Kryptologie 2 Sommersemester 2010
Johannes Köbler, Sebastian Kuhnert 12. Mai 2010

Übungsblatt 5

Aufgabe 36 ***mündlich***

Welche Angriffe sind möglich, wenn ein Schlüssel k sowohl für CBC-Verschlüsselung als auch für einen CBC-MAC einer Nachricht m verwendet wird?

Aufgabe 37 ***mündlich***

Sei $E_k\colon \{0,1\}^n \to \{0,1\}^n$, $k \in \{0,1\}^l$, eine Familie von Verschlüsselungsfunktionen. Ein darauf basierender CMAC arbeitet ähnlich wie der CBC-MAC, verwendt jedoch eine andere Preprocessing-Funktion: Zunächst werden Varianten des Schlüssels $k \in \{0,1\}^l$ berechnet: $k_1 = E_k(0^n) \cdot u$ und $k_2 = E_k(0^n) \cdot u^2$, wobei die Multiplikation in $\mathbb{F}_{2^n} = \mathbb{F}_2[u]/m(u)$ für das lexikographisch kleinste irreduzible Polynom $m(u)$ mit der minimalen Anzahl von positiven Koeffizienten stattfindet. Hat der letzte Klartextblock volle Länge $j = n$, so wird bitweise k_1 addiert; bei $j < n$ wird er mit 10^{n-j-1} gepadded und bitweise k_2 addiert. Das Ergebnis wird dann wie im CBC-MAC weiterverarbeitet.

Zeigen Sie, dass tatsächlich zwei zusätzliche Schlüsselvarianten notwendig sind, indem Sie für $k_2 = k_1$ einen Substitutionsangriff durchführen.

Aufgabe 38 ***mündlich***

Faktorisieren Sie die Zahlen 262063, 9420457 und 181937053 mit dem ρ-Algorithmus von Pollard. Wieviele Iterationen werden hierzu jeweils bei Verwendung der Funktion $f(x) = x^2 + 1$ benötigt?

Aufgabe 39 ***mündlich***

Beschreiben Sie eine Modifikation des Algorithmus von Shanks, die den diskreten Logarithmus von β zur Basis α in Zeit $\mathcal{O}(\sqrt{r-l})$ berechnet, falls bereits bekannt ist, dass dieser im Teilintervall $[r,l]$ von $[0, \mathrm{ord}(\alpha) - 1]$ liegt.

Aufgabe 40 ***mündlich***

Berechnen Sie in der Gruppe $\mathbb{Z}_p^*$ mit $p = 458009$ den diskreten Logarithmus von $\beta = 56851$ zur Basis $\alpha = 2$ mit der Ordnung $\mathrm{ord}(\alpha) = 57251$.

Aufgabe 41 ***mündlich***

Sei p eine ungerade Primzahl.

(a) Zeigen Sie, dass α oder $\alpha + p$ ein Erzeuger von $\mathbb{Z}_{p^2}^*$ ist, falls α ein Erzeuger von $\mathbb{Z}_p^*$ ist.

(b) Überlegen Sie, wie sich effizient verifizieren lässt, dass 3 sowohl ein Erzeuger von $\mathbb{Z}_{29}^*$ als auch von $\mathbb{Z}_{29^2}^*$ ist.

(c) Bestimmen Sie die Ordnung von 3 in $\mathbb{Z}_m^*$ mit $m = 29^3$.
Hinweis: Es ist bekannt, dass α für alle $k \geq 1$ ein Erzeuger von $\mathbb{Z}_{p^k}^*$ ist, falls α ein Erzeuger von $\mathbb{Z}_p^*$ und von $\mathbb{Z}_{p^2}^*$ ist.

(d) Bestimmen Sie einen Erzeuger von $\mathbb{Z}_{29}^*$, der nicht gleichzeitig Erzeuger von $\mathbb{Z}_{29^2}^*$ ist.

(e) Berechnen Sie mit dem Algorithmus von Pohlig und Hellman den diskreten Logarithmus von $\beta = 3344$ zur Basis $\alpha = 3$ in der Gruppe $\mathbb{Z}_m^*$ mit $m = 29^3$.

Aufgabe 42 ***mündlich***

Für zwei Dokumente x_1 und x_2 seien die ElGamal-Signaturen (γ, δ_1) bzw. (γ, δ_2) bekannt, d.h. es wurde beidesmal dasselbe r verwendet.

(a) Beschreiben Sie, wie sich hieraus r im Fall $\mathrm{ggT}(\delta_1 - \delta_2, p-1) = 1$ effizient berechnen lässt, und wie sogar der geheime Exponent a bestimmt werden kann.

(b) Seien $p = 31847$, $g = 5$ und $b = 25703$. Berechnen Sie r und a anhand der Dokumente $x_1 = 8990$, $x_2 = 31415$ sowie der Unterschriften $(23972, 31396)$ und $(23972, 20481)$.

Aufgabe 43 ***10 Punkte***

In der Vorlesung wurde ein Angriff gegen das ElGamal-Signaturverfahren vorgestellt, mit dem sich eine gültige Signatur (γ, δ) für ein zufälliges Dokument x berechnen lässt (nichtselektive Fälschung bei bekanntem Verifikationsschlüssel). Hierbei berechnet der Gegner für beliebige Parameter i, j mit $0 \leq i, j \leq p-2$ und $\mathrm{ggT}(j, p-1) = 1$ die Fälschung (x, γ, δ) mittels

$$\gamma := g^i b^j \bmod p, \qquad \delta := -\gamma j^{-1} \bmod p-1 \text{ und} \qquad x := -\gamma i j^{-1} \bmod p-1.$$

(a) Berechnen Sie eine Fälschung (x, γ, δ) für den Verifikationsschlüssel $k = (b, g, p)$ mit $p = 467$, $g = 2$ und $b = 132$. (Wählen Sie $i = 99$ und $j = 179$.)

(b) Ähnlich wie oben lässt sich auch eine nichtselektive Fälschung (x', γ', δ') bei bekannter Signatur (x, γ, δ) vornehmen, indem für beliebige Parameter h, i, j mit $0 \leq h, i, j \leq p-2$ und $\mathrm{ggT}(h\gamma - j\delta, p-1) = 1$

$$\begin{aligned} \gamma' &:= \gamma^h g^i b^j \bmod p, \\ \delta' &:= \delta\gamma'(h\gamma - j\delta)^{-1} \bmod p-1 \text{ und} \\ x' &:= \gamma'(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod p-1 \end{aligned}$$

gewählt wird. Zeigen Sie, dass die Signatur (x', γ', δ') als echt anerkannt wird.

(c) Das Dokument $x = 100$ hat unter ElGamal (mit $p = 467$, $g = 2$ und $b = 132$) die Signatur $(\gamma, \delta) = (29, 51)$ erhalten. Berechnen Sie hieraus ein signiertes Dokument, das Oskar bei Verwendung der Werte $h = 102$, $i = 45$ und $j = 293$ erzeugen kann. Überprüfen Sie die Verifikationsbedingung.