Datensicherheit, Zusammenfassung Vorlesung 11

Henry Haustein, Dennis Rössel

Was charakterisiert den Algorithmus AES?

Substitutions-Permutations-Netzwerk mit wahlweise 10, 12 oder 14 Runden

Wie erfolgt bei AES die Verschlüsselung?

Verschlüsselung von Klartextblöcken der Länge 128 Bit (vorgeschlagene Längen von 192 und 256 Bits nicht standardisiert), Schlüssellänge wahlweise 128, 192 oder 256 Bits, Rundenanzahl r hängt von Schlüssel- und Klartextlänge ab:

- Schlüssellänge 128 Bit: 10 Runden
- Schlüssellänge 192 Bit: 12 Runden
- Schlüssellänge 256 Bit: 14 Runden

Runde 0: $\oplus k_0$
Struktur der ersten $r-1$ Runden: SubBytes, ShiftRow, MixColumn, $\oplus k_i$
Struktur der r-ten Runde: SubBytes, ShiftRow, $\oplus k_r$

Wie werden die Teilschlüssel erzeugt?

Schlüsselexpansion mit Rot (zyklische Verschiebung), SubWord (Substitution mit S_8) und Rcon (Rundenkonstante)

Wie erfolgt die Entschlüsselung?

Runde r: $\oplus k_r$, ShiftRow^{-1}, SubBytes^{-1}
Runde $1, ..., r-1$: $\oplus k_i$, MixColumn^{-1}, ShiftRow^{-1}, SubBytes^{-1}
Runde 0: $\oplus k_0$

Was versteht man unter synchronen/selbstsynchronisierenden Chiffren?

Synchrone Stromchiffre: Verschlüsselung eines Zeichens ist abhängig von der Position bzw. von vorhergehenden Klartext- oder Schlüsselzeichen

Selbstsynchronisierende Stromchiffre: Verschlüsselung ist nur von begrenzter Anzahl vorhergehender Zeichen abhängig

Wie erfolgen Ver- und Entschlüsselung bei den Betriebsarten ECB und CBC?

ECB: Jeder Block wird einzeln verschlüsselt/entschlüsselt

CBC: $c_i = enc(k, m_i \oplus c_{i-1})$, $m_i = dec(k, c_i) \oplus c_{i-1}$