Kryptografie und -analyse, Zusammenfassung Vorlesung 8

Henry Haustein

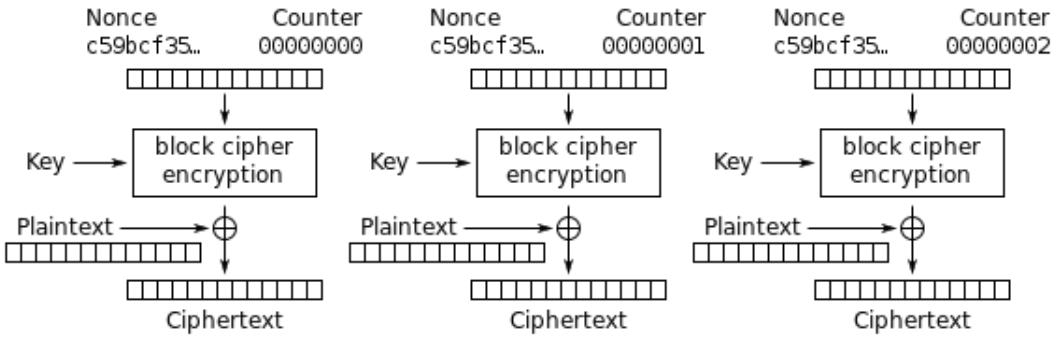
Warum und wie kann CBC zur Authentikation verwendet werden? Welche Schwachstelle ist bekannt?

Verkettung der Schlüsseltextblöcke macht Manipulationen erkennbar, weil sich die Veränderung bis zum Ende durchzieht. Eine Schwachstelle ist existenzielles Brechen: Durch Manipulation des vorherigen Schlüsseltextes können einzelne Bytes des aktuelles Klartextes verändert werden. Die Veränderung fällt ab dem nächsten Schlüsseltext auf. Das kann mit CBC-MAC verhindert werden, allerdings gibt es dort eine andere Schwachstelle namens *Length-Extension*: Ein Angreifer kann aus zwei gültigen Nachricht-MAC-Paaren einen gültigen MAC für eine neue Nachricht (die Konkatenation der beiden Nachrichten) erzeugen. Zwei Modifikationen können diesen Angriff verhindern: Jeder Nachricht kann die Nachrichtenlänge vorangestellt werden oder der MAC-Block wird zusätzlich mit einem zweiten Schlüssel verschlüsselt.

Ein interessantes Youtube-Video dazu (behandelt allerdings CFB, der obige Angriff funktioniert aber fast genau so): https://www.youtube.com/watch?v=i-2UgCDdhpM&t=822s

Wie funktioniert der Countermode?

Zur Verschlüsselung wird ein Initialisierungsvektor IV mit dem Schlüssel k verschlüsselt und so ein Zwischenschlüssel produziert. Dieser wird im Anschluss mittels einer XOR-Operation mit dem Klartext kombiniert. Daraus entsteht der Geheimtext.



Counter (CTR) mode encryption

Wie wirken sich bei dieser Betriebsart Fehler bzw. Manipulationen während der Übertragung aus?

Fehler und Manipulationen fallen im aktuellen Block auf, falls ein Block gelöscht wird, geht die gesamte Synchronisation verloren.

Warum darf der Zähler bei Verwendung desselben Schlüssels nur einmal verwendet werden?

Das erzeugt die selbe Folge von Schlüsseln und damit wird der selbe Plaintext zum selben Ciphertext.

Welche Elemente gehören zu $\mathbb{Z}_n$, $\mathbb{Z}_n^*$ bzw. $\mathbb{Z}_p$, $\mathbb{Z}_p^*$?

$\mathbb{Z}_n = \{0, 1, ..., n-1\}$, $\mathbb{Z}_n^* = \{\text{teilerfremde Zahlen zu } n\}$, wenn n prim, dann $\mathbb{Z}_n^* = \{1, 2, ..., n-1\}$

Wie wird die Anzahl der Elemente dieser Gruppen bestimmt ($n = p \cdot q$; p, q prim)?

$\mathbb{Z}_n$ hat n Elemente, $|\mathbb{Z}_n^*| = \Phi(n) = \Phi(p \cdot q) = (p-1)(q-1)$

Wie werden multiplikative Inverse bestimmt?

Erweiterter euklidischer Algorithmus: EEA(a, n) $\Rightarrow ua + vn = 1 \Rightarrow u = a^{-1} \mod n$

Wie können Primzahlen erzeugt werden?

Probabilistischer Test nach Rabin-Miller: Falls p prim, dann $\forall a \in \mathbb{Z}_p^* : a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Falls p nicht prim, dann gilt dies höchstens für $\frac{1}{4}$ der möglichen a.

Was versteht man unter einer zyklischen Gruppe? Was unter Generator?

Alle Elemente einer Gruppe G lassen sich durch einen Generator $g \in G$ "generieren" durch Potenzieren: $G = \{g^0, g^1, ...\} = \langle g \rangle$