Kryptografie und -analyse, Zusammenfassung Vorlesung 7

Henry Haustein

Auf welchem Prinzip beruht der Algorithmus AES?

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

Wie funktioniert AES prinzipiell (Struktur, Iterationsrunden, Anzahl der Runden ...)?

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 funktioniert die Entschlüsselung beim AES?

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

Wie kann die Entschlüsselung in äquivalenter Reihenfolge wie die Verschlüsselung durchgeführt werden?

Es gilt:

- SubBytes(ShiftRow(s_i))=ShiftRow(SubBytes(s_i))
- SubBytes^{-1}(ShiftRow^{-1}(s_i)) = ShiftRow^{-1}(SubBytes^{-1}(s_i))
- MixColumn($s_i \oplus k_i$) = MixColumn(s_i) $\oplus$ MixColumn(k_i)
- MixColumn^{-1}($s_i \oplus k_i$) = MixColumn^{-1}(s_i) $\oplus$ MixColumn^{-1}(k_i)

Reihenfolge der Abarbeitung wie bei Verschlüsselung, $k'_i = \text{MixColumn}^{-1}(k_i)$

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

Was versteht man unter synchroner bzw. selbstsynchronisierender Chiffre?

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 funktionieren die Betriebsarten ECB und CBC, welche Eigenschaften haben sie?

ECB (Electronic Code Book)

- Selbstsynchronisierend (Abhängigkeit von 0 Blöcken)
- Länge der verarbeiteten Einheiten: entsprechend Blockgröße der Blockchiffre (AES: $l = 128$ Bit)
- Keine Abhängigkeiten zwischen den Blöcken

CBC (Cipher Block Chaining)

- Selbstsynchronisierend (Abhängigkeit von 1 Block)
- Länge der verarbeiteten Einheiten: entsprechend Blockgröße der Blockchiffre (AES: $l = 128$ Bit)
- Abhängigkeiten zwischen den Blöcken: gleiche Klartextblöcke liefern unterschiedliche Schlüsseltextblöcke
- Initialisierungsvektor IV muss nicht geheim sein, darf aber nicht vorhersagbar sein

Welchen Nachteil hat ECB bzgl. Sicherheit?

gleiche Klartextblöcke liefern gleiche Schlüsseltextblöcke $\Rightarrow$ ggf. Kodebuchanalysen möglich

Wie wirken sich Fehler bzw. Manipulationen während der Übertragung bei ECB und CBC aus?

EBC: Synchronisationsfehler: keine Fehlerfortpflanzung $\Rightarrow$ gezieltes Einfügen und Entfernen von Blöcken möglich

CBC: Fehler während der Übertragung

- additive Fehler: Fehlerfortpflanzung in den Folgeblock
- Synchronisationsfehler: 2 Blöcke betroffen

$\Rightarrow$ Verfahren eignet sich zur Authentikation: Manipulationen, Einfügen und Entfernen von Blöcken erkennbar