Authenticatie met privacy én veiligheid (opgaven en antwoorden)

Greg Alpár, greg.alpar@ou.nl

August–September 2018

Opgave 5.3.6. In de definitie hierboven hadden we $x \in \mathbb{Z}_n^*$ moeten schrijven. Maar de kans dat $x \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ is zeer klein. Wat is deze kans? Toon aan dat als je een element in deze verschilverzameling hebt, dat je dan de priemfactoren van n kunt vinden.
Antwoord: $|\mathbb{Z}_n| = |\{0, 1, 2, \ldots, n-1\}| = n$ en $|\mathbb{Z}_n^*| = |\varphi(n)| = (p-1)(q-1)$ (het aantal gehele getallen relatief priem met n). De kans is dan $1 - \frac{(p-1)(q-1)}{n} = \frac{p+q-1}{pq} \approx \frac{2\sqrt{n}}{n} = \frac{2}{\sqrt{n}}$ (p en q zijn over het algemeen van dezelfde bit-lengte). In de praktijk is $\sqrt{n}$ minstens 1024 bits lang, omdat p en q dat ook zijn. De kans is dan $\frac{1}{2^{1023}}$, d.w.z. praktisch 0.
Als je een $x \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ vindt, dan $\gcd(x, n) > 1$, wat betekent dat x deelbaar is door p of q. Omdat de ggd efficiënt berekend kan worden met het algoritme van Euclides kunnen we de priemfactoren van n nu makkelijk vinden.
Omdat de kans om zo'n getal te vinden verwaarloosbaar is, en het verschil tussen de twee verzamelingen geheim is, is er praktisch geen verschil tussen $x \in \mathbb{Z}_n^*$ en $x \in \mathbb{Z}_n$.

Opgave 5.3.8. Om met dit idee te experimenteren, rekenen we eerst in een groep van priem-orde. Welke paren (a, e) voldoen aan de vergelijking $5 \equiv a^e \pmod{p}$ als *(a)* $p = 7$ of *(b)* $p = 11$?
Antwoord: *(a)* Als $p = 7$ dan bevatten de ondergroepen $\{1, 2, 4\}$ en $\{1, 6\}$ niet 5. Dus, slechts twee getallen brengen de hele groep voort: 1. $a = 3$. Omdat $\langle 3 \rangle = \{3, 2, 6, 4, 5, 1\}$, $e = 5$, d.w.z. $3^5 \equiv 5 \pmod{7}$; en 2. $a = 5$. Duidelijk is dat hier $e = 1$. De twee antwoorden zijn $(3, 5), (5, 1)$.
(b) Voor $p = 11$ brengen de elementen ondergroepen voort van de volgende ordes: 1, 10, 5, 5, 5, 10, 10, 10, 5, 2, voor respectievelijk de elementen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. (Merk op dat 10 $= -1$ in deze groep, die brengt een ondergroep met twee elementen voort.) Er zijn dus slechts 4 voortbrengers van de hele groep: 2, 6, 7 en 8.
Omdat 1 en 10 niet 5 kunnen maken door machtsverheffing, kunnen we die uitsluiten van de rest van de berekening.
Er zijn 12 verschillende oplossingen. Iedere voortbrenger geeft een unieke oplossing (a, e): $(2, 4)$, $(6, 6)$, $(7, 2)$, $(8, 8)$. Groepselementen van orde 5 geven elk twee aparte oplossingen, waarin de corresponderende exponenten 5 verschillen (de exponenten zijn hetzelfde modulo 5): $(3, 3), (3, 8)$, $(4, 2), (4, 7)$, $(5, 1), (5, 6)$, $(9, 4), (9, 9)$.

Opgave 5.3.9. Bewijs: als n en $|QR_n|$ bekend zijn, dan kan men de priemfactoren van n berekenen.
Antwoord: We weten dat $n = pq$ en $|QR_n| = \frac{(p-1)(q-1)}{4}$. Er zijn twee onbekenden en twee vergelijkingen, en ze zijn duidelijk onafhankelijk. Daarom kunnen p en q berekend worden.
Als we een constructief bewijs willen, dan kunnen we de priemfactoren ook uitrekenen. Door het stelsel vergelijkingen op te lossen vinden we een tweedegraads vergelijking: $p^2 - bp + n = 0$, waarbij $b = n - 4 \cdot |QR_n| + 1$ (in feite $b = p + q$). De twee oplossingen zijn de twee priemgetallen, omdat hun rollen symmetrisch zijn in de oorspronkelijke twee vergelijkingen:

$$p = \frac{b + \sqrt{b^2 - 4n}}{2} \quad \text{en} \quad q = \frac{b - \sqrt{b^2 - 4n}}{2}.$$

Opgave 5.3.10. Wat zijn de priemfactoren van $n = 853453$, als we weten dat $|QR_n| = 212887$?
Antwoord: Met de formule van de vorige opgave vinden we $p + q = b = 1906$ en de twee priemgetallen zijn 719 en 1187.

Opgave 5.3.12. Neem aan dat er een magische "clouddienst" bestaat die elk RSA-probleem kan oplossen. Hoe kun je die dienst gebruiken om de Sterke RSA-aanname te breken?
Antwoord: Laten we aannemen dat een voorbeeld van het Sterke RSA-probleem $a^e \equiv b \pmod{n}$ is, waarbij a en e onbekend zijn. Als we een oplossing kunnen vinden, dan is de Sterke RSA-aanname gebroken. Het enige verschil tussen een "normaal" en een Sterk RSA-probleem is dat de exponent vastligt in het eerste geval. Door *vrijelijk* een exponent $e := \bar{e}$ te kiezen, kunnen we het volgende RSA-probleem naar de magische clouddienst sturen: $a^{\bar{e}} \equiv b \pmod{n}$. De clouddienst komt met het unieke antwoord $\bar{a}$. Daarmee hebben we het Sterke RSA-probleem opgelost, en de oplossing is $a = \bar{a}$, $e = \bar{e}$.

Opgave 5.3.13. Een manier om alle elementen van de kwadraatrest-groep QR_n te bepalen is om alle elementen van $\mathbb{Z}_n^*$ te kwadrateren. Bijvoorbeeld, als $p = 7$ en $q = 11$, dan $|\mathbb{Z}_n^*| = (p-1)(q-1) = 60$ en $|QR_n| = 60/4 = 15$. De verzameling $QR_n = \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 8^2, \ldots, 76^2\}$ heeft ogenschijnlijk 60 elementen, maar in feite zijn er slechts 15 verschillende, die elk viermaal voorkomen. (Merk op dat $\mathbb{Z}_n^*$ alleen gehele getallen bevat die geen deler gemeen hebben met 77, d.w.z. met 7 en 11; bijv. 7, 66 en 70 zitten niet in de groep.)

Bedenk een andere manier om alle 15 elementen te berekenen.
Antwoord: In de beschrijving zien we dat QR_n een cyclische groep is. Dat betekent dat er minstens één voortbrenger is (in feite, $(p'-1)(q'-1)$, en dat is 8 in dit geval). Dus kunnen we één van de kwadraatresten kiezen en alle $|QR_n|$ elementen maken: bijv. $4, 4^2, 4^3, \ldots, 4^{15}$. Als een verkeerd element was gekozen (bijv. 9 – waarom brengt die niet QR_n voort?), die niet alle 15 elementen voortbrengt, probeer dan een andere.

Opgave 5.3.15. Beschouw L voortbrengers als in de definitie hierboven. Laat $\omega := |\langle g \rangle|$ de orde van de groep $\langle g \rangle$ zijn. Bewijs, aannemende dat de exponenten worden gereduceerd modulo ω, dat het aantal verschillende representaties ω^{L-1} is.
Antwoord: $L-1$ exponenten, zeg de eerste $L-1$, kunnen vrij worden gekozen uit $\{0, \ldots, \omega-1\}$, en de laatste is daardoor uniek bepaald. Merk op dat het berekenen van deze laatste unieke exponent een DL-probleem is. Op deze manier krijgen we alle representaties, en die zijn allemaal verschillend. Met de eerder gebruikte notatie: in een groep van priem-orde $\omega = q$, in een Sterk RSA-systeem, $\omega = |QR_n| = \frac{(p-1)(q-1)}{4}$.

Opgave 5.3.17. Gegeven de groep $\mathbb{Z}_{11}^*$ en drie voortbrengers: $2, 7, 8$. Bepaal minstens vier verschillende representaties voor 5, m.a.w., wat kunnen de exponenten zijn in het product $2^{x_1} \cdot 7^{x_2} \cdot 8^{x_3} \equiv 5 \pmod{11}$?
Antwoord: Uit opgave 5.3.8 weten we de discrete logaritme van 5 bij de grondtallen 2, 7 en 8: 4, 2 en 8, respectievelijk. Dit idee geeft drie representaties: $(\mathbf{0}, \mathbf{0}, \mathbf{8})$, $(\mathbf{0}, \mathbf{2}, \mathbf{0})$ en $(\mathbf{4}, \mathbf{0}, \mathbf{0})$.
In die opgave hadden we al alle getallen berekend die 2, 7 en 8 voortbrengen in deze groep. Daarmee vinden we makkelijk andere drietallen door willekeurig twee exponenten te kiezen en de derde dan op te zoeken. Bijvoorbeeld, $(\mathbf{3}, \mathbf{7}, \mathbf{4})$ is een representatie omdat $2^3 \equiv 8$, $7^7 \equiv 6$ en $8^4 \equiv 4 \pmod{11}$. Dus, $2^3 \cdot 7^7 \cdot 8^4 \equiv 5 \pmod{11}$.

Opgave 5.3.18. Neem aan dat we werken in een groep waarin de discrete logaritme-aanname geldt. Bewijs dat als in de vergelijking $H = \prod_{i=0}^{L} g_i^{x_i} \in \mathbb{G}$ alle getallen bekend zijn behalve x_0, dat het niet doenbaar is om een geldige representatie te vinden.
Antwoord: In dit geval hebben we $H = \prod_{i=0}^{L} g_i^{x_i} = g_0^{x_0} \prod_{i=1}^{L} g_i^{x_i}$. Dit betekent dat

$$g_0^{x_0} = H \cdot \left(\prod_{i=1}^{L} g_i^{x_i} \right)^{-1}$$

waarbij g_0 een voortbrenger is en de rechterkant is een concreet geheel getal. Dit is dus een discrete logaritme-probleem, dat moeilijk is volgens de aanname.

Opgave 5.3.20. Laten we nu een situatie nemen van Sterke RSA, waarbij n het product van twee veilige priemgetallen is, en QR_n de kwadraatrest-ondergroep van Z_n^*. Gegeven een voortbrenger R en extra voortbrengers $(R_1, \ldots, R_L) \in \langle R \rangle^L$, wat is het Pedersen-commitment $C(a_1, \ldots, a_L)$ voor L waarden $(a_1, \ldots, a_L)$? Bewijs ook dat $C(a_1, \ldots, a_L) \in QR_n$.
Antwoord: $C(a_1, \ldots, a_L) = R^a \cdot \prod_{i=1}^{L} R_i^{a_i}$, waarbij $a \in_R \mathcal{I}$, waarbij $\mathcal{I}$ een groot interval $\{0, 1, 2, 3, \ldots, 2^\ell\}$ is (ℓ is een veiligheids-parameter[1]).
We weten dat $(R_1, \ldots, R_L) \in \langle R \rangle^L$, en dus kan $C(a_1, \ldots, a_L)$ worden geschreven als een macht van R. Aangezien R een voortbrenger is van QR_n, is het resulterende element $(R^{\cdots})$ ook in QR_n.

Opgave 5.3.21. Neem aan dat we weer toegang hebben tot de magische clouddienst die het DL-probleem kan oplossen. Bewijs dat een committeerder in dit geval vals kan spelen. Bewijs ook dat niemand anders dat kan. (Hint: Bedenk eerst wat "vals spelen" betekent in deze twee gevallen.)
Antwoord: 1. De committeerder kan valsspelen. "Valsspelen" is in dit geval dat de committeerder de exponenten kan veranderen zonder de waarde van het commitment te veranderen. Met toegang tot de clouddienst kan de committeerder simpelweg alle exponenten $(\bar{a}_1, \ldots, \bar{a}_L)$ vrij kiezen (zij kan dit zelfs doen als ze niet de originele waarden kende), en ze geeft het volgende discrete logaritme-probleem aan de clouddienst:

$$\left(g,\ C(a_1, \ldots, a_L) \cdot \prod_{i=1}^{L} g_i^{-\bar{a}_i} \right),$$

en die zal $\bar{a}$ teruggeven zodat $C(a_1, \ldots, a_L) = g^{\bar{a}} \cdot \prod_{i=1}^{L} g_i^{\bar{a}_i}$. Merk op dat nu $C(a_1, \ldots, a_L) = C(\bar{a}_1, \ldots, \bar{a}_L)$, wat precies is wat een valsspelende committeerder wil.
2. Anderen kunnen niet valsspelen. "Valsspelen" betekent in dit geval dat iemand anders achter enkele of alle exponenten zou kunnen komen. Maar dat is onmogelijk vanwege de randomiseerder a. Zelfs als iemand een geldige representatie voor $C(a_1, \ldots, a_L)$ m.b.t. $(g, g_1, \ldots, g_L)$ zou kunnen vinden, is er geen manier om er achter te komen of dit degene is waaraan de committeerder zich gecommitteerd had, omdat voor elk rijtje $(a_1, \ldots, a_L)$ er een exponent a is die het commitment geldig maakt.

Opgave 5.3.22. Wat is de CL-handtekening over één attribuut? Hoe kan deze handtekening worden geverifieerd?
Antwoord: De CL-handtekening op één attribuut wordt gemaakt door eerst priemgetal e en v random te kiezen, en dan

$$A := \left(\frac{Z}{S^v R^a R_1^{a_1}} \right)^{1/e \pmod{\varphi(n)}} \pmod{n}$$

te berekenen. De handtekening is (A, e, v) op attribuut a_1.
De handtekening kan geverifieerd worden met de publieke sleutel van de ondertekenaar (Z, S, R, R_1), de handtekening (A, e, v) en het attribuut a_1 samen met de (Pedersen) randomiseerder a:

$$Z \stackrel{?}{\equiv} A^e \cdot S^v \cdot R^a \cdot R_1^{a_1} \pmod{n}.$$

Opgave 5.3.23. Bewijs dat de gerandomiseerde handtekening $(\bar{A}, e, \bar{v})$ over hetzelfde bericht geldig is.
Antwoord: Inderdaad, deze gerandomiseerde handtekening is ook geldig voor R' (dat is, op de attributen):

$$\bar{A}^e S^{\bar{v}} R' \equiv A^e S^{-er} S^v S^{er} R' \equiv A^e S^v R' \equiv Z \pmod{n}.$$

Opgave 5.3.24. Bewijs dat de verificatie-vergelijking in Schnorr's identificatie inderdaad geldt, mits de bewijzer de juiste geheime waarde x gebruikt.
Antwoord: We moeten de correctheid van de verificatie-vergelijking bewijzen. Omdat $r \equiv cx + w \pmod{q}$ en $h \equiv g^x \pmod{p}$, krijgen we $g^r \cdot h^{-c} \equiv g^{cx+w} \cdot g^{x-c} \equiv g^{cx} \cdot g^w \cdot g^{-cx} \equiv g^w \equiv a \pmod{p}$. Dus, $a \equiv g^r \cdot h^{-c} \pmod{p}$.

[1] In de praktijk, als de grootte van de RSA-modulus 2048 bits is, dan $\ell = 256$.

Opgave 5.3.26. Wat is het bewijs van kennis als de gebruiker het tweede en vijfde attribuut uit een credential met vijf attributen wil tonen? Dus deze twee attributen zijn gemeenschappelijke input voor de bewijzer en de verifieerder. Maak de volgende componenten expliciet: de publieke en privé-sleutel van de uitgever, de gerandomiseerde handtekening, de privé-sleutel van de gebruiker, de attributen en het bewijs.
Antwoord: De publieke sleutel van de uitgever is $n, Z, A, S, R, R_1, R_2, R_3, R_4, R_5$. Zijn privé-sleutel is de priemfactoren van n: p, q. De gerandomiseerde handtekening is $(\bar{A}, e, \bar{v})$ op de attributen $(a_1, a_2, a_3, a_4, a_5)$. De privé-sleutel van de gebruiker is a.
De attributen a_2, a_5 wetende, kan de verifieerder $R_2^{-a_2} R_5^{-a_5}$ berekenen, en dat vermenigvuldigen met Z. De bewijzer en de verifieerder kunnen dan samenwerken om het volgende kennisvrije bewijs te maken:

$$\mathrm{PK}\{e, \bar{v}, a, a_1, a_3, a_4 | Z R_2^{-a_2} R_5^{-a_5} \equiv \bar{A}^e \cdot S^v \cdot R^a R_1^{-a_1} R_3^{-a_3} R_4^{-a_4} \pmod{n}\}.$$