STOFFÜBERSICHT SMS3 IM WS 2005/06

1. Grundbegriffe der Kryptographie und Informationstheorie

(1) * Grundbegriffe der Codierungstheorie: Um welches Problem geht es in der Kanalcodierung? (Mitschrift)
(2) * Begriffe der Kryptographie: [Ecker, 2004, Seite x], [Ecker, 2004, Kapitel 1].
(3) * Ziele der Kryptographie: [Menezes et al., 1997, Seite 4, nach Definition 1.1]: Die Aufstellung über die *Cryptographic Goals*.
(4) Bewertungen der Sicherheit: [Menezes et al., 1997, 1.13.3] (Models for evaluating security).
(5) * Unterscheidung zwischen symmetrischen und assymmetrischen Verfahren. [Ecker, 2004, Seiten 4-5].

2. Zahlentheoretische Grundlagen

(6) * Zahlentheorie: Teilbarkeit und ggT: Mitschrift (vgl. [Menezes et al., 1997, 2.79-2.92]).
(7) * Der Euklidsche Algorithmus zum Berechnen von $\mathrm{ggT}(a, b)$ und der Zahlen u, v mit $\mathrm{ggT}(a, b) = ua + vb$: Mitschrift (vgl. [Menezes et al., 1997, 2.107, Extended Euclidean Algorithm]).
(8) * Lösen der Kongruenz $a \cdot x \equiv b(\mathrm{mod} n)$: Mitschrift (vgl. [Aichinger, 2005]).
(9) * Der Ring $\mathbb{Z}_n$: drei Grundrechungsarten $+, -, \cdot$. Mitschrift (vgl. [Aichinger, 2005]).
(10) * Invertieren in $\mathbb{Z}_n$. Mitschrift (vgl. [Aichinger, 2005]).
(11) * Satz von Fermat und Satz von Euler. Mitschrift.
(12) * Das RSA-Verfahren: Aufgaben für den Systementwerfer, den Verschlüsseler und den Entschlüsseler: Mitschrift, [Menezes et al., 1997, 8.2.1, Description of RSA]
(13) Das Finden großer Primzahlen mit dem Rabin-Miller Test. Mitschrift, [Ecker, 2004, Seiten 37-38, Satz 2.46 - Algorithmus 2.50].
(14) Der BBS-Zufallszahlengenerator. Mitschrift, [Menezes et al., 1997, 5.5.2].
(15) * Namen der Attacken auf RSA und eine Zeile Beschreibung: Faktorisieren, wiederholte Verschlüsselung, gleiche Moduln, kleiner Verschlüsselungsexponent (Mitschrift).
(16) Funktion der Attacken auf RSA: Faktorisieren: quadratisches Sieb (Mitschrift, [Ecker, 2004, S.27, 2.8.3]), wiederholte Verschlüsselung, gleiche Moduln, kleiner Verschlüsselungsexponent (Mitschrift).

Date: January 10, 2006.

3. Identifikation und Authentifizierung

(1) * Hash Funktionen ([Ecker, 2004, Definition 4.1 und 4.2]).
(2) * Digitale Signaturen ([Menezes et al., 1997, 1.6]).
(3) Lamport's OWF-based one-time passwords. [Menezes et al., 1997, 10.6, 10.7, 10.8].
(4) Challenge-Response identification ([Menezes et al., 1997, 10.17], SKID3-Protokoll).
(5) Zero-knowledge Protokolle: Fiat Shamir Protokoll. [Menezes et al., 1997, 10.24]. Umgehung durch einen Betrüger, der e voraussagen kann.

4. Digitale Unterschriften

(1) * Basic definitions [Menezes et al., 1997, von 11.2.1 den Teil, der auf Seite 426 steht]
(2) * RSA Unterschriftenschema [Menezes et al., 1997, 11.3.1] (mit Hash statt Redundanzfunktion).
(3) DSA Digital Signature Algorithm [Menezes et al., 1997, 11.5.1], Programm auf der Webseite der Lehrveranstaltung.

5. Schlüsseltauschverfahren

(1) Diffie-Hellman Schlüsselvereinbarung [Menezes et al., 1997, 12.47].
(2) "Woman in the middle"-Attacke auf Diffie Hellman [Ecker, 2004, Algorithmus 3.37].
(3) MTI/A0-Protokoll [Menezes et al., 1997, 12.53].

Prüfungsinformation

Die Prüfung besteht aus einem ersten Teil ohne Unterlagen (8:50 - 9:45) und einem zweiten Teil (10:00-11:15) mit Unterlagen und Computer. Die mit * versehenen Teile sollten Sie ohne Unterlagen wissen. Die nicht mit * versehenen Teile sollten Sie verstanden haben; diese Teile müssen Sie aber nicht auswendig beherrschen. Sie sollen die für die Verschlüsselung mit dem RSA-Verfahren notwendigen Rechenoperationen mit Mathematica durchführen können.

References

[Aichinger, 2005] Aichinger, E. (2005). Unterlagen zur elementaren Zahlentheorie. Vorlesungsunterlagen, FH Oberösterreich, Standort Hagenberg.

[Ecker, 2004] Ecker, J. (2004). Automatentheorie und Kryptologie. Vorlesungsskriptum, FHS Hagenberg.

[Menezes et al., 1997] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (1997). *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL. With a foreword by Ronald L. Rivest.