**Framtiden av kryptografi**

Vi lever idag i ett högst digitalt samhälle. Och vart man än ser så finns det tjänster som kräver konton. Allt ifrån Försvarsmaktens största hemligheter till din Netflix-historik ligger gömd bakom massvis med kryptografi. Kryptografi är läran om att transformera information så att det blir felaktigt i sin olösta form. Denna konsten har funnits ända sedan antiken, faktum är att ett av de mest välkända metoderna, ceasarförskjutning, kommer från romarrikets Julius Ceasar själv. Idag finner man inte riktigt Ceasarförskjutning utanför klassrummet, då det är väldigt enkelt att knäcka, men man utgår även idag från samma principer som romarna. Men hur fungerar det idag då?

Jo, den vanligaste metoden är så kallad Hashing. Hashing går ut på att klienten, den som ska ha åtkomst till informationen, och servern, den som ska tilldela informationen, båda har en s.k. ”nyckel” som är unik för just klientens konto. Du loggar in med lösenordet på din dator, men innan det skickas till servern, så krypteras det med denna ”nyckel”. Detta gör att lösenordet blir praktiskt taget oläsligt för någon som inte har tillgång till nyckeln. När den krypterade strängen av karaktärer kommer fram till servern så använder den nyckeln för att dekryptera meddelandet igen, vilket ger servern det originella lösenordet. Det här kan kännas ganska säkert, men hur kommer det se ut i framtiden?

Först måste vi förstå oss på hur datorer ser bokstäver; Datorer talar inte i vårat språk, inte ens heller i språk som Python, Java, eller C++. Datorer talar i sin renaste form i ettor och nollor, och varje bokstav och symbol i vårat alfabet har en sträng med ettor och nollor associerad med sig. Varje etta eller nolla representerar en transistor i datorn som är på (1) eller av (0). En sak i framtiden som kan problematisera detta är uppkomsten av så kallade kvantumdatorer. Kvantumdatorer är baserade på qubits, som kan vara både ettor och nollor samtidigt pga något som kallas superpositionering (vilket vi inte kommer gå in på nu). Detta innebär att en kvantumdator i teori kan testa alla möjliga kombinationer av ettor och nollor på ett ögonblick, och därför få omedelbar åtkomst till vilket konto som helst.

Detta må låta obehagligt, men kvantumdatorer är i ett väldigt tidigt stadie av utveckling, och den mest kraftfulla kvantumdatorn som finns, byggd av IBM, är ungefär en hundradel så kraftfull som den måste vara för sådan här kodknäckning. Och faktumet är att vi redan har kommit en lång bit på vägen till att utveckla s.k. kvantumsäkra lösningar. Så var inte orolig, kryptografin kommer som så många gånger förut hjälpa oss att hålla information tillgänglig till den som ska ha den.