Aufgaben zu Multimediadatensicherheit

Lösen Sie die nachfolgenden Aufgaben zur Klausurvorbereitung.

MMDS 01.

a) Ein $m \cdot n$ ($m, n \in \mathbb{N}\backslash\{0\}$) Pixel großes (Grauwert-)Bild soll durch Permutation seiner Pixel verschlüsselt werden. Geben Sie eine Formel an, die die Anzahl der möglichen Verschlüsselungsergebnisse allgemein bestimmt.

b) Geben Sie eine Formel an, die die Anzahl aller möglichen $m \cdot n$ ($m, n \in \mathbb{N}\backslash\{0\}$) Pixel großen (Grauwert-)Bilder allgemein bestimmt, wenn $p \in \mathbb{N}\backslash\{0\}$ verschiedene Grauwerte pro Pixel möglich sind.

c) Wie groß ist der Schlüsselraum (die Anzahl der Möglichkeiten, die bei einem Bruteforce-Angriff im schlimmsten Fall ausprobiert werden müssen) eines mit dem in a) beschriebenen Verfahren verschlüsselten Bildes für $m = n = 4$ bei vier möglichen Grauwerten pro Pixel?

d) Kann ein mit dem in a) beschriebenen Verfahren verschlüsseltes Bild immer erfolgreich dekodiert werden, wenn es vor der Entschlüsselung JPEG-komprimiert wurde?

MMDS 02.

a) Ein Verschlüsselungsalgorithmus ändere die Vorzeichen aller AC-Koeffizienten eines $4 \cdot 4$-Blockes in einem H.264-kodierten Video. Wie groß ist der Schlüsselraum maximal?

b) In einem H.264-Bitstrom werden nur die Vorzeichen jener AC-Koeffizienten gespeichert, die ungleich null sind. Wie klein ist der Schlüsselraum für den Algorithmus aus a) minimal, wenn der Algorithmus direkt auf dem Bitstrom arbeitet?

MMDS 03.

a) Ein Block eines JPEG-Bildes sei durch fünf vertauschbare Bitgruppen (bestehend aus Huffman-Codewörtern) kodiert. Durch Verschlüsselung wird die Reihenfolge der Bitgruppen zufällig verändert. Wie groß ist die Wahrscheinlichkeit, dass sich deren Reihenfolge nicht ändert, wenn alle Anordnungsmöglichkeiten gleich wahrscheinlich sind?

b) Wie ändert sich die Wahrscheinlichkeit aus a), wenn zwei unabhängige Blöcke betrachtet werden?

c) Kann der Algorithmus aus a) derart abgewandelt werden, dass er die Bits innerhalb einer Bitgruppe auf gleiche Weise vertauscht, wenn der verschlüsselte Block formatkonform sein soll?

Lösungen (zur Überprüfung)

MMDS 01. a) $(m \cdot n)!$, b) $p^{m \cdot n}$, c) $2^{32} = 4.294.967.296$
MMDS 02. a) 32.768, b) 1
MMDS 03. a) $\frac{1}{120}$, b) $\frac{1}{14.400}$