Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Dr. Christopher Wolf
Alexander Meurer

RUHR UNIVERSITÄT BOCHUM RUB

Präsenzübungen zur Vorlesung

Kryptographie 2

SS 2010

Blatt 2 / 28. April 2010

AUFGABE 1. Formalitäten.
Wir beweisen hier formal ein fehlendes Detail aus dem Beweis zur hybriden Verschlüsselung (siehe Folie 35). Sei $\mathcal{A}^{hy}$ ein Angreifer auf das Hybridverfahren Π^{hy} bestehend aus einem CPA-sicheren asymmetrischen Verfahren Π (gegenüber passiven Angreifern) und einem symmetrischen Verfahren mit ununterscheidbaren Verschlüsselungen (gegenüber passiven Angreifern).
Betrachten Sie den folgenden Angreifer $\mathcal{A}_1$ der Nachrichten des Public Key Verfahrens Π belauscht:

1. $\mathcal{A}_1$ erhält als Eingabe den öffentlichen Schlüssel pk. Er wählt zufällig $k \leftarrow \{0,1\}^n$ und gibt das Paar von Nachrichten $(k, 0^n)$ zurück. Anschließende erhält er einen Challenge-Ciphertext c_1.
2. $\mathcal{A}_1$ ruft $\mathcal{A}^{hy}(pk)$ auf und bekommt m_0, m_1 zurückgeliefert.
3. $\mathcal{A}_1$ berechnet $c_2 \leftarrow \mathsf{Enc}'_k(m_0)$ und sendet die Challenge (c_1, c_2) an $\mathcal{A}^{hy}$. $\mathcal{A}_1$ gibt das Bit b' aus, welches von $\mathcal{A}^{hy}$ ausgegeben wird.

Zeigen Sie, falls Π ununterscheidbare Verschlüsselungen bzgl. eines passiven Angreifers hat, dann gilt:

$$\frac{1}{2}(\mathbf{Pr}\left[\mathcal{A}^{hy}(\mathsf{Enc}_{pk}(k), \mathsf{Enc}'_k(m_0)) = 0\right] + \mathbf{Pr}\left[\mathcal{A}^{hy}(\mathsf{Enc}_{pk}(0^n), \mathsf{Enc}'_k(m_0)) = 1\right]) \leq \frac{1}{2} + \mathsf{negl}.$$

AUFGABE 2. Algebraisches.
Sei $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N : \mathrm{ggT}(x, N) = 1\}$ die Einheitengruppe von $(\mathbb{Z}_N, \cdot)$ und sei $\phi(N) = |\mathbb{Z}_N^*|$ die Eulersche Phi-Funktion. Zeigen Sie:

a) $\phi(p) = p - 1$ für jede Primzahl p

b) $\phi(pq) = (p-1)(q-1)$ für zwei Primzahlen $p \neq q$

c) Zeigen Sie, dass die Textbook-RSA Verschlüsselung *korrekt* ist für jede Nachricht $m \in \mathbb{Z}_N^*$. Was passiert, wenn $m \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*$?

AUFGABE 3. Faktorisieren.
Sei $N = pq$ ein RSA-Modul und sei $(N, e, d) \leftarrow \mathsf{GenRSA}$. Wir wollen in abgeschwächter Form zeigen, dass das Berechnen von d äquivalent zum Faktorisieren von N ist. Beweisen Sie hierzu folgende Aussagen:

a) Wenn man N effizient faktorisieren kann, so kann man d effizient berechnen.
Bemerkung: Das zeigt die Rückrichtung der Äquivalenz

b) Sind $\phi(N)$ und N bekannt, so kann man p und q berechnen.

c) Ist $e = 3$ und $d \in \mathbb{N}$ mit $ed \equiv 1 \bmod \phi(N)$, so kann man effizient p und q berechnen.
Bemerkung: Das zeigt die Hinrichtung der Äquivalenz im Spezialfall $e = 3$, der allgemeine Beweis ist nicht-trivial[1]

AUFGABE 4. Common modulus.
Seien $pk_1 = (N, e_1)$ und $pk_2 = (N, e_2)$ zwei öffentliche Schlüssel von Textbook RSA mit $gcd(e_1, e_2) = 1$. Ein Angreifer erfährt die Verschlüsselungen der gleichen Nachricht m unter den beiden Public Keys, d.h. er kennt

$$c_1 = m^{e_1} \bmod N \qquad \text{und} \qquad c_2 = m^{e_2} \bmod N$$

a) Erklären Sie, wie der Angreifer die Nachricht m berechnen kann.

b) Führen Sie den Angriff für die Werte $N = 143, e_1 = 3, e_2 = 5, c_1 = 8, c_2 = 54$ durch.

[1] siehe auch A.May: „*Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring*“, CRYPTO 2004, Lecture Notes in Computer Science Volume 3152, pages 213-219