Zufallszahlen und Stromchiffre - Kontrollaufgaben

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

1. Grundlagen

Fragen

1.1. Zufallszahlen

1. Wie unterscheidet sich ein TRNG von einem PRNG?
2. Welche Formen der Unvorhersagbarkeit gibt es?
3. Beschreiben Sie Maurer's Test auf Zufälligkeit.
4. Ist ein Lauflängentest besser geeignet als ein Häufigkeitstest, um die Zufälligkeit einer Bitfolge zu überprüfen?
5. Welche Anforderungen stellen wir an ein *Seed*?
6. Welche grundsätzlichen Möglichkeiten gibt es Pseudozufallszahlen zu erzeugen?
7. Welche Betriebsmodi für Blockchiffren sind geeignet für die Erzeugung von Pseudozufallszahlen.
8. Wenn man einen TRNG hat, der (leicht) verzerrt ist, wie kann dieser konditioniert werden?
9. Was besagt der Wert, der durch die Shannon-Entropie berechnet wird (nicht normalisiert)?

Fragen

1.2. Stromchiffren

1. Welche Bedeutung hat der Schlüssel bei Stromchiffren?
2. Welche Bedeutung hat der IV/die Nonce bei Stromchiffren?
3. Wie unterscheiden sich die Funktionen zur Berechnung des nächsten Zustands und die Schlüsselstromfunktion bei Stromchiffren?