Tentamen cryptografie

(Licht bewerkt voor tentamenbundel DESDA)

Tussen [haakjes] staat het aantal punten dat je voor deze opgave kunt halen. Het maximum aantal punten is 45.
Je cijfer voor dit tentamen is 1+(behaalde punten)x0.2 .

Opgave 1. [10] Een cryptosysteem gebaseerd op RSA heeft als publieke gegevens N, een product van twee onbekende priemgetallen p, q. Twee gebruikers A en F gebruiken dezelfde N, en hebben respectievelijk publieke sleutels 17 en 37. Bob stuurt hetzelfde bericht $m \in \mathbb{Z}/N\mathbb{Z}$ naar hen beide, en stuurt dus publiekelijk de ciphertexten c_1 en c_2. Leg uit hoe een "eavesdropper" het bericht m kan achterhalen.

$c_1 = m^{17}, c_2 = m^{37}$. Vind nu gehele getallen a, b zodat $17a + 37b = 1$, bijvoorbeeld $a = 24, b = -11$. Dan $c_1^a c_2^b = m$.

Een kleine reminder: als G een abelse groep is van p^n elementen, dan is de groep isomorf met

$$\mathbb{Z}/(p^{n_1}\mathbb{Z}) \times \mathbb{Z}/(p^{n_2}\mathbb{Z}) \times \cdots \times \mathbb{Z}/(p^{n_m}\mathbb{Z})$$

waar $n_1 + n_2 + \ldots + n_m = n$. (Speciaal geval van de klassificatie van abelse groepen.)

Opgave 2. [15] Een elliptische kromme E over $\mathbb{F}_p$ heeft als vergelijking $y^2 = x^3 + ax + b$ voor bepaalde $a, b \in \mathbb{F}_p$. Na wat rekenwerk vinden we alle oplossingen $(x, y) \in \mathbb{F}_p^2$ van de vergelijking. We vinden $P_1 = (a_1, b_1)$ t/m $P_8 = (a_8, b_8)$. De groep horend bij de elliptische kromme noemen we G.
a) [2] Welke groep kan G zijn?
b) [7] Gegeven is dat $P_1 + P_2 \neq \mathcal{O} \in G$. Het blijkt dat de lijn door P_1 en P_2 geen derde snijpunt met E oplevert. Wat is er aan de hand? Wat kan $P_1 \oplus P_2$ zijn?
c) [6] Gegeven is dat $P_4 \oplus 2P_5 = \mathcal{O}$, en dat $2P_4 \oplus P_5 \neq \mathcal{O}$ (waar $\mathcal{O}$ voor het nulelement in G staat). Bepaal welke groep G is.

a) Er zijn 8 punten en natuurlijk $\mathcal{O}$, dus 9 punten en de groep kan dus $\mathbb{Z}/9\mathbb{Z}$ of $\mathbb{Z}/3\mathbb{Z}^2$ zijn. Typische fout zal zijn : groep heeft 8 elementen.
b) Dan is de lijn een raaklijn in P_1 of P_2, en is dus $2P_1 \oplus P_2 = 0$ of $P_1 \oplus 2P_2 = 0$.
c) Je hebt dus $(P_4 \oplus 2P_5) + (2P_4 \oplus P_5) \neq \mathcal{O}$. Dus $3(P_4 \oplus P_5) \neq \mathcal{O}$. Dat kan niet in de groep $(\mathbb{Z}/3\mathbb{Z})^2$, en dus is het de groep $\mathbb{Z}/9\mathbb{Z}$.
Mocht je 8 elementen hebben gedahct bij a) (dat blijken toch wel meer studenten te zijn dan gedacht), dan kun je niet zoveel (en loop je dus punten mis). Iets wat kan is dat je dus afleidt dat $3(P_4 + P5) = 0$ en omdat er in een groep met 8 elementen geen lementen van orde 3 zijn behalve het eenheidselement, moet er gelden dat $P_4 + P_5 = 0$. En dan houdt het wel een beetje op.

Opgave 3. [10] Van een symetrisch cryptosysteem is gegeven dat het per bericht een nieuwe sleutel k gebruikt. De mogelijke berichten zijn: willekeurige "woorden" van lengte 5 m.b.v. de 26 letters A,B, C,..., Z. De sleutels zijn getallen uit $\mathbb{Z}/N\mathbb{Z}$ waar N een product is van twee priemgetallen van 9 cijfers. De ciphertexts worden binaire codes (i.e. bestaand uit 0 en 1) bestaande uit 60 bits.

In de bijgeleverde beschrijving wordt beweerd dat dit systeem "perfect security" heeft. Kan dit het geval zijn bij deze parameters?

$\#P = 26^5$, $\#K = N$, $\#\mathbb{C} = 2^{60}$. Als je perfect security hebt, dan moet je hebben dat $\#K \geq \#C \geq \#P$.
$13^5 = 371293 < 524288 = 2^{19}$ dus $\#P = 26^5 = 2^5 13^5 < 2^{24} < 2^{40} = \#\mathbb{C}$. Dus dat is OK. Hoe vergelijken $\#\mathbb{C}$ en $\#K = N$? N is een product van twee priemgetallen met 9 cijfers. Dus $N < 10^9 10^9 = 10^{18}$. Laten we dat eens vergelijken, hoe verhoudt 10^{18} zich tot 2^{60}? Blijkbaar is $2^{60} = 1.1529215x10^{18}$.
Dus $\#K < \#C$ en dus is er geen perfect security.

Opgave 4. [10] Beschrijf het Schnorr protocol. Het is van belang om te vertellen wat in welke volgorde door wie berekend wordt (geef elk van de 3 stappen), je hoeft *niet* te bewijzen of uit te leggen waarom dat in die volgorde gebeurt e.d. Je hoeft alleen maar te vertellen wat wie berekent in welke stap.