laborationer") finns krypterade filer att utgå ifrån när du testar ditt program. Kopiera dessa filer till ditt eget bibliotek.

Det finns många olika algoritmer för kryptering men vi forutsätter att texten är krypterad med "caesarrullning" vilket innebär att varje bokstav har bytts ut mot en bokstav ett visst antal steg framåt i alfabetet. Nyckeln är antalet positioner man rullar. Med 2 positioners rullning blir "The zebra has stripes" krypterat till "Vjg bgdtc jcu uvtkrgu". Med vetskap om att "e" är den vanligaste bokstaven i engelsk text kan texten forceras med hjälp av ett frekvensdiagram. Om t ex bokstaven "g" är den mest frekventa i kryptotexten kan man gissa att rullningen är 2 steg.



Ditt program ska läsa in den krypterade texten (inklusive blanktecken och radbytestecken) från en fil till en vektor bestående av tecken. Skriv även ut den krypterade texten på skärmen. Därefter visas ett frekvensdiagram (använd t ex `pie` i MATLAB) över de 10 mest frekventa bokstäverna i den krypterade texten. Det blir enklare om du först gör om alla bokstäver till versaler. Därefter väljer du antal rullningssteg och skriver ut texten efter rullning. Ditt program bör lämna andra tecken än bokstäver oförändrade. När texten visar en vettig mening är rullningen korrekt.

En trevlig bok om kryptering är Simon Singh, “Kodboken”. I slutet av boken finns en dekrypteringstävling som var öppen för alla i hela världen att försöka knäcka. Först ut att lösa detta krypto var ett gäng Datalogi-doktorander från KTH.

MZDLB UJMM!