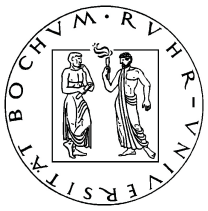
Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Mathias Herrmann



Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2009

Blatt 5 / 24. Juni 2009

AUFGABE 1:
Wir betrachten im Folgenden Varianten der Definition für Sicherheit von Signaturen. Geben Sie für jeder der beiden Varianten an, ob eine Textbook-RSA Signatur sicher ist oder nicht und begründen Sie Ihre Antwort.

1. In der ersten Variante verläuft das Spiel folgendermaßen:

   - Der Angreifer erhält den öffentlichen Schlüssel und eine zufällige Nachricht m.
   - Er darf dann einmalig ein Signaturorakel nach einer Nachricht ungleich m befragen.
   - Danach gibt er eine Signatur σ aus und gewinnt, falls $\mathsf{Vrfy}_{pk}(m, \sigma) = 1$.

   Wie üblich sagen wir, dass das System sicher ist, wenn der Angreifer mich höchstens vernachlässigbarer Wahrscheinlichkleit das Spiel gewinnt.

2. Die zweite Variante ist analog zur ersten, allerdings darf der Angreifer das Orakel **nicht** befragen.

AUFGABE 2:
Ein Versuch sichere RSA Signaturen zu erzeugen ist das **encoded RSA**. Dabei sind privater und öffentlicher Schlüssel wie in Textbook-RSA und eine öffentliche *encoding Funktion* enc wird fixiert. Die Signatur einer Nachricht m wird berechnet als $\sigma := [\mathsf{enc}(m)^d \bmod N]$.

1. Wie wird bei encoded-RSA die Verifikation durchgeführt?
2. Warum verhindet eine gute Wahl der encoding-Funktion einen *no-message-Angriff*?
3. Zeigen Sie, dass mit $e = 3$ encoded-RSA für $\mathsf{enc}(m) = 0||m||0||m$ unsicher ist.
   ($|m| = (||N|| - 1)/2$ und m nicht der Nullstring.)

Hinweis zur Notation: Analog zum Buch von Katz/Lindell verwenden wir:

- $||x||$ für die Länge der Binärrepräsentation der Zahl x, geschrieben mit einer führenden 1.
- $|x|$ für die Länge des binären Strings x mit möglicherweise führenden Nullen.
- $x||y$ für die Konkatenation der Strings x und y.