Kryptologie 2 Sommersemester 2010
Johannes Köbler, Sebastian Kuhnert 19. Mai 2010

Übungsblatt 6

Aufgabe 44 ***mündlich***

Betrachten Sie die folgende Variante des ElGamal-Signaturverfahrens. Die Schlüssel werden ähnlich wie beim ElGamal-Signaturverfahren generiert: p ist prim, α ist ein Erzeuger von $\mathbb{Z}_p^*$, a ist der geheime Exponent und $\beta = \alpha^a \bmod p$. Allerdings wird a jetzt aus $\mathbb{Z}_{p-1}^*$ (anstelle von $\mathbb{Z}_{p-1}$) gewählt. Ein Dokument $x \in \mathbb{Z}_p$ wird unter $\hat{k} = (p, \alpha, a)$ mit $sig(\hat{k}, x, z) = (\gamma, \delta)$ signiert, wobei gilt:

$$\gamma = \alpha^z \bmod p \text{ und } \delta = (x - z\gamma)a^{-1} \bmod (p-1) \ .$$

Dieses Verfahren unterscheidet sich also auch in der Berechnung von δ.

(a) Beschreiben Sie, wie sich die Unterschrift (γ, δ) eines Dokuments x bei Kenntnis des Verifikationsschlüssels $k = (p, \alpha, \beta)$ verifizieren lässt.

(b) Welchen Vorteil bei der Berechnung der Signatur besitzt diese Variante gegenüber dem ursprünglichen Verfahren?

Aufgabe 45 ***mündlich***

Berechnen Sie den diskreten Logarithmus $\log_\alpha \beta$ in $\mathbb{Z}_p^*$ mit dem ρ-DLP-Algorithmus von Pollard für $p = 458009$, $\alpha = 2$ und $\beta = 56851$.

Hinweis: Die Ordnung von α in $\mathbb{Z}_p^*$ ist $n = 57251$. Benutzen Sie den Pseudozufallsgenerator aus der Vorlesung mit dem Startwert $x_0 = 1$.

Aufgabe 46 ***mündlich***

Sei A ein generischer DLP-Algorithmus für die Berechnung des diskreten Logarithmus $\log_\alpha \beta$ über der additiven Gruppe $\mathbb{Z}_{19}$, deren Elemente durch zufällig gewählte Bitstrings der Länge 5 kodiert sind. Wir nehmen an, dass A bei Eingabe $\alpha = 01100$ und $\beta = 10111$ zur Berechnung der Gruppenelemente $\alpha^c\beta^d$ die Orakelfragen (c, d) für alle Paare in der Menge

$$C = \left\{(1 - i^2 \bmod 19, i \bmod 19) \;\middle|\; i = 0, 1, 2, 4, 7, 12\right\}$$

stellt.

(a) Berechnen Sie $Good(C)$.

(b) Angenommen, A erhält folgende Orakelantworten:

$(1,0)$	$(0,1)$	$(16,2)$	$(4,4)$	$(9,7)$	$(9,12)$
01100	10111	00110	01010	00100	11001

Welche Information lässt sich hieraus über den Wert von $\log_\alpha \beta$ ableiten?

Aufgabe 47 ***mündlich***

Seien die Primzahl $p = 227$ und der Erzeuger $\alpha = 2$ von $\mathbb{Z}_p^*$ gegeben.

(a) Berechnen Sie die Potenzen α^{32}, α^{40}, α^{59} und α^{156} in $\mathbb{Z}_p^*$ und faktorisieren Sie diese über der Faktorbasis $B = \{2, 3, 5, 7, 11\}$.

(b) Bestimmen Sie die diskreten Logarithmen $\log_\alpha p$ der Basisprimzahlen $q \in B$.

(c) Berechnen Sie $\log_\alpha \beta$ für $\beta = 173$ mit der Index-Calculus Methode.

Hinweis: Benutzen Sie die Faktorbasis B und die Zufallszahl 177.

Aufgabe 48 ***mündlich***

(a) Falls sich bei der Berechnung einer ElGamal-Signatur der Wert $\delta = 0$ ergibt, muss eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie sich aus einer ElGamal-Signatur (γ, δ) mit $\delta = 0$ und dem öffentlichen Verifikationsschlüssel der geheime Signaturschlüssel berechnen lässt.

(b) Beim DSA muss auch im Fall $\gamma = 0$ eine neue Zufallszahl z gewählt werden. Überlegen Sie, wie aus einer DSA-»Signatur« (γ, δ) mit $\gamma = 0$ die benutzte Zufallszahl z bestimmt werden kann, und wie sich daraus für ein beliebiges Dokument x eine gefälschte »Signatur« (γ, δ) mit $\gamma = 0$ erhalten lässt.

Aufgabe 49 ***10 Punkte***

Betrachten Sie die mittels

$$y^2 = x^3 - 3x - 2$$

über den reellen Zahlen definierte elliptische Kurve E.

(a) Skizieren Sie zeichnerisch den Verlauf von E.

(b) Berechnen Sie die Summe $P + Q$ für $P = (3, 4)$ und $Q = (2, 0)$.

(c) Berechnen Sie die Punkte $2P = P + P$ und $2Q = Q + Q$.