

**Aufgabe 1 (19 Punkte)**

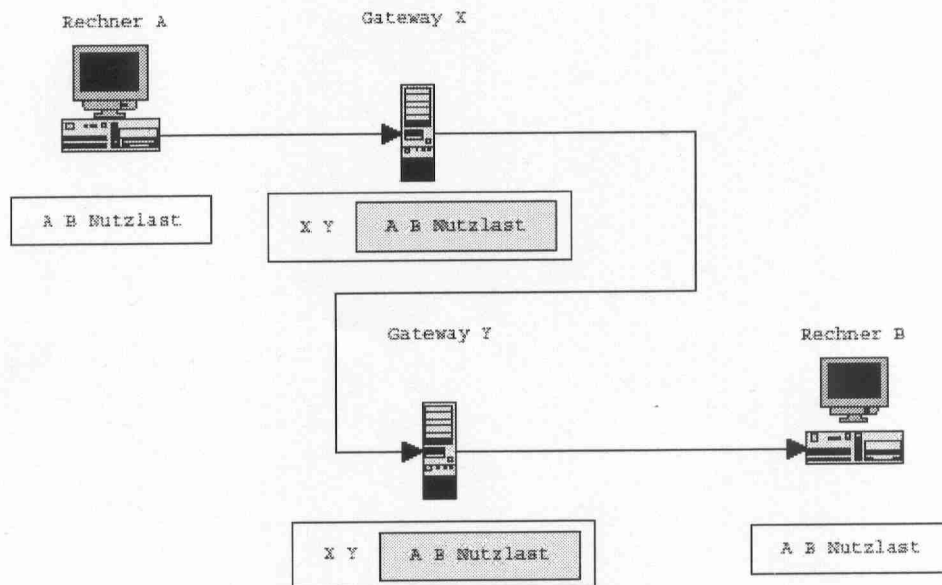
- Was versteht man unter linearer Kryptoanalyse ? (7 Punkte)
- Die lineare Kryptoanalyse wurde entwickelt, um einen speziellen Verschlüsselungsalgorithmus anzugreifen, welchen ? (4 Punkte)
- Beschreiben Sie kurz das Prinzip der linearen Kryptoanalyse. (8 Punkte)

**Aufgabe 2 (19 Punkte)**

- Nennen Sie kurz die Hauptmaßnahmen, die man benutzt um einen privaten PC zu schützen. (7 Punkte)
- Erklären Sie wie man sich als Benutzer unter Windows gegen die folgenden Viren schützen kann:
  - Boot Sektor Viren (6 Punkte)
  - Dateiviren (6 Punkte)

**Aufgabe 3 (19 Punkte)**

Das Prinzip des Tunneling von IP-Paketen bezeichnet eine Technik, bei der beliebige Datenpakete komplett als Nutzlast in einem anderen IP-Paket versendet werden.



- Aus welchen Teilen besteht ein IP-Paket (5 Punkte)
- Falls das Gateway X das ursprüngliche IP-Paket verschlüsseln soll, bevor es in das neue IP-Paket verpackt wird: Welche Klasse von Verschlüsselungsverfahren wird benutzt, und wie tauschen die Gateways die Schlüssel aus ? (14 Punkte)

**Aufgabe 4 (5 Punkte)**

- Welche 3 Arten von Anbietern werden im Kurs unterschieden ? (3 Punkte)
- An welche Art Anbieter richten sich die Telefondienst-Gesetze ? (2 Punkte)

**Aufgabe 5 (19 Punkte)**

- Welche Arten von Intrusion Detection Systemen (IDS) werden im Kurs unterschieden ? (3 Punkte)
- Welche dieser Arten erkennt in der Regel nicht den Angriff selbst, sondern nur seine Auswirkung ? (2 Punkte)
- Wir betrachten ein Networ-based IDS, das von jedem IP-Paket source address und destination address (je 32 Bit) betrachtet. Das betrachtete IP-Netz hat eine Bandbreite von 100MBit/s (1M = 1Million) und sei von IP-Paketen der festen Länge 60 Byte zu 60 % ausgelastet. Wie viele Daten muss das IDS pro Tag mindestens protokollieren, wenn alle Adressen gespeichert werden ? (14 Punkte)

**Aufgabe 6 (19 Punkte)**

- Was versteht man unter URL Hacking ? (7 Punkte)
- Wie kann man im folgenden Programm einen Buffer-Overflow-Angriff ausführen ? (12 Punkte)

```
# include <stdio.h>
int main (int argc, char *argv[])
{
    char strng1[8]="TestWd\0";
    char strng2[8];

    printf("Input Key:\n");
    gets(strng2);

    if(strncmp(strng1, strng2, 8)) {printf("Wrong\n"); exit(-1);}
    else main_application();

    return();
}
```