Hashfunktionen - Kontrollaufgaben

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de, Raum 149B
Version: 1.0

1. Verständnis

Hashfunktionen

1.1. Beurteilen Sie folgende Aussagen

01	Die Anforderungen an eine Hashfunktion sind vom Einsatzbereich abhängig.
02	Zur Virenerkennnung werden - unter anderem - auch Hashfunktionen verwendet.
03	Hashfunktionen sind nicht deterministisch.
04	Hashfunktionen können zur Absicherung der Integrität verwendet werden.
05	Die Mindestausgabelänge für eine sichere Hashfunktion beträgt mindestens 512 Bit.
06	Der Input eine Hashalgorithmuss muss ein vielfaches der Blockgröße des Hashes betragen.
07	Poly 1305 ist nur deswegen sicher weil die Nonce 96Bit lang ist.
08	Jeder Hashalgorithmus, der starke Kollisionsresistenz bietet, kann zur Absicherung der Integrität verwendet werden.
09	Jeder Hashalgorithmus, der schwache Kollisionsresistenz bietet, kann zum Hashing von Passwörtern verwendet werden.
10	Preimage Resistance ist nur beim Hashen von Passwörtern relevant.
11	HMAC und Poly 1305 sind Algorithmen, die dem gleichen Zweck dienen.
12	Bei Poly 1305 und HMAC kann der Schlüssel mehrfach verwendet werden.
13	Bei HMACs wird der Schlüssel, der als Eingabe dient immer erst gehasht.
14	Poly 1305 ist eine Merkle-Damgard Konstruktion.
15	Eine Nonce ist eine Zahl, die einmal generiert wird und möglichst zufällig sein sollte. Danach kann diese für die Absicherungen mehrer Verbindungen mit den selben Partnern wiederverwendet werden.