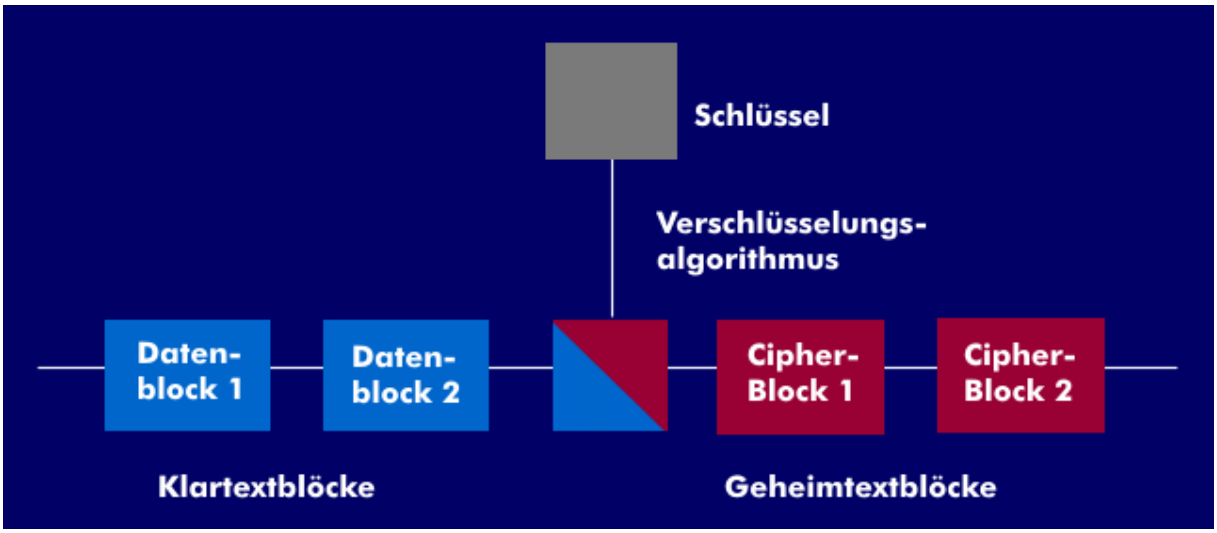
Blockchiffre

Blockchiffre, Block Cipher, ist ein Verschlüsselungsverfahren bei dem Klartext in Bitgruppen, also Datenblöcken, bearbeitet wird. Die Blockchiffre arbeitet immer mit Datenblöcken fester Länge, beispielsweise 64 Bit. Diese Datenblöcke werden unabhängig voneinander ver- und entschlüsselt. Sollte ein Datenblock nicht die erforderliche Blocklänge aufweisen, wird er mit Füll-Bits aufgefüllt. Beim Blockchiffre wird immer mit dem gleichen Schlüssel verschlüsselt, das kann zur Folge haben, dass Blöcke mit identischem Informationsinhalt auch den gleichen Chiffretextblock haben. Dies umgehen einige Varianten, indem sie zwischen benachbarten Blöcken Verknüpfungen herstellen.



Prinzip des Blockchiffre

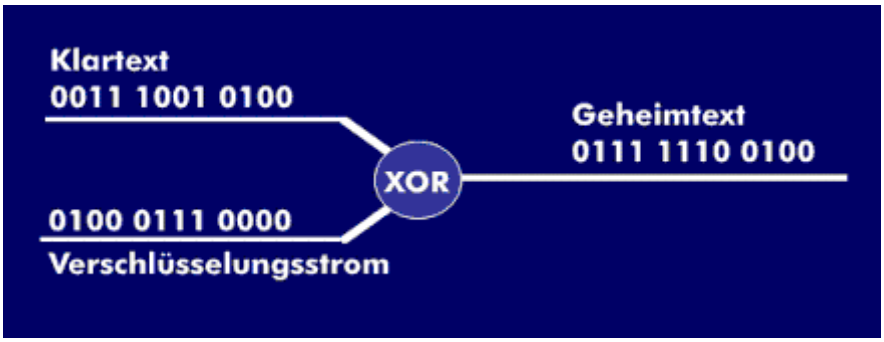
Der internationale Standard ISO 10116 definiert für blockorientierte Verschlüsselungsalgorithmen vier verschiedenen Betriebsarten:

Blockchiffre		Verschlüsselungsart
ECB	Electronic Code Book	Jeder Datenblock wird einzeln verschlüsselt. Blockchiffre ohne Rückkopplung.
CBC	Cipher Block Chain	Verknüpfung eines Datenblocks mit dem vorhergehenden Chiffratblock.
CFB	Cipher Feedback	Kleine Klartextinkremente werden in Geheimtext gewandelt.
OFB	Output Feedback	Blockchiffre mit einer Rückkopplung ähnlich CBC.

Blockchiffre-Verfahren
Blockchiffre-Verfahren arbeiten mit logischen Verknüpfungen wie XOR, mit Substitution, Permutation und arithmetischen Operationen der Dualarithmetik. Um eine mögliche Entschlüsselung so weit als möglich zu verhindern, arbeiten Blockchiffre-Verfahren bei der Verschlüsselung in mehreren Runden. Eine Runde soll für Verwirrung und Zerstreuung sorgen, wobei durch die Verwirrung (Confusion) der Zusammenhang zwischen Geheimtext und Schlüssel so komplex wie möglich gemacht wird. Die Zerstreuung (Diffusion) versucht die Redundanz im Klartext über den gesamten Geheimtext zu verteilen. Das Durchlaufen mehrerer Runden sorgt für eine weitere Erhöhung von Confusion und Diffusion.

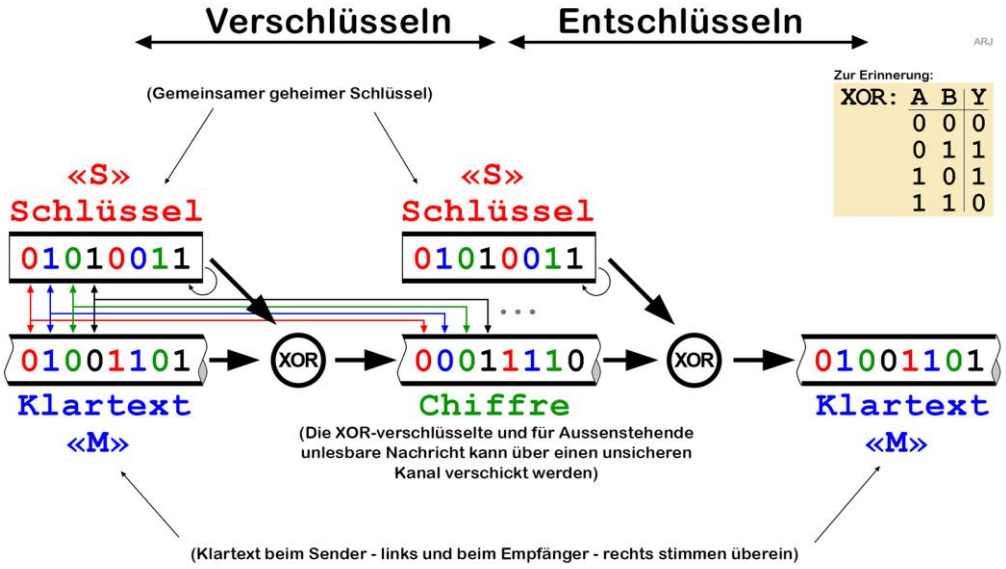
Stromchiffre

Stromchiffre, Stream Cipher, ist eine Verschlüsselung bei der die Information kontinuierlich zeichenweise oder bitweise verschlüsselt wird. Die Zeichen eines Datenstroms werden mit dem Verschlüsselungsstrom verknüpft, der aus dem Schlüssel im Schlüsselstromgenerator generiert wird. Beim Stromchiffre werden die Zeichen des Klartextes in einer XOR-Verknüpfung mit dem Verschlüsselungsstrom verknüpft. Aus dieser Verknüpfung entsteht der Geheimtext. Der Verschlüsselungsstrom hat die gleiche Länge wie der Klartext. Der Vorteil des Stromchiffre gegenüber der Blockchiffre liegt in der verzögerungsfreien Ver- und Entschlüsselung und in der Länge der Dokumente.



Stromchiffre als XOR-Verknüpfung von Klartext und Verschlüselungsstrom

Bei der Entschlüsselung wird der Geheimtext wiederum mit dem Verschlüsselungsstrom in einer XOR-Verknüpfung verknüpft und daraus der Klartext gewonnen. Beim synchronen Stromchiffre erzeugen der Sender und der Empfänger den Verschlüsselungsstrom synchron.



Aufgaben

1. Welche Verschlüsselungen verwenden Blockchiffren?
2. Welche Verschlüsselungen beinhalten Stromchiffren?
3. Bilden Sie den Stromchiffre mit dem Klartext 1001 1110 und dem Schlüssel 1101 0010 !