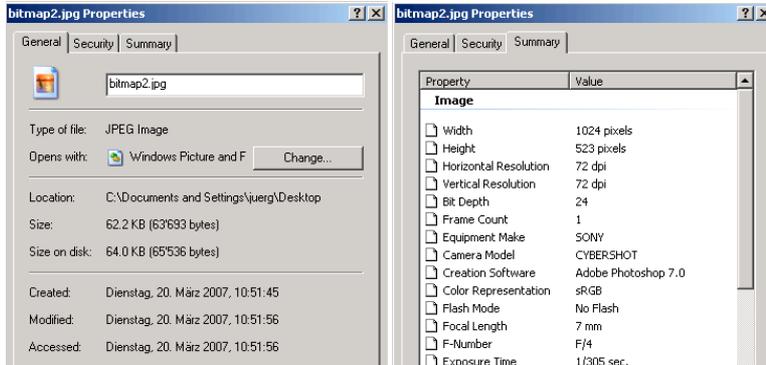


Zeit: 35' Pro Aufgabe max. 1P

Aufgabe 1

Wie klein (in Prozent!) ist das vorliegende «bitmap2.jpg» gegenüber dem unkomprimierten Originalbild (=100%). In ihrer Berechnung soll nur das reine Bitmap einfließen! Ohne Fileheader etc.)



Originalbild: 1024 x 523 x 3B = 1606656 B
JPG: 63693 B

$100 / 1606656 \times 63693 = 3.964 \%$

Bildeigenschaften von bitmap2.jpg

Aufgabe 2

Wie viele **Kilo-Bytes** würde das File mit selbiger Auflösung (d.h. gleich viel Pixel in Länge und Breite) **maximal** benötigen, wenn es im **GIF-Format** gespeichert würde? Beachten Sie, dass 1kB auf dem Harddisk tatsächlichen 1k Byte entsprechen. Im weiteren ist die gewählte Blockgröße des benutzten Filesystems 4k, d.h. es wird jeder angebrochene 4k-Block mitgezählt. (Bsp.: Ein File mit der Größe 6kB belegt auf dem HD zwei 4k-Blöcke, somit also 8k!)

Originalbild: 1024 x 523 x 1B = 535552 B ; $535552 \text{ B} / 1024 = 523\text{kB}$ Somit 524kB

Aufgabe 3

Ein farbiges 24-Bit-Farbpixel hat die dezimalen RGB-Werte von $P_1(186/28/58)$ Welchem Graustufenwert in Dezimal entspricht dieses weinrote Pixel P_1 ?

Rotanteil: 30% Grünanteil 60% Blauanteil 10%: $186 \times 0.3 + 28 \times 0.6 + 58 \times 0.1 = 78$

Aufgabe 4

Ein Bild mit den Abmessungen 640 Pixel x 480 Pixel, was übrigens dem VGA-Standard entspricht, wird mit 4:2:2-Subsampling (Unterabtastung) datenreduziert. Um wieviel % wurde das Bild komprimiert?

4:2:2 bedeutet:

$100\% + 50\% + 50\% = 200\%$ gegenüber dem Original mit $100\% + 100\% + 100\% = 300\%$

Das Bild wurde somit um 33.3% datenreduziert!

Aufgabe 5

Welche Bildartefakte ergeben sich, wenn man beim JPG-Format eine zu starke Komprimierung wählt?

Blockartefakte. Quadratische Pixelblöcke mit derselben Farbe.

Aufgabe 6

Sie möchten auf ihrer Auto-Webseite mit einer Art Daumenkino die Funktion eines Kolbenmotors und dazu noch Fotografien von aktuellen Motoren zeigen. Welche Medienformate wählen sie, damit sie den grösstmöglichen Nutzerkreis erreichen können?

Daumenkino: Animiertes GIF, Fotos: JPG

Aufgabe 7

Sie erhalten folgende geheime Botschaft mit ROT3 (Rotationschiffre) übermittelt: **WHFKQLN**
 Was heisst im Klartext?

TECHNIK

Aufgabe 8

Eine Personengruppe mit **658 Teilnehmern** möchte sich gegenseitig **symmetrisch** verschlüsselte Files zuschicken. Wie viele Schlüssel müssen dafür insgesamt erstellt werden?

$s = n \cdot (n-1) / 2$; $s = 658 \cdot (658-1) / 2 = 216 \cdot 153$ Schlüssel

Aufgabe 9

Was versteht man unter einem sog. **hybriden** Verschlüsselungsverfahren?

Kombination von asymmetrischer Verschlüsselung für Schlüsseltausch und anschliessender symmetrischer Verschlüsselung der Botschaft.

Aufgabe 10

Auf ihrer Webseite stellen sie Gratis-Software zur Verfügung. Interessierte sollen sich diese SW herunterladen und bei sich installieren können. Um die Authentizität und Integrität der Software zu überprüfen, stellen sie auf ihrer Webseite auch ihr Public-Key-Zertifikat zur Verfügung. Man nennt das digital signieren! Erklären die mit ein paar Worten oder einem Bild den technischen Vorgang bei der digitalen Signatur und zwar auf Erzeugerseite (hier der SW-Lieferant) und Verbraucherseite (hier des SW-Bezüger)!

Vom Dokument wird ein Hashwert erzeugt und dieser mit dem Private-Key des Absenders verschlüsselt. Der Empfänger erhält das ungeschützte Originalfile und den verschlüsselten Hashwert. Der Empfänger entschlüsselt den Hashwert mit dem Public-Key des Absenders und vergleicht den entschlüsselten Hashwert mit dem selber generierten Hashwert des Originaldokuments. Die Hashwerte müssen übereinstimmen, sonst liegt eine Fälschung vor!