Bearbeitung von Praktikumsaufgabe 2

Aufgabe 1

a Mit Hilfe von Abbildung 1 und NIST SP800-108 erklärt sich die Funktionsweise dieser KDF[1] wie folgt:

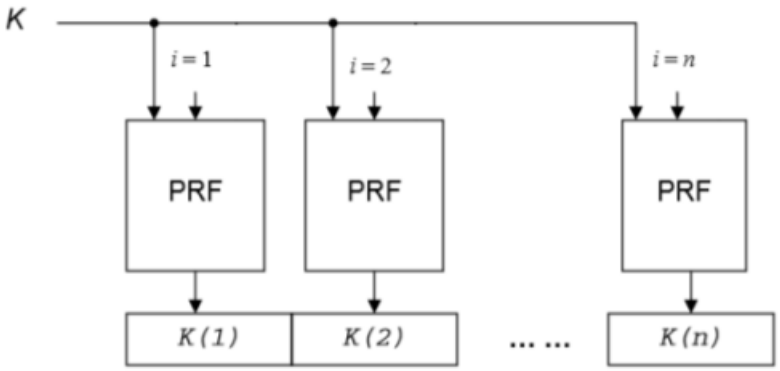

Abbildung 1: Aus dem Übungsblatt

Vom Eingangsschlüssel K mit der Länge n wird ein Ausgangsschlüssel $K(1), K(2), \ldots, K(n)$ abgeleitet. Dazu wird die i-te Stelle des Eingangsschlüssel durch eine definierte PRF[2] auf $K(i)$ transformiert. Wenn $K(i)$ länger ist als die i-te Stelle, dann wird der Eingangsschlüssel auf den Ausgangsschlüssel „expandiert“.

b In Kapitel 4 des Standards werden als geeignete Primitive fr die PRF MACs[3] genannt: Kryptographische Algorihmen, die mit symmetrischen Schlüsseln arbeiten. Sie können verschieden lange Inputwerte auf immer gleich lange Ausgangswerte transformieren. Untergruppe davon sind HMAC und CMAC.
ZusÃ¤tzlich eignen sich Verkettete Verschlüsselungen / Blockchiffre als Kandidaten für die PRF, bekannt aus KVA 1: CBC [4], OFB [5], CFB [6] und CTR [7].

c Die im Standard beschriebenen KDFs erinnern an bekannte Konstruktionen.
Die erste KDF, siehe Abbildung 2, ist eine Hashkonstruktion, weil unterschiedlicher Input in Blöcke gleicher Länge ausgegeben wird. Außerdem wird die Ausgabe nicht weiter in den folgenden Schritten berücksichtigt. Die zweite KDF in Abbildung 3 hat eben diese Verkettung zwischen vorherigem Ausgabeblock und nächstem Eingabeblock, sie erinnert also an eine CBC-Konstruktion. Die dritte und letzte KDF in Abbildung 4 ist stellt eine Addition der beiden vorherigen dar: Der obere Teil ist ein CBC, dessen schrittweise Ausgabe nochmal gehasht wird.

[1] Key Derivation Function
[2] Pseudo-Random Function
[3] Message Authentication Code
[4] Cipher Block Chaining Mode
[5] Output Feedback Mode
[6] Cipher Feedback Mode
[7] Counter Mode

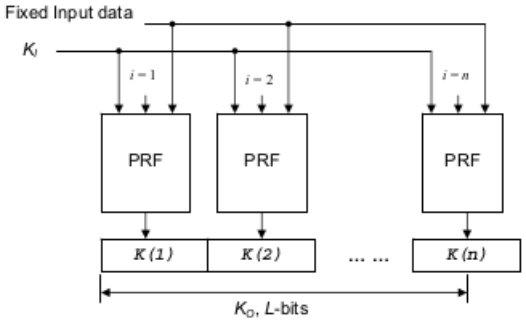

Abbildung 2: Aus dem Standard (Figure 1): „KDF in Counter-Mode“

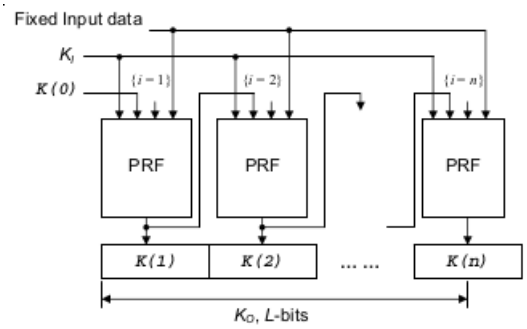

Abbildung 3: Aus dem Standard (Figure 3): „KDF in Feedback Mode“

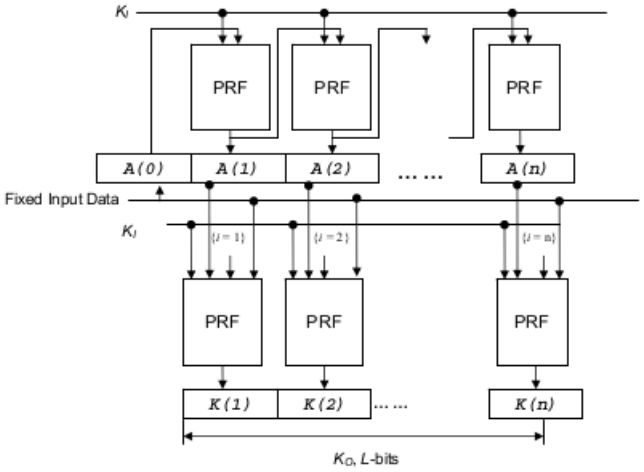

Abbildung 4: Aus dem Standard (Figure 4): „KDF in Double-Pipeline Iteration Mode“

d Nach der Betrachtung der Konstruktion ist klar, dass der Eingangsschlüssel so zufällig sein muss, dass er mit hoher Wahrscheinlichkeit einmalig ist. Diese Einmaligkeit ist nicht bei allen Passwörtern gegeben. Ein Angreifer macht sich den beschränkten Passwortraum (im Vergleich zum unbeschränkten zufälligen Schlüsselraum) zur Nutze und berechnet für alle möglichen Eingaben im Passwortraum die ausgegebenen Werte. Abschließend vergleicht er die den anzugreifenden Ausgabewert mit seinen Berechneten und kann bei Gleichheit auf den Eingabewert schließen.