Dozent: Prof. Dr. Johannes Blömer
Tutoren: Pascal Bemmann, Fabian Eidens, Jakob Juhnke und Peter Günther
Ausgabedatum: 29.01.2016
Abgabe: Mo. 08.02.2016 bis 14:00 (D3 Kasten)/14:45 Uhr (Fürstenallee)

Einführung in Kryptographie

WS 2015/2016

Heimübungszettel 7

AUFGABE 1 (8 Punkte)**:**
Gegeben sei eine Blockchiffre $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ mit $\mathcal{P} = \mathcal{C} = \mathcal{K} = \{0,1\}^n$. Diese Blockchiffre soll nun zur Konstruktion eines MACs für eine Nachricht benutzt werden.

a) Der MAC $h_k(x)$ einer Nachricht $x \in \{0,1\}^{bn}$ mit $x = x_1 x_2 \dots x_b, x_i \in \{0,1\}^n, 1 \leq i \leq b$ entspreche der Verschlüsselung von x im ECB Modus unter Verwendung der obigen Blockchiffre. Wir erhalten also die Abbildung $h_k : \{0,1\}^{bn} \to \{0,1\}^{bn}, b \in \mathbb{N}, b \geq 2$ fest. Zeigen Sie am Beispiel dieser Konstruktion, dass Verschlüsselungsverfahren im Allgemeinen keine Authentizität gewährleisten.

b) Nun ersetzen wir den ECB Modus durch den OFB Modus, so dass wir $h_k : \{0,1\}^{bn} \to \{0,1\}^{(b+1)n}, b \in \mathbb{N}$ erhalten. Wie kann ein Angreifer auch hier den MAC $h_k(x)$ der Nachricht x nutzen, um einen MAC $h_k(x')$ für $x' \neq x$ zu generieren?

c) Nun betrachten wir die CBC-MAC Konstruktion aus der Vorlesung. Um beliebig lange Nachrichten verarbeiten zu können, wird der Parameter b hier jedoch nicht fest gewählt. Wir erhalten also $h_k : \bigcup_{b \in \mathbb{N}} \{0,1\}^{bn} \to \{0,1\}^n$ mit

$h_k(x), x = x_1 x_2 \cdots x_b, x_j \in \{0,1\}^n, b \in \mathbb{N}$
1 $z_0 := 0^n$
2 $z_i := E_k(z_{i-1} \oplus x_i), i = 1, \dots, b, E_k \in \mathcal{E}$
3 $h_k(x) := z_b$

Zeigen Sie, dass diese Konstruktion nicht sicher gegen Fälschungen ist.

Tipp: Wählen Sie zwei Nachrichten $x, y \in \{0,1\}^n$ zu denen ein Angreifer die MACs $h_k(x), h_k(y)$ besitzt. Wie kann der Angreifer daraus einen MAC für eine Nachricht $z \in \{0,1\}^{2n}$ fälschen.

AUFGABE 2 (4 Punkte)**:**
Betrachten Sie das RSA-Signaturverfahren. Zeigen Sie, wie ein Angreifer zu einer beliebigen gegebenen Nachricht $m \neq 0 \mod N$ im Chosen-Message-Modell eine Signatur fälschen kann.

AUFGABE 3 (6 Punkte)**:**
DSA ist Teil des Digital Signature Standards des NIST. Das NIST schlägt einige Verbesserungen vor, die nun auch in den deutschen Standarts umgesetzt werden sollen. Aus aktuellem Anlass hat die deutsche Regierung die Befürchtung, dass die NSA hinter den Verbesserungsvorschlägen steckt und bittet Sie als Experten die Vorschläge zu prüfen.[1] Wie beurteilen Sie die folgenden Verbesserungen:

[1] Diese Geschichte ist frei erfunden.

a) Da es schwierig ist zufällige Zahlen zu erzeugen, soll das k aus Schritt 1 der DSA Unteschriften beim Signieren nicht zufällig gewählt werden. Stattdessen wird k initial zufällig gleichverteilt gewählt. Dann wird k von Signatur zu Signatur um 2 inkrementiert.

Zeigen Sie, dass nun aus zwei Signaturen (r_1, s_1), bzw. (r_2, s_2) mit $r_1 = (g^k \mod p) \mod q$ und $r_2 = (g^{k+2} \mod p) \mod q$ für ein unbekanntes $k \in \mathbb{Z}_q^*$ der geheime Signaturschlüssel berechnet werden kann.

Hinweis: Sie dürfen dabei annehmen, dass $r_1 s_2 - r_2 s_1$ modulo q invertierbar ist.

b) Um kürzere Signaturen als $2 \cdot 160$ bit zu erhalten soll q bei der DSA Schlüsselerzeugung auf $2^{99} < q < 2^{100}$, also 100 bit reduziert werden. An der Größe von p soll sich nichts ändern. Angenommen die NSA verfügt über einen Supercomputer, der 2^{60} Exponentiationen in $\mathbb{Z}_p^*$ am Tag berechnen kann. Zeigen Sie, dass die NSA aus einem öffentlichen Schlüssel (p, q, g, A) mit $A = g^a$ den geheimen Schlüssel (p, q, g, a) an einem Tag berechnen kann.

Hinweis: Benutzen Sie Ihr Wissen vom letzten Heimübungszettel.