Datensicherheit, Zusammenfassung Vorlesung 12

Henry Haustein, Dennis Rössel

Wie erfolgt Ver- und Entschlüsselung bei der Betriebsart CTR?

Zählvariable verschlüsseln/entschlüsseln und $\oplus$ mit Klartext

Was sind Eigenschaften der Betriebsarten ECB, CBC und CTR?

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

CTR (Counter Mode)

- synchron
- Abhängigkeit von Position der verarbeiteten Einheit
- Direktzugriff auf einzelne Schlüsseltextblöcke möglich

Wie wirken sich additive bzw. Synchronisationsfehler bei diesen Betriebsarten aus?

ECB: keine Fehlerfortpflanzung bei additivem Fehler und Synchronisationfehler

CBC: Fehlerfortpflanzung in den Folgeblock bei additivem Fehler, 2 Blöcke bei Synchronisationfehler bzgl. ganzem Block betroffen bzw. Entschlüsselung fehlerhaft, bei Synchronisationsfehler bzgl. Bits (bis Blockgrenzen neu festgelegt werden)

CTR: keine Fehlerfortpflanzung bei additivem Fehler, anfällig gegen Synchronisationsfehler

Welchen Vorteil bietet der Counter Mode?

Effizienz

Welche dieser Betriebsarten eignet sich für die Berechnung eines MACs? Warum?

CBC-MAC

Wie erfolgt die Berechnung bzw. das Testen des MACs?

letzten Schlüsseltextblock als MAC anhängen (Empfänger verschlüsselt ebenfalls und vergleicht dann)

Was bedeutet *multiplikatives Inverses*? Wie kann es bestimmt werden?

$x \cdot x^{-1} \equiv 1 \mod n$, Bestimmung mittels erweiterter Euklidischer Algorithmus