KRYPTOGRAFIAN ALKEET

6. RÄKNEÖVNINGEN

Eftersom denna övning är den sista på kursen, innehåller den förutom elliptiska kurvor även repetitionsuppgifter.

(1) Följande uppgifter är alternativa. I båda beräknar man ordningar. Notera att ifall ordningen för punkten P är n, så är ordningen för punkten jP även n, ifall $\text{sgd}(n, j) = 1$, och $\frac{n}{\text{sgd}(n,j)}$ annars.
   (a) I uppgift 5a) i förra räkneövningen betraktade vi kurvan $y^2 = x^3 + 200x + 192$, och dess punkter räknades upp. Använd nu en dator för att beräkna ordningen för alla punkter på kurvan.
   (b) Beräkna ordningen för alla punkter på kurvan $y^2 = x^3 - 5x$ modulo 7.

(2) På den elliptiska kurvan $y^2 = x^3 + 9x + 17$ modulo 23 har punkten $P = (16, 5)$ ordningen 32. Dra utgående från detta slutsatsen att P är en generator för kurvan (alltså att man som multiplar av P får alla punkter på kurvan).

(3) Nedan finns en lista på multiplarna av punkten $P = (16, 5)$ på kurvan $y^2 = x^3 + 9x + 17$ modulo 23:

$P = (16, 5)$	$2P = (20, 20)$	$3P = (14, 14)$	$4P = (19, 20)$
$5P = (13, 10)$	$6P = (7, 3)$	$7P = (8, 7)$	$8P = (12, 17)$
$9P = (4, 5)$	$10P = (3, 18)$	$11P = (5, 7)$	$12P = (18, 10)$
$13P = (1, 21)$	$14P = (10, 7)$	$15P = (15, 10)$	$16P = (17, 0)$
$17P = (15, 13)$	$18P = (10, 16)$	$19P = (1, 2)$	$20P = (18, 13)$
$21P = (5, 16)$	$22P = (3, 5)$	$23P = (4, 18)$	$24P = (12, 6)$
$25P = (8, 16)$	$26P = (7, 20)$	$27P = (13, 13)$	$28P = (19, 3)$
$29P = (14, 9)$	$30P = (20, 3)$	$31P = (16, 18)$	$32P = O$

   Antag att Alice vill ta emot meddelanden som är krypterade med ElGamals system med nyckeln $(23, (16, 5), (1, 2))$. Använd ovanstående lista för att skicka henne meddelandet $(12, 17)$.

(4) Alice och Bob vill ha ett gemensamt lösenord. De besluter sig för att använda Diffie-Hellmanns nyckelutbytesprotokoll på den elliptiska kurvan $y^2 = x^3 + 9x + 17$ (mod 23) (se uppgift 3). Alice väljer talet 7 och Bob väljer talet 5. Vad blir deras gemensamma lösenord?

(5) Välj ett primtal p och någon elliptisk kurva. Generera en offentlig nyckel åt dig själv enligt ElGamals system.

(6) Vi använder Hills krypteringssystem i ett alfabet med 26 tecken med matrisen

$$\begin{pmatrix} 5 & 2 \\ 11 & 5 \end{pmatrix}.$$

Bestäm matrisen som behövs för att dekryptera meddelandet (kom ihåg att alla operationer utförs modulo 26), och kontrollera lösningen genom att först kryptera och sedan dekryptera ordet “sana”.

(7) Välj de nödvändiga parametrarna och beräkna den offentliga och den hemliga nyckeln i RSA.