Übungsblatt 6

Aufgabe 1 (Kryptologie)

1. Was ist Kryptographie?
2. Was ist Kryptoanalyse?
3. Was ist Kryptologie?
4. Was ist Steganographie?
5. Was ist der Unterschied zwischen Symmetrischen und Asymmetrischen Kryptosystemen?
6. Nennen und beschreiben Sie zwei Arten von kryptoanalytischen Angriffen.
7. Wie arbeiten Transpositionsverfahren?
8. Nennen Sie ein Beispiel für ein Transpositionsverfahren.
9. Wie arbeiten Monoalphabetische Substitutionsverfahren?
10. Nennen Sie zwei Beispiele für Monoalphabetische Substitutionsverfahren.
11. Wie arbeiten Polyalphabetische Substitutionsverfahren?
12. Nennen Sie zwei Beispiele für Polyalphabetische Substitutionsverfahren.
13. Wie arbeiten Monographische Substitutionsverfahren?
14. Nennen Sie zwei Beispiele für Monographische Substitutionsverfahren.
15. Wie arbeiten Polygraphische Substitutionsverfahren?
16. Nennen Sie ein Beispiel für ein Polygraphisches Substitutionsverfahren.
17. Was ist der Unterschied zwischen Stromchiffren und Blockchiffren?
18. Welche Aufgabe haben der Diffie-Hellmann-Algorithmus und der Elgamal-Algorithmus?
19. Beschreiben Sie die Gefahr des Man-in-the-Middle-Angriffs bei Diffie-Hellmann.
20. Was kann gegen die Gefahr des Man-in-the-Middle-Angriffs bei Diffie-Hellmann getan werden?
21. Was ist die Aufgabe einer Hashfunktion bzw. Streuwerfunktion?

22. Woran bemisst sich die Qualität einer Hashfunktion?
23. Nennen Sie zwei Hashfunktionen.
24. Wofür verwendet man Regenbogentabellen?
25. Was kann gegen die Verwendung von Regenbogentabellen unternommen werden?

Aufgabe 2 (Steganographie)

1. Was ist Steganographie?
2. Was sind Semagramme?
3. Was sind Zinken?
4. Nennen Sie die beiden Zielsetzungen von Steganographie.
5. Was ist Steganalyse?
6. Was sind Plagiatsfallen?
7. Was sind Wasserzeichen?
8. Beschreiben Sie Traitor Tracing mit Hilfe digitaler Fingerabdrücke.