Räkna med slutsiffran

$8+5=13$. Slutsiffran i svaret är 3. Om vi bara bryr oss om slutsiffran och bortser från att svaret har en etta som första siffra skriver vi $8+5\equiv 3$. Man använder alltså ett likhetstecken med tre streck. Metoden kallas för ”räkning modulo tio”, förkortat ”mod10”.

(Egentligen ska man skriva $[8]+[5]\equiv[3]$, men ofta ”fuskar” man av bekvämlighetsskäl.)

Om man tar tex. talet 8 och adderar 10, så händer ingenting med slutsiffran: $8+10=18$. Men vi bryr oss bara om sista siffran i varje tal och därför skriver vi, i detta nya sammanhang, $8+0\equiv 8$. Det ”händer alltså ingenting” med slutsiffran då man adderar vilket tal som helst, som slutar med en nolla.

I skolan brukar man träna barnen på att finna ”tiokamrater”, alltså tal vars summa blir tio. Ett exempel är talen 4 och 6, eftersom $4+6=10$. Med vårt nya sätt att skriva blir detta $4+6\equiv 0$.

Antag nu att Gustav vill skriva ned ett hemligt nummer, tex. 749, på en lapp åt Erik, men att ingen annan ska få reda på numret. Ett sätt är att gömma lappen på ett ställe där bara Erik kan hitta den. Ett annat sätt vore följande:
Gustav kan addera 4 till varje siffra i numret och sedan bara notera slutsiffrorna som uppstår.

$$7+4\equiv 1,\ 4+4\equiv 8 \text{ och } 9+4\equiv 3.$$

Gustav kan alltså skriva numret 183 på lappen och behöver inte smussla med den längre. Ingen kan ju ana att det rätta numret är 749, när det står 183 på lappen.

Men Erik måste få veta att han ska addera 6 till varje siffra i numret och bara beakta slutsiffran i de tal som då uppstår. Erik gör alltså följande uträkningar:

$$1+6\equiv 7,\ 8+6\equiv 4 \text{ och } 3+6\equiv 9.$$

Därmed har Erik fått fram 749, som ju var det ursprungliga numret.

At metoden fungerar beror ju på att slutsiffran inte ändras då man adderar ett tal med 0 som slutsiffra och att $4+6\equiv 0$.

”Addera 4” kallas för krypteringsnyckel, och ”Addera 6” kallas för dekrypteringsnyckel. Exemplet är ett elementärt *osymmetriskt* krypto, alltså ett krypto med olika nycklar för kryptering och dekryptering.

Man brukar även kalla sådana krypton för *krypton med öppen krypteringsnyckel*. Gustav kunde nämligen skriva på en anslagstavla att alla som vill skicka honom ett hemligt nummer ska kryptera detta genom att addera exempelvis talet 3 och sedan bara bry sig om att notera slutsiffran. Gustav vet ju i så fall att man får fram det korrekta numret genom att addera 7. Det ska han ju naturligtvis inte berätta för någon. Men, i sanningens namn, så är ju detta ganska lätt att genomskåda utan större skarpsinnighet. Men ovanstående är ett exempel på hur ett asymmetriskt krypto fungerar.

Man kan komplicera det hela och så småningom komma fram till världens mest svårforcerade krypton, nämligen RSA-krypton. Alla steg på vägen dit skulle jag tro att Gustav och Erik faktiskt skulle kunna förstå.

Några små utmaningar tänkte jag härmed föreslå, till att börja med.

1. Hur kan man med ovanstående teknik göra så att två personer bara kan få reda på ett hemligt nummer samtidigt, tex. koden till ett kassaskåp?
2. Om man går över från addition till multiplikation, varför fungerar då endast nyckelparen $(3,7)$, $(7,3)$ och $(9,9)$?

3. Alfabetet består av 28 bokstäver. Dessutom finns mellanslag och ett antal skiljetecken. Genom att addera och räkna med de två sista siffrorna kan man åstadkomma ett assymetriskt krypto för textmeddelanden. Något att ta sig an?
   (Normalt brukar man bara använda versaler vid kryptering av text. Varken mellanslag eller skiljetecken brukar krypteras. Men, då blir klartexten svårläst för den otränade.)
4. Försök finna nyckelpar som fungerar under multiplikation när man räknar med de två sista siffrorna!
5. Varför kan man inte använda 0 som nyckel vid krypteringen, varken när man använder addition eller multiplikation?
6. Varför kan man inte använda 1 som nyckel vid multiplikation?