**11. Verschlüsselungsverfahren**

Sie lösen die folgenden 3 Aufgaben 11.1 bis 11.3 und mindestens die  
 Zusatzaufgaben und melden alle Ihre Probleme bzw. Unklarheiten spätestens bei der Besprechung!

**Aufgabe 11.1:** XOR-Anwendung

Binäre Ver- und Entschlüsselung mit der XOR-Verknüpfung:

Verwandeln Sie im Folgenden die ASCII-Codewerte der Buchstaben in Binärzahlen:   
Verschlüsseln Sie (mit Papier und Bleistift) die ersten vier Buchstaben des Wortes „FACHSCHULE“ mit dem Schlüssel „IFA“ durch eine XOR-Operation.

Prüfen Sie die Entschlüsselung durch erneutes XOR-verknüpfen des Schlüssels,   
nun aber mit dem Chiffrat.

**Aufgabe 11.2:** RSA-Verschlüsselung

Lesen Sie das Dokument „Funktionsweise RSA-Verschlüsselung“ und   
spielen Sie das Beispiel mit folgenden Zahlenwerten durch: p = 17 ; q = 3 ; e = 5 ; m = 11

**Aufgabe 11.3:** Anwendung der RSA-Verschlüsselung

In den Modulunterlagen finden Sie die Software Gpg4win.

Installieren Sie diese auf Ihren vmWP1 (inkl. Der Optionen Kleopatra und GpgEX).

- Erstellen Sie ein neues Schlüsselpaar (IET-Mailadresse verwenden). Exportieren Sie nun Ihren öffentlichen Schlüssel in eine Datei. Deponieren Sie diese wiederum in den Ordner «Keys» auf dem Klassenshare.

- Importieren Sie den öffentlichen Schlüssel Ihres Nachbarn.

- Verschlüsseln Sie nun eine Datei (Kontextmenu im Explorer) mit dem öffentlichen Schlüssel Ihres Nachbarn und senden Sie ihm diese per Mail zu.

- Kann Ihr Nachbar die Datei entschlüsseln?

**Zusatzaufgabe für Interessierte:** CRC-Prüfsumme

Um die korrekte Übertragung von Ethernet-Frames und vielen anderen Dateien zu   
garantieren wird die CRC-Prüfsumme vor dem Versand gebildet und   
nach dem Empfang geprüft.