Vorlesung am 28.04.2014

Das unmodifizierte RSA-Verfahren hat mehrere Schwächen
Einsatz probabilistischer Verfahren notwendig (siehe Ende der Vorlesung)

Beispiel (Erste Schwäche). Das RSA-Verfahren ist deterministisch.

- Angreifer kann Klartext raten
- mit öffentlichem Schlüssel verschlüsseln und vergleichen

Angriff funktioniert für symmetrische Verfahren nicht

Definition 4.3 (Indistinguishability under chosen plaintext attack, IND-CPA)**.**
Gegeben asymmetrisches Verschlüsselungsverfahren und Schlüsselpaar

- Angreifer wählt zwei Klartexte m_1, m_2
- Einer der Klartexte wird ausgewählt und verschlüsselt
- Angreifer muss raten, welcher Text verschlüsselt wurde

Verfahren ist IND-CPA sicher, wenn Erfolg für Angreifer nahe bei 1/2.

Einige Bemerkungen:

- RSA ist nicht IND-CPA sicher (siehe erstes Beispiel)
- Hier nur informelle Definition (siehe Vorlesung Kryptologie)
  - Angreifer: randomisierter polynomieller Algorithmus
  - Nahe 1/2: Wkeit in $[1/2 - \epsilon, 1/2 + \epsilon]$ für sehr kleines ϵ
    ($\epsilon < 1/p(n)$ für jedes Polynom p und n Sicherheitsniveau)

Beispiel (Zweite Schwäche).

RSA-Entschlüsselung $\mathbb{Z}_n \longrightarrow \mathbb{Z}_n; m \mapsto m^d$ ist multiplikativ. Angriff:

Nachricht m wurde zu $c = m^e \bmod n$ verschlüsselt
Angreifer möchte m ermittlen

- Wähle Wert $r \in \mathbb{Z}_n$ und berechne $r^e \bmod n$ (e ist öffentlich)
- Bilde $c' = c \cdot r^e = m^e \cdot r^e$, überrede Inhaber c' zu entschlüsseln (z.B. für Probeverschlüsselung)
- Angreifer erhält also $c'^d = (c \cdot r^e)^d = (m^e \cdot r^e)^d = m \cdot r \bmod n$
- Multiplikation mit r^{-1} liefert m

Beispiel (Dritte Schwäche).

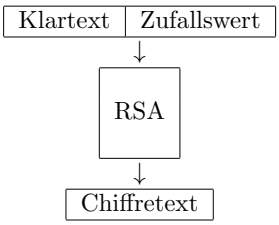
Kleine Verschlüsselungsexponenten: Sei $e = 3$.

- Angreifer kennt Ciphertexte $c_1 = m^3 \bmod n$ und $c_2 = (m+1)^3 \bmod n$.
- Berechnung von m ohne Nutzung von d:

$$\begin{aligned} \frac{c_2 + 2c_1 - 1}{c_2 - c_1 + 2} &= \frac{(m+1)^3 + 2m^3 - 1}{(m+1)^3 - m^3 + 2} = \frac{(m^3 + 3m + 3m^2 + 1) + 2m^3 - 1}{(m^3 + 3m + 3m^2 + 1) - m^3 + 2} \\ &= \frac{3m^3 + 3m + 3m^2}{3m + 3m^2 + 3} = m \end{aligned}$$

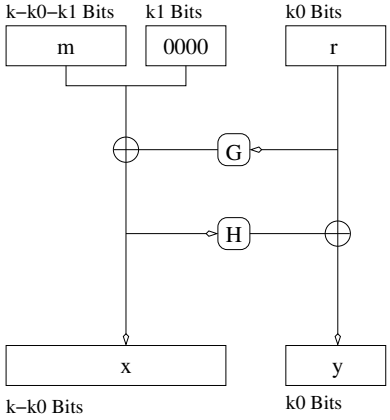
Verallgemeinerung Für $m_2 = \alpha \cdot m_1 + \beta$ und beliebige Exponenten e:
Laufzeit $\mathcal{O}(e^2)$: also nur für kleine e praktikabel.

Lösung: Setze probabilistische Verfahren ein.



- Klartextraum wird vergrößert.
- Annäherung an Gleichverteilung (erschwert statistische Angriffe).
- Obiger Angriff nicht mehr möglich.

Beispiel (OAEP, Optimal asymmetric encryption padding).



- Auffüllen von m mit k_1 Nullen
- r: Zufallswert der Länge $k_0 \geq 100$ Bit
- Funktion G erweitert r auf $k - k_1$ Bits.
- $x := (m||0 \cdot 0) \oplus G(r))$
- Funktion H reduziert x auf k_0 Bits.
- $y := H(x) \oplus r$.
- $m_r := x||y$ wird zu c verschlüsselt.

Empfänger entschlüsselt c zu $x||y$ und erhält m aus $x||y$ wie folgt:

- Berechne $r = y \oplus H(x)$ und
- $m||0 \cdots 0 = x \oplus G(r)$.

Übung: Zeigen Sie, dass das RSA-Verfahren mit OAEP IND-CPA sicher ist, wenn H und G Einwegfunktionen sind.

Elgamal Entwickelt von Taher Elgamal 1984.

Sicherheit: Vermutete Schwierigkeit des Diskreten Logarithmusproblems.

Problem DL:
Eingabe: Zwei Zahlen $g, h \in G$.
Ausgabe: $\log_g h$, d.h. $x \in \mathbb{N}$ mit $g^x = h$.

G heißt kr. stark, wenn das DL-Problem in G praktisch nicht lösbar ist.
Bsp.: $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$, p sehr große Primzahl.

Eigenschaften:

- Diese Gruppen sind zyklisch, d.h.
  Es gibt $g \in \mathbb{Z}_p^*$ mit $\{g^n; n \in \mathbb{N}\} = \{1, 2, \ldots, p-1\}$
  g ist dann Erzeuger der Gruppe. Insb. $\mathbb{Z}_p^* = \{g^n; 1 \leq n \leq p-1\}$.

- Ist $g \in \mathbb{Z}_p^*$ Erzeuger, dann ex. f.a. $h \in \mathbb{Z}_p^*$ ein $x \in \mathbb{N}$ mit $g^x = h$.
  D.h. $\log_g h = x$ existiert.

Schlüsselgenerierung:

- Wähle eine endl. zykl. Gruppe G und Erzeuger $g \in G$.
- Wähle $j \leq |G| - 1$ und setze $h = g^j$.
- Geheimer Schlüssel: j, öffentlicher Schlüssel: (h, g, G).

Verschlüsselung einer Nachricht $m \in G$:

- Wähle $k \leq |G| - 1$, setze $f = g^k$.
- Verschlüsselung: $(f, c = h^k \cdot m)$.

Entschlüsselung:

- Berechne $f^{-j} \cdot c = g^{-kj} h^k m = g^{-kj} g^{kj} m = m$.

Übung: Zeigen Sie, dass Elgamal ist IND-CPA sicher ist.

Hybride Verschlüsselung

- Alice will Bob eine vertrauliche Nachricht $m \in \{0,1\}^*$ schicken
- Bob hat RSA-Schlüsselpaar $(pk = (e, n), sk = d)$, Alice kennt pk
- Alice wählt symm. Schlüssel $k \in \{0,1\}^{128}$, berechnet $c_1 = k^e \bmod n$, $c_2 = \text{AES}(m, k)$ und sendet c_1, c_2 an Bob
- Bob berechnet $c_1^d \bmod n = k$ und kann c_2 entschlüsseln