Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Security

SoSe 24
LV 4120, 7240

Übungsblatt 7

Aufgabe 7.1 (Reduktionsbeweise und Eigenschaften von Hashfunktionen):

In der IT-Sicherheit werden häufig Reduktionsbeweise verwendet, bei denen ein Problem auf ein anderes Problem reduziert wird. Die Idee dabei ist, dass eine Hierarchie zwischen Problemen aufgebaut werden kann, um:

a) die Konsequenzen für den Verlust von Sicherheitseigenschaften aufzuzeigen oder

b) die Sicherheit einer Funktion auf die Schwierigkeit der Lösung eines Problems zu reduzieren (z.B. RSA und Primfaktorzerlegung).

Bilden Sie eine Hierarchie zwischen den drei Eigenschaften einer Hashfunktion (Einwegeigenschaft, schwache Kollisionsresistenz, starke Kollisionsresistenz) durch Benutzung des Reduktionsbeweises. Die Hierarchie sollte aufzeigen, wie die Nicht-Erfüllung einer Eigenschaft zum Brechen einer anderen Eigenschaft ausgenutzt werden kann.

Aufgabe 7.2 (Design von Hashfunktionen):

Gegeben seien die folgenden Funktionen f wobei alle Werte der Funktionen bekannt sind, außer anderweitig angegeben

a) $f(m) = a \cdot m + b \mod p$ für zufällige Zahlen a und b sowie einer Primzahl p, die alle eine Bitlänge von 2048 haben.

b) $f(m) = g^m \mod p$ für eine bekannte Basis g und bekannte Primzahl p, die beide eine Bitlänge von 2048 haben. Hinweis: Nutzen Sie die Eigenschaft, dass für Primzahlen p gilt:
$f(m) = g^m \mod p \equiv g^{m \mod \phi(p)} \mod p \equiv g^{m \mod (p-1)} \mod p$.

c) $f(m) = (g^m \mod N) \mod 2^{128}$ für eine bekannte Basis g, einen bekannten 4096-bit Modulus $N = p \cdot q$ und unbekannte Primzahlen p, q.

d) $f(m) = ENC_K(m)$ mit der Verschlüsselungsfunktion $ENC_K(\cdot)$, einer Blockchiffre mit einem geheimen Schlüssel K. Zur $f(m)$ existiert eine inverse Funktion $DEC_K(\cdot)$, die Bitlänge des Schlüssels beträgt 256-Bit und ist damit doppelt so groß wie die Blockgröße der Chiffre.

Welche der Eigenschaften für kryptographische Hashfunktionen (Einwegeigenschaft, schwache- oder starke Kollisionsresistenz) sind jeweils für die Funktionen erfüllt? (*Tipp:*) Nutzen Sie den Reduktionsbeweis, um die Funktionen auf als schwer bekannte Probleme zurückzuführen.

Aufgabe 7.3 (Zufallszahlen):

a) Welche Eigenschaften muss eine Zufallszahl für kryptographische Applikationen haben? Erläutern Sie jede der Eigenschaften kurz.

b) Nach der AIS31 sind deterministische Zufallszahlengeneratoren in folgende Klassen aufgeteilt.

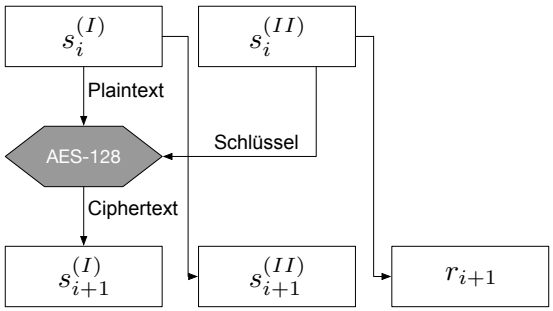
Klasse	Abkürzung	Beschreibung
1	DRG.1	Pseudozufallszahlengenerator mit perfekter vorwärts gerichteter Geheimhaltung (forward secrecy) nach [ISO18031]
2	DRG.2	DRG.1 mit zusätzlicher perfekter rückwärts gerichteter Geheimhaltung (backward secrecy) nach [ISO18031]
3	DRG.3	DRG.2 mit verbesserter backward secrecy
4	DRG.4	DRG.3 mit verbesserter forward secrecy (Hybrider Pseudozufallsgenerator)

In diesem Konzept werden deterministische Zufallszahlengeneratoren als Moore oder Mealy-Automaten interpretiert. Mit einer allgemeinen Übergangsfunktion $\Phi : S \rightarrow S$, so dass der nächste Zustand s_{n+1} von einem vorherigen Zustand s_n abhängt $S_{n+1} := \Phi(s_n) \forall n \geq 1$. Das Ausgaben Alphabet R hängt dann zumindest von Zustandsalphabet S ab und wird mit der Ausgabefunktion Ψ: $S \rightarrow R$ generiert, so dass gilt: $r_n : \Psi(s_n) \forall n \geq 1$.

Gegeben sei folgende Konstruktion eines Pseudozufallszahlengenerators:

- Der Pseudozufallszahlengenerator hat einen internen Zustand der aus einem Tuple $s_i = (s_i^{(I)}, s_i^{(II)})$ für jeden Iterationsschritt (diskreter Zeitpunkt) i besteht.
- $s_{i+1} = \Phi(s_i) = (AES_{s_i^{(II)}}(s_i^{(I)}), s_i^{(I)})$, mit $C = AES_K(P)$ ein AES-128 mit dem Schüssel K und dem Ciphertext C und Plaintext P darstellt.
- $r_{i+1} = \Psi(s_i) = s_i^{II}$

Die nachfolgende Grafik verdeutlichet den Aufbau des Zufallzahlengenerators, der einenAES-128 Blockchiffre als zentrales Element benutzt



b1) Zu welcher Klasse der deterministische Zufallszahlengeneratoren gehört diese Konstruktion? Begründen Sie Ihre Aussage.

b2) Warum erfüllt diese Konstruktion das Kriterium der backward secrecy?

b3) Kann die Konstruktion durch eine Anpassung von $\Psi(\cdot)$ noch zu einem DRG.2 angepasst werden? Welche Eigenschaft muss $\Psi(\cdot)$ haben?

Aufgabe 7.4 (Zufallszahlen und Integrität für die sichere Schlüsselverwaltung):

a) Herrn Seky ist seit letzter Woche aufgefallen, dass er für seinen Vorschlag, ein DHKE für den Schlüsselaustausch zu nutzen, auch eine Zufallszahl benötigt. Da bei dem DHKE die Zufallszahl niemals nach Aussen kommuniziert wird, wird es seiner Ansicht nach schwer sein, diese zu erraten. Aus diesem Grund beschließt er, einen Pseudozufallszahlengenerator auf Basis eines LFSR aufzubauen ($s_{i+m} \equiv \sum_{j=0}^{m-1} p_j \cdot s_{i+j} \mod 2; s_i, p_i \in 0, 1; i = 0, 1, 2, \dots$). Was muss Herr Seky bei der Wahl des Polynoms beachten?

b) Herrr Seky wählt das Polynom $P(x) = x^8 + x^4 + x^3 + x + 1$ aus. Zeichnen Sie das Blockschaltbild des LFSR.

c) Der LFSR soll im B2D-Server genutzt werden zur zufälligen Auswahl der K_{pr} für das DHKE-Protokoll und als Salt, um die Passwörter für die Benutzerkonton als Hashwert sicher auf dem Server zu speichern. Sehen Sie bei dieser Vorgehensweise von Herrn Seky ein Problem, wenn ja welches?