Rechnersicherheit - Übung 02

Dennis Hägler und Martin Görick

29. April 2015

1 Aufgabe 1

a) In der Partitions- oder Festplattenverschlüsselung

b) Die Sektornummer des Chifriertextes müssen vorhersagbar sein

c) Weil zusammenhängende Texte zusammen gespeichert werden, wenn keine Fragmentierung vorliegt.

d) durch Permutation des Chifriertextes

2 Aufgabe 2

a) Durch die kleinen S-Boxen kann über raten von Texten den Schlüssel erhalten.

b) Über ein lineares Gleichungssystem kann man ohne Substitution den Schlüssel erhalten.

3 Aufgabe 3

Bei AES geht es um längere Texte, deshalb werden diese in kleine Parts aufgeteilt und diese mittels einer SPN verschlüsselt und am Ende zusammengefuegt. Um dies sicherer zu gestallten wird der Geheimtext des vorherigen Block auf den aktuellen Adddiert und fuer den ersten Block ein Initialvektor genommen.

4 Aufgabe 4

b) Wenn der letzte Block fehlerhaft übertragen wurde, dann ist nur der letzte Klartextblock davon betroffen, da dieser nur fuer diese Entschlüsselung verwendet wird. Ansonsten der Klartextblock des Geheimblockes und der folgende, da Beide diesen verwenden.