Dr. Dirk Frettlöh 26.6.2019

Übungen zur Vorlesung Kryptographie

Blatt 12

Aufgabe 45: (Kollision II)
Wir betrachten hier die Kompressionsfunktion $f(x, y) = 5^x \cdot 19^y \bmod 2017$. Die Zahl 2017 ist eine Primzahl.

(a) Zeigen Sie, dass 5 und 19 Primitivwurzeln in Z^*_{2017} sind.

(b) Finden Sie durch brute-force eine Kollision (m, m') für f (mit $m, m' \notin \{0, 1\}$). Wieviele Wertepaare müssen Sie ausprobieren? Wieviele wären zu erwarten gewesen?

(c) Finden Sie durch einen Geburtstagsangriff eine von Kollision von f. D.h.: Ersetzen Sie im Geburtstagsangriff-Algorithmus im Skript die Punkte 3 und 4 durch:

3. Falls r $= 0$ füge 5^i zu X hinzu, sonst füge 19^i zu Y hinzu.

4. Falls ein Element $x = 5^i$ aus der Liste X auch als $x = 19^j$ in der Liste Y auftaucht, gib aus i, j.

Wie finden Sie daraus eine Kollision für f? Wieviele Wertepaare müssen Sie hier ausprobieren? Nehmen Sie den Mittelwert von 10 Versuchen. Wieviele Versuche wären zu erwarten gewesen?

Aufgabe 46: (Korrektheit der ElGamal-Signatur)
Zeigen Sie, dass das ElGamal-Signaturverfahren korrekt ist. Genauer: zeigen Sie, dass mit $r \in \{2, 3, \ldots, p-2\}$ und $\mathrm{ggt}(r, p-1) = 1$ sowie $s \equiv (m - bg^r)r^{-1} \bmod p-1$ (wobei b Bobs geheimer Schlüssel ist) tatsächlich $g^m \equiv (g^b)^{g^r} \cdot (g^r)^s \bmod p$ gilt.
Zeigen Sie auch umgekehrt: Falls $s \not\equiv (m-bg^r)r^{-1} \bmod p-1$, dann ist $g^m \not\equiv (g^b)^{g^r} \cdot (g^r)^s \bmod p$.
(Wenn man's richtig macht geht beides in einem.)

Aufgabe 47: (Angriff auf ElGamal-Signatur)
Führen Sie den in der Vorlesung beschriebenen Angriff von Alice auf Bobs ElGamal-Signatur durch, falls Bob zweimal dieselbe Zufallszahl r bzw somit zweimal denselben Teilschlüssel g^r verwendet, in der folgenden konkreten Situation:

Bob benutzt die öffentliche Primzahl $p = 337741$ und den öffentlichen Schlüssel $g^b \bmod p$ mit $g = 173$. Der geheime Schlüssel von Bob ist b. Bob wählt eine geheime zufällige Zahl r und berechnet den Teilschlüssel $g^r \equiv 163949 \bmod p$. Bob verschlüsselt damit m_1 als c_1 und m_2 als c_2, berechnet die Signaturen $s_1 \equiv (m_1 - bg^r)r^{-1} \equiv 28774 \bmod p-1$ und $s_2 \equiv (m_2 - bg^r)r^{-1} \equiv 191293 \bmod p-1$ und sendet (c_1, g^r, s_1) und (c_2, g^r, s_2) an Alice. Alice entschlüsselt c_1 als $m_1 = 120324$ und c_2 als $m_2 = 201027$. Alice fällt auf, dass zweimal derselbe Teilschlüssel g^r verwendet wurde. Wie berechnet Alice die geheimen Informationen r und b?

Aufgabe 48: (Gehaltsvergleich)
In vielen Unternehmen weiß fast niemand in den gehobenen Positionen, was die Kollegen verdienen, und niemand möchte sein Gehalt verraten. Alice, Bob und Carol möchten wissen, ob sie "genug" verdienen in dem Sinne, ob sie jeweils mehr oder weniger als das Durchschnittsgehalt der drei verdienen. Dazu nutzen sie folgendes Verfahren:

1. Alice wählt eine geheime Zufallszahl r, addiert ihr Gehalt a und gibt $a + r$ an Bob weiter.
2. Bob addiert sein Gehalt b und gibt $a + b + r$ an Carol weiter.
3. Carol addiert ihr Gehalt c und gibt $a + b + c + r$ an Alice weiter.
4. Alice subtrahiert r und gibt $\frac{1}{3}(a + b + c)$ bekannt.

(a) Begründen Sie, warum das Verfahren sicher ist, d.h.: Warum kann Alice nicht b oder c ermitteln, warum Bob nicht a oder c, und warum Carol nicht a oder b?

(b) Analog zum oben geschilderten anonymen Berechnen des Durchschnittsgehalts von drei Leuten, finden Sie eine Methode zum anonymen Berechnen des Durchschnittsgehalts von n Leuten ($n \geq 3$).

(c) Wie viele Leute müssen sich oben bzw bei Ihrer Methode mindestens verabreden, um alle Gehälter ermitteln zu können? (Sie teilen untereinander alle Informationen, die sie haben; sie verraten damit natürlich auch Ihre eigenen Gehälter, zumindest untereinander.) Angenommen, alle Beteiligten sitzen an einem runden Tisch, wie genau muss diese Minimalzahl von verabredeten Leuten sitzen, um alle Gehälter zu erfahren?

Dienstag	Philipp Braukmann	pbraukmann@techfak.uni-bielefeld.de
Donnerstag	Oliver Tautz	otautz@techfak.uni-bielefeld.de