CBC-MAC & CCM

Luc Spachmann

FSU Jena

27. Januar 2022

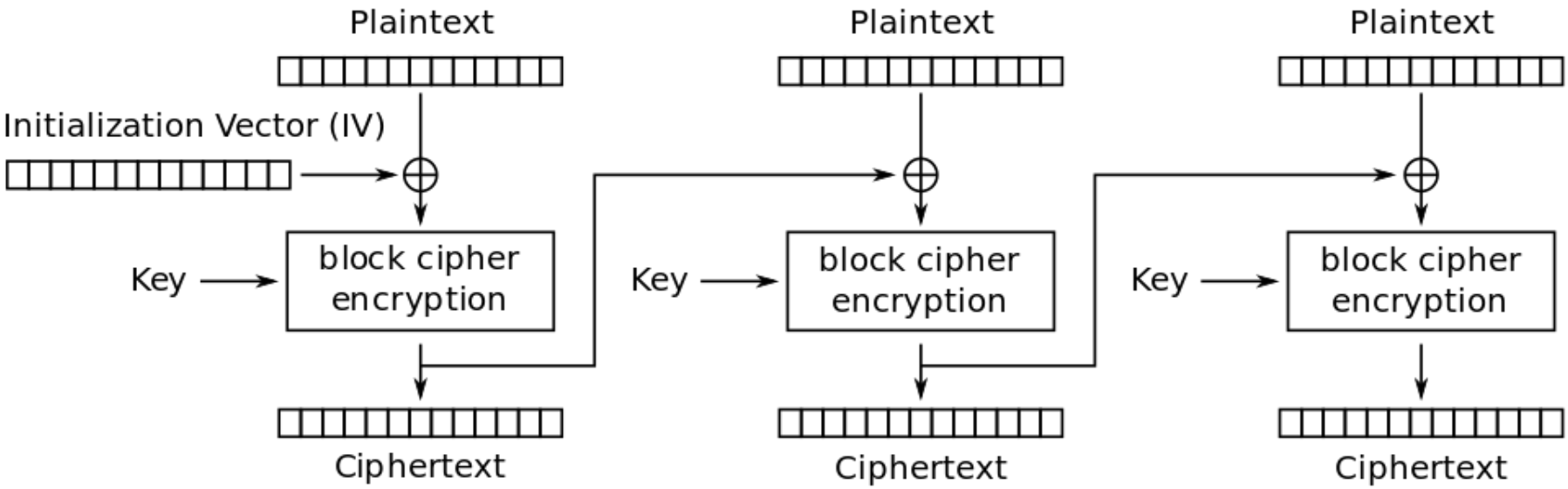
MACs

- 'Message Authentification Code'
- Hashfunktionen mit Schlüssel
- Schlüsselraum K
- Hashfunktion $h : K \times \Sigma^* \to \Sigma^m$
- Symmetrische Schlüssel
- Anwendung: Nachrichtenauthentifizierung

CBC-MAC

- Benutze symmetrische Blockchiffre im CBC-Modus mit Verschlüsselungsfunktion $E(k, m)$
- CBC = Cipher-Block-Chaining
- Schlüssel von MAC entspricht Schlüssel k von Blockchiffre
- Blockchiffre hier: AES
- Für Eingabe x wird erst $E(k, x)$ verschlüsselt.
- Letzter Block ist dann Hashwert

Erinnerung: CBC



Cipher Block Chaining (CBC) mode encryption

Abbildung: Quelle: Wikipedia

- IV$=0$

CCM-Modus (Counter with CBC-MAC)

- Sei $x = x_1||...||x_n$ Klartext mit Blocklänge m (für AES: $m = 128$)
- Gegeben: Schlüssel k und 64 Bit Zahl *nonce*
- *nonce* muss nicht geheim sein, aber nur einmalig verwendet
- Sei $ctr = nonce||00..0$ mit 00...0 64 Bit lang.
- Berechne Folge $T_i = ctr + i \mod 2^m$ für $i = 0, ..., n$
- Verschlüssele $y_i = x_i \oplus E(k, T_i)$ für $i = 1, ..., n$
- $tmp =$ CBC-MAC(k, x) und $y' = T_0 \oplus tmp$
- Kryptotext ist $y = y_1||...||y_n||y'$
- Entschlüsseln vollkommen Analog
  $y_i = x_i \oplus E(k, T_i) \Leftrightarrow x_i = y_i \oplus E(k, T_i)$
- Verifiziere CBC-MAC$(k, x) = y' \oplus T_0$

Aufgaben

- Implementiere CBC-MAC und CCM
- Benutze dazu AES aus früherer Übung