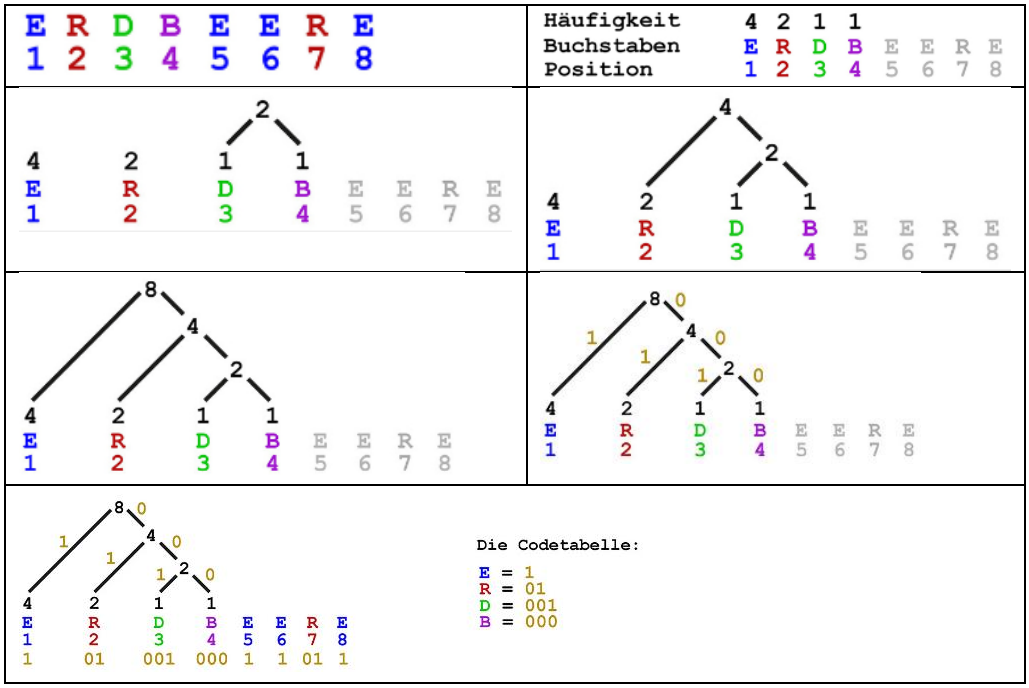
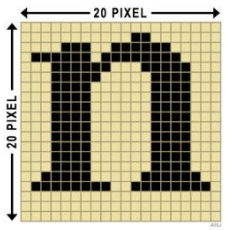
Verlustlose Komprimierung

Der Huffmancode



RLC (Run Length Coding)



Ab erstem Pixel oben links:
31 x Weiss,
2 x Schwarz,
11 x Weiss,
3 x Schwarz,
2 x Weiss,
6 x Schwarz,
6 x Weiss,
6 x Schwarz,
1 x Weiss,
8 x Schwarz,
4 x Weiss

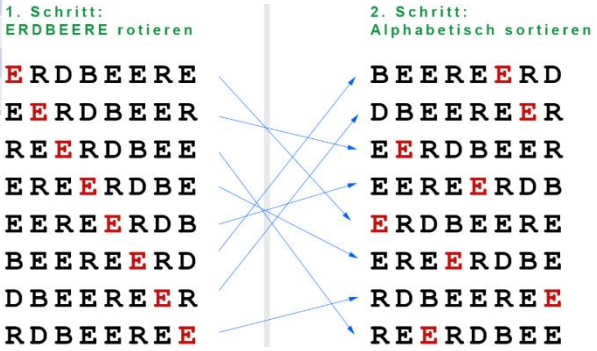
➔ 11111
00010
01011
00011
00010
00110
00110
00001
01000
00100

LZW (Lexikalisches Verfahren)

Schritt	Zeichenkette	Gefunden	Gespeichert	Temporärer Wörterbucheintrag
1.	ENTGEGENGENOMMEN	E	E	EN → «256»
2.	ENTGEGENGENOMMEN	N	N	NT → «257»
3.	ENTGEGENGENOMMEN	T	T	TG → «258»
4.	ENTGEGENGENOMMEN	G	G	GE → «259»
5.	ENTGEGENGENOMMEN	E	E	EG → «260»
6.	ENTGEGENGENOMMEN	GE → «259»	«259»	GEN → «261»
7.	ENTGEGENGENOMMEN	N	N	NG → «262»
8.	ENTGEGENGENOMMEN	GEN → «261»	«261»	GENO → «263»
9.	ENTGEGENGENOMMEN	O	O	OM → «264»
10.	ENTGEGENGENOMMEN	M	M	MM → «265»
11.	ENTGEGENGENOMMEN	M	M	ME → «266»
12.	ENTGEGENGENOMMEN	EN → «256»	«256»	-

Schritt	Übermittelte Zeichenkette	Aktuelles Zeichen	Ausgabe	Temporärer Wörterbucheintrag
1.	ENTGE«259»N«261»OMM«256»	E	E	-
2.	ENTGE«259»N«261»OMM«256»	N	N	EN → «256»
3.	ENTGE«259»N«261»OMM«256»	T	T	NT → «257»
4.	ENTGE«259»N«261»OMM«256»	G	G	TG → «258»
5.	ENTGE«259»N«261»OMM«256»	E	E	GE → «259»
6.	ENTGE«259»N«261»OMM«256»	G	GE	EG → «260»
7.	ENTGE«259»N«261»OMM«256»	N	N	GEN → «261»
8.	ENTGE«259»N«261»OMM«256»	G	GEN	NG → «262»
9.	ENTGE«259»N«261»OMM«256»	O	O	GENO → «263»
10.	ENTGE«259»N«261»OMM«256»	M	M	OM → «264»
11.	ENTGE«259»N«261»OMM«256»	M	M	MM → «265»
12.	ENTGE«259»N«261»OMM«256»	E	EN	ME → «266»

BWT (Burrows-Wheeler-Transformation)



1 : BEEREERD
2 : DBEEREER
3 : EERDBEER
4 : EEREERDB
5 : ERDBEERE
6 : EREERDBE
7 : RDBEEREE
8 : REERDBEE

Lösung:
- DRRBEEEE5
- D2RB4E5

Verlustvolle Komprimierung

Auflösung reduzieren

durch Verkleinern der Bildgrösse, weil es dann weniger Pixel benötigt, um es abzuspeichern.

Speicherreduzieren durch reduzieren der Farbauflösung, Speicherreduzieren durch Erstellen einer Farbtabelle, das macht man um nicht jeden Pixel mit RGB darzustellen, sondern mit einer Farbtabelle (kann nur 256 Farben darstellen, wenn man benachbarte Pixel kombiniert sieht es aus als ob es eine Drittfarbe hat)

Speicherreduzieren durch verringern der Bildwiederholrate, wenn man die Rate an Bilder pro Sekunde verkleinert läuft es immer noch flüssig benötigt aber weniger Speicher.

Speicherreduzieren durch darstellen der Differenzbilder bei Video, wenn man nur das darstellt was sich ändert, kann man Speicher sparen, da man nicht das ganze Bild ändern muss.

Chroma-Subsampling, Bei 4:1:1 bedeutet dies Y=100%, Cb=25%, Cr=25% und somit gegenüber dem Original (300%) Dateigrösse halbiert. Man wandelt das RGB-Bild in ein YCbCr

Speicherreduzieren durch reduzieren der Samplingrate, das ist wenn man die Grenzfrequenz tiefer stellt und man kann auch noch die Auflösung herunter tun um Speicher zu sparen. Theoretische Ersparnis bei einer Samplingrate-Reduktion von 44.1kHz auf 8kHz.

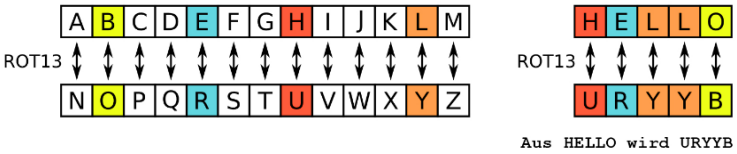
MPEG/h.264: H. 264 oder MPEG-4 AVC (Advanced Video Coding) ist ein Videocodierungsformat für das Aufzeichnen und Verteilen von Full-HD-Video und Audio. Dieses Format wurde von der ITU-T Video Coding Experts Group (VCEG) gemeinsam mit der ISO/IEC JTC1 Moving Picture Experts Group (MPEG) entwickelt und gepflegt.
MPEG4: MP4 ist die digitale Containerdatei und MPEG-4 ist der Standard für die Kodierung der Videoinhalte in MP4-Dateien.

Progressive/Interleaced (Halbbildverfahren)

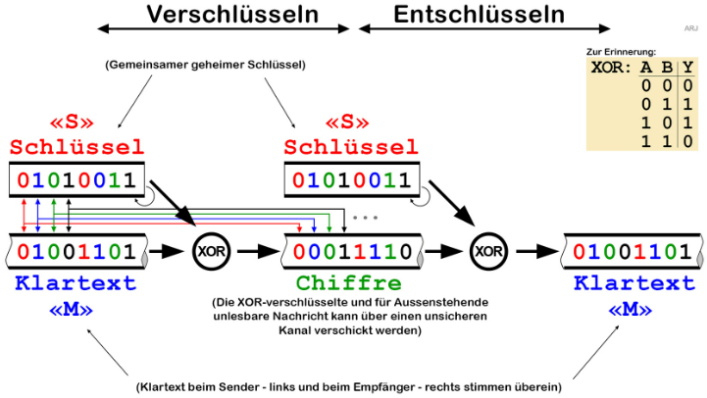
Bei 1080p und 1080i handelt es sich beides Mal um die Auflösung von 1920 x 1080 Pixeln. Der Unterschied besteht im Bildaufbau. So steht das **P** für „**P**rogressive Scan“ und beschreibt, dass jedes einzelne Bild aus einem Vollbild (*Frame*) besteht. Das **I** steht für „**I**nterlaced“ (*dt. Zeilensprungverfahren*) und sagt aus, dass die Bilder als Halbbilder (*Fields*) gesendet werden. Dabei baut sich ein vollständiges Bild somit aus zwei unterschiedlichen Halbbildern auf. Zuerst werden dabei alle ungeraden Zeilen (*Upper Field, Odd-Field*) mit Bildinformationen versorgt und danach die geraden Zeilen (*Lower Field, Even-Field*).

Symmetrische Verschlüsselung

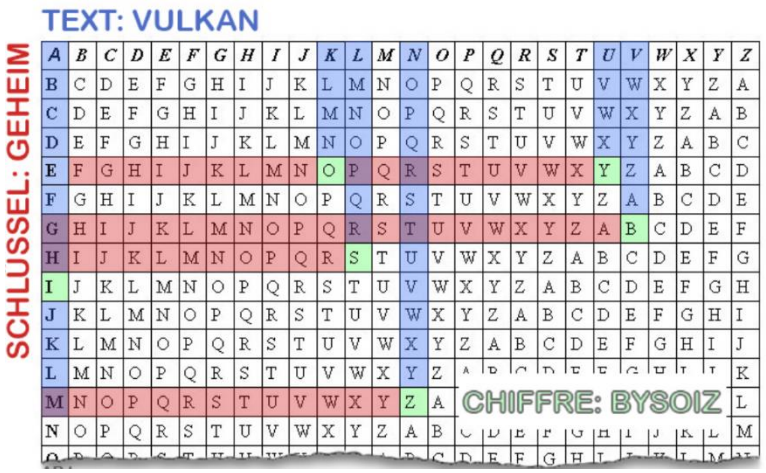
Die Rotationschiffre ROT (Klassische Verfahren)



Die XOR-Stromchiffre (Aktuelle Verfahren)



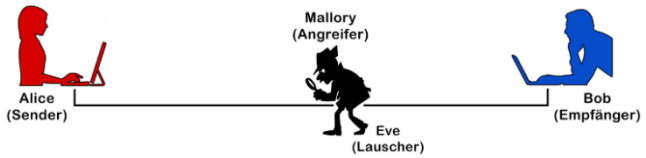
Die Vigenèreverschlüsselung (KlassischeVerfahren)



Schlüsslberechnung

Anzahl Teilnehmer * Anzahl Teilnehmer (-1) /2 (Beispiel: 4*3=12=6)
Anzahl Schlüssel = pro Teilnehmer Ein Private Key und ein Public key (zählen als einer)

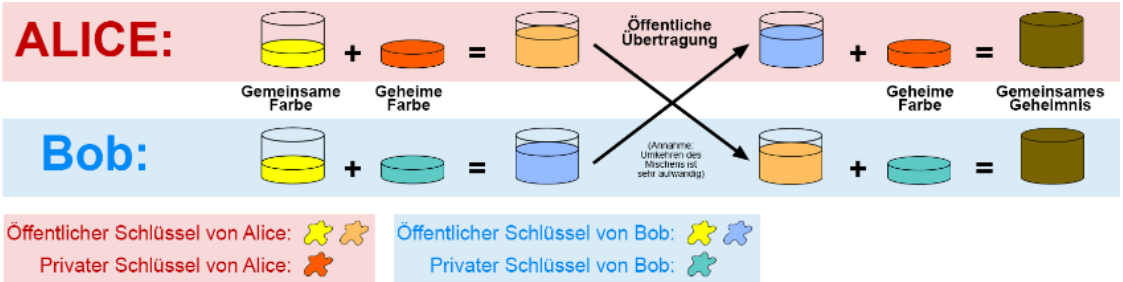
Vorteile	Nachteile
• Unkompliziert, da nur ein Schlüssel für Ver- und Entschlüsselung genutzt wird • Hohe Geschwindigkeit für Ver- und Entschlüsselung von Daten	• Anzahl der Schlüssel wächst mit der Anzahl der Teilnehmer quadratisch • Schlüssel muss geheim gehalten werden

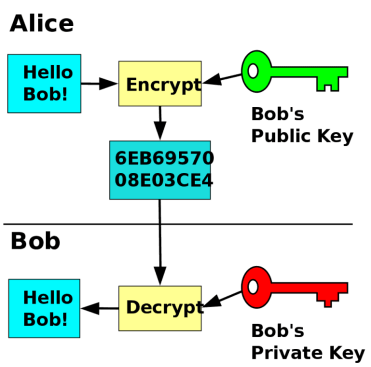


Asymmetrische Verschlüsselung

Bei der **Public-Key**-Kryptographie werden Daten mit zwei verschiedenen Schlüsseln verschlüsselt oder signiert, wobei einer der Schlüssel, der öffentliche Schlüssel, für jeden zugänglich ist. Der andere Schlüssel wird als privater Schlüssel bezeichnet.

DiffieHellman





Digital signieren

Das möchte man erreichen:

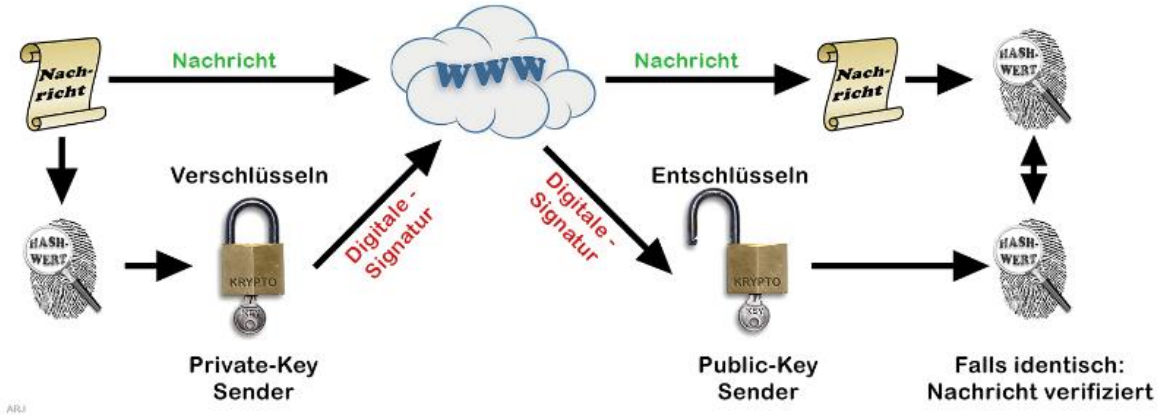
- Authentisierung - Sicherstellung der Identität eines Kommunikationspartners
- Vertraulichkeit - Zugänglichkeit der Nachricht nur für bestimmten Empfängerkreis
- Integrität - Schutz vor Verfälschung von Nachrichten bei der Übermittlung
- Autorisierung - Prüfung der Zugriffsberechtigung auf Ressourcen
- Verfügbarkeit - Schutz vor Datenverlust, Sicherstellung des laufenden Betriebs
- Verbindlichkeit - Sicherer Nachweis der Absendung bzw. des Empfangs

Und da kommt die digitale Signatur ins Spiel:

- Sichere Identifizierung des Absenders eines Dokumentes
- Sicherheit vor nachträglichen Manipulationen des Dokumentes
- Elektronisch signierte Dokumente sind mit unterschriebenen Papierdokumenten gleich gesetzt
- Ist ein Prüfwert einer Information
- Die Digitale Signatur hat die Aufgabe einer Unterschrift und eines Siegels

Das Konzept

- Der Inhalt der Nachricht wird auf eine eindeutige Kenngrösse abgebildet. Dazu bedient man sich eines **Hash-Algorithmus**
- Der Hash-Wert wird mit dem **privaten Schlüssel** verschlüsselt und zur Nachricht hinzugefügt
- Der Empfänger kann mit Hilfe des **öffentlichen Schlüssel** des Senders prüfen, ob die Information wirklich vom Absender stammt und nicht verändert wurde



Hybride Verfahren RSA/AES

- Symmetrische Verfahren gelten allgemein als sicherer, weil deren Verschlüsselungsalgorithmen weniger Angriffsfläche bieten. Auf der anderen Seite hat man ein Problem den Sitzungsschlüssel sicher auszutauschen.
- Asymmetrische Verfahren sind meist komplexer und langsamer bei der Verschlüsselung. Auf der anderen Seite lösen asymmetrische Verfahren das Problem mit dem Schlüsselaustausch.

Kombiniert man symmetrische und asymmetrische Verfahren löst man auf wunderbare Weise die Nachteile, die beide mit sich bringen. Hybride Verschlüsselungsverfahren setzen ein asymmetrisches Verfahren für den Schlüsselaustausch ein und verschlüsseln die Datenübertragung mit einem symmetrischen Verfahren.

Group of Pictures
Dabei werden Bilder die gleich sind nicht mehrmals gespeichert sondern werden 1 mal gespeichert und wieder gleich gezeigt.

Blockartefakte
Blockartefakte= Zusammenschluss Blockartig von Pixeln welche gleich aussehen
Fotos immer im tiff oder raw bearbeiten und erst am ende der Bearbeitungsphase vollkommen um jpg format speichern.

1. Schritt -> Drehdingsbums
2. Schritt -> Alphabetisch
3. Schritt -> Ablesen

EILF1
FEIL 2<
IFLE3
LEFI4

E
F
I
L