

Grundlagen der Kryptologie

Kryptographie, Kryptoanalyse, klassische und moderne Verfahren

Tom Gries



Dokumenten URL:

<http://docs.tx7.de/TT-TK6>

Autor:

Tom Gries <TT-TK6@tx7.de>
@tomo@chaos.social

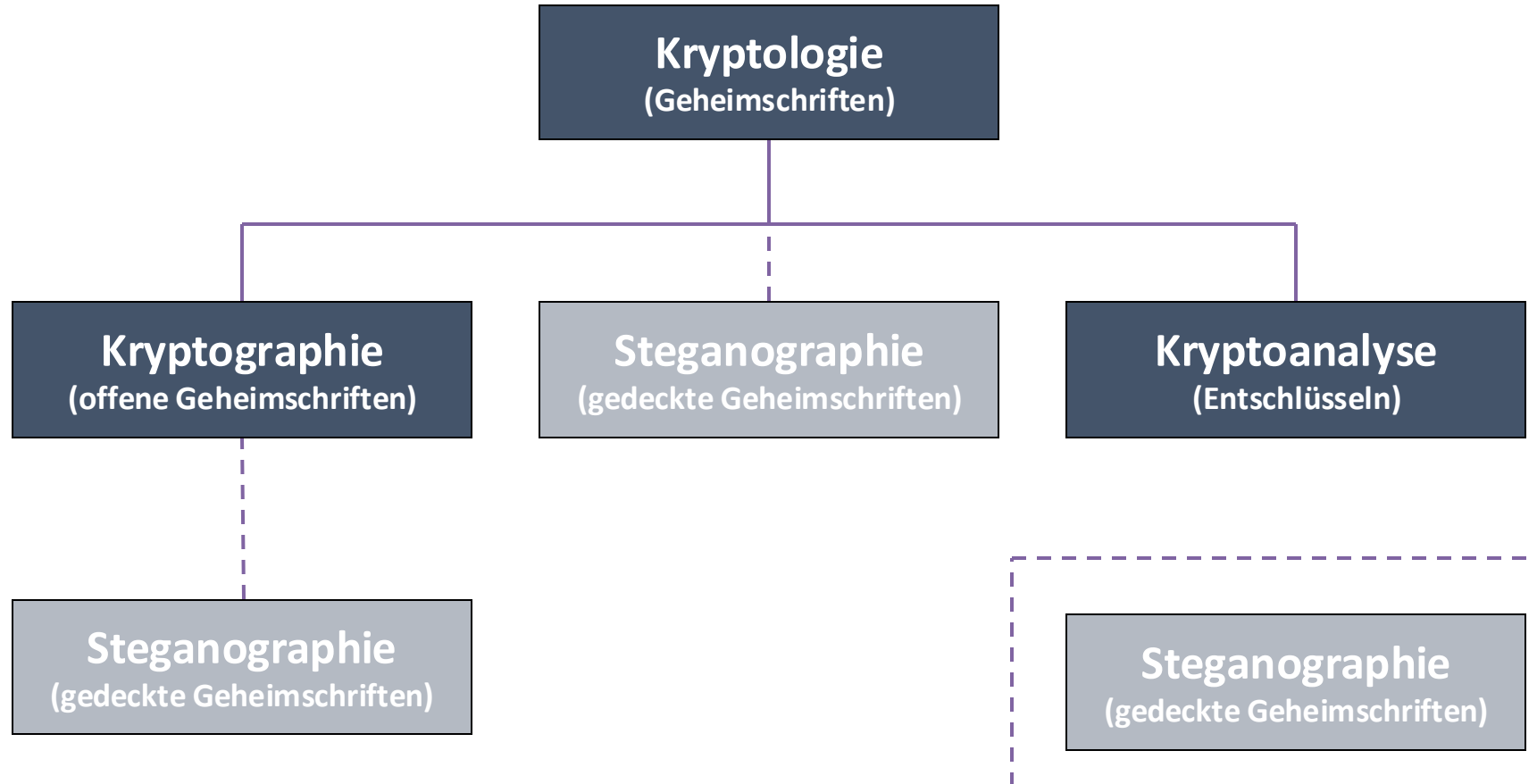
Lizenz:

Creative Commons BY-NC-ND

Version:

7.3.0 vom 22.07.2025





Die Kryptologie ist die Wissenschaft der Verschlüsselung und Entschlüsselung von Informationen.



Hauptziele der Kryptographie

Die Kryptographie hat 4 Hauptziele:

1. Confidentiality (Wahrung der Vertraulichkeit)
2. Integrity (Sicherstellung der Datenintegrität)
3. Authenticity (Sicherstellung der Echtheit)
4. Non Repudiation (Nichtabstreitbarkeit)

Die allgemeine IT-Security hat darüber hinaus noch das Ziel der Availability (Sicherstellung der Verfügbarkeit). Der Geheimschutz kennt nur [1] und [2]. Bei Confidentiality, Integrity und Availability spricht man von der **CIA-Triade**.



Eine kleine Aufgabe

Entschlüsse den Text auf der folgenden Seite. Erkläre anschließend, wie Du auf die Lösung gekommen bist und um welche Chiffre es sich handelt.

Text unter <http://docs.tx7.de/TT-TUV> abrufbar



FIMWTMIP GEIWEV GLMJJVI

HMI OVCTXSKVETLMI MWX HIV DAIMK HIV OVCTXSPSKMI, HIV WMGL QMX HIQ
ZIVWGLPYIWWIPR ZSR MRJSVQEXMSRIR FIJEWWX.

HMI OVCTXSEREPCWI MWX HMI AMWWIRWGLEJX, MRJSVQEXMSRIR EYW
ZIVWGLPYIWWIPXIR XIBXIR DY KIAMRRIR. HMIWI MRJSVQEXMSRIR OSIRIR WSASLP
HIV ZIVAIRHIXI WGLPYIWWIP EPW EYGL HIV SVMKMREPXIBX WIMR. AIWIRXPMGLI
DMIPI HIV OVCTXSEREPCWI WMRH HEW EYJLIFIR HIV WGLYXDJYROXMSR, HEW
YQKILIR HIV WGLYXDJYROXMSR WSAMI HIV REGLAIMW YRH UYERXMJMDMIVYRK
HIV WMGLIVLIMX IMRIW ZIVJELVIRW.

Text unter <http://docs.tx7.de/TT-TUV> abrufbar



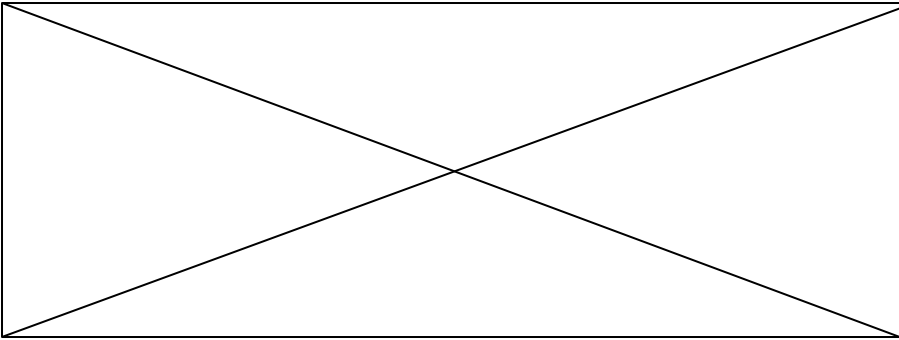
BEISPIEL CAESAR CHIFFRE

DIE KRYPTOGRAPHIE IST DER ZWEIG DER KRYPTOLOGIE, DER SICH MIT DEM VERSCHLUESSELN VON INFORMATIONEN BEFASST.

DIE KRYPTOANALYSE IST DIE WISSENSCHAFT, INFORMATIONEN AUS VERSCHLUESSELTEN TEXTEN ZU GEWINNEN. DIESE INFORMATIONEN KOENNEN SOWOHL DER VERWENDETE SCHLUESSEL ALS AUCH DER ORIGINALTEXT SEIN. WESENTLICHE ZIELE DER KRYPTOANALYSE SIND DAS AUFHEBEN DER SCHUTZFUNKTION, DAS UMGEHEN DER SCHUTZFUNKTION SOWIE DER NACHWEIS UND QUANTIFIZIERUNG DER SICHERHEIT EINES VERFAHRENS.



Verfahren der Kryptographie

	Symmetrische Chiffre	Asymmetrische Chiffre
Klassisch	<ul style="list-style-type: none">⇒ Transposition (Anagramm/vertauschen)⇒ Substitution (ersetzen)<ul style="list-style-type: none">▪ Monoalphabetische Substitution▪ Polyalphabetische Substitution	
Modern (IT)	<ul style="list-style-type: none">⇒ Blockchiffre⇒ Stromchiffre <p>Schlüssel ≤ 512 Bit</p>	<ul style="list-style-type: none">⇒ Public-Key Verfahren <p>Schlüssel ≥ 1.024 Bit</p>



Verfahren der Kryptographie

Klassische Verfahren

Transpositionsverfahren:

- ⇒ Skytale
- ⇒ Fleißnersche Schablone

Substitutionsverfahren (monoalphabetisch):

- ⇒ Caesar

Substitutionsverfahren (polyalphabetisch):

- ⇒ Vigenère-Verschlüsselung
- ⇒ ENIGMA

Spezialfall: Homophone Verschlüsselung

Moderne Verfahren

Symmetrische Blockchiffren:

- ⇒ AES
- ⇒ Twofish

Symmetrische Stromchiffren:

- ⇒ ChaCha20 (Alternative zu AES)

Publik-Key Verfahren (asymmetrisch):

- ⇒ RSA
- ⇒ Ed25519



Klassische Verfahren der Kryptographie: Transpositionsverfahren

Bei den Transpositionsverfahren werden die Buchstaben des Klartextes vertauscht (permutiert). Die Zeichen selber und die Anzahl jedes einzelnen Zeichens werden nicht verändert.

Beispiel:

Klartext: FRIKADELLE

Geheimtext: LEKADEFRIIL

Frage:

Wie viele Permutationen und mögliche Geheimtexte gibt es bei den Klartextworten TOR, ZOO und MONOTON?



Klassische Verfahren der Kryptographie: Transpositionsverfahren

TOR:

6 Permutationen: TOR - TRO - ROT - RTO - OTR - ORT

$$3! = 6$$

ZOO:

3 Permutationen: ZO₁O₂ - ZO₂O₁ - O₁ZO₂ - O₂ZO₁ - O₁O₂Z - O₂O₁Z
ZOO - OZO - OOZ

$$\frac{3!}{2!} = \frac{6}{2} = 3$$

MONOTON:

420 Permutationen: MO₁N₁O₂TO₃N₂ - MO₁N₂O₂TO₃N₁ - ...
MONOTON - MONOTNO - ...

$$\frac{7!}{2! \times 3!} = \frac{5.040}{2 \times 6} = 420$$

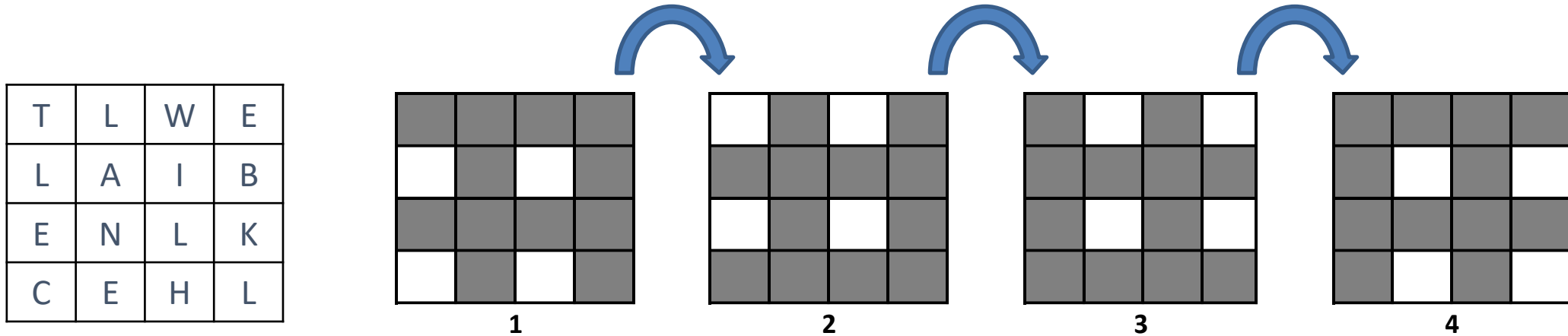


Die Skytale:





Die Fleißnersche Schablone:





Klassische Verfahren der Kryptographie: Substitutionsverfahren

Die monoalphabetische Substitution:

Caesar - Verschiebung um 5	
Klartextalphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

ROT 13	
Klartextalphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

Atbash	
Klartextalphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Allgemein	
Klartextalphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet	W U E G H J M B X D N S Q A Y K R V L C Z O P I T F



Klassische Verfahren der Kryptographie: Substitutionsverfahren

Die monoalphabetische Substitution:

Bei der Substitution können anstatt Buchstaben natürlich auch Zahlen verwendet werden.

Substitution durch Zahlen																											
Klartextalphabet		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Es können auch beliebig andere Zeichen verwendet werden. Zum Beispiel selbstausgedachte Zeichen.

Substitution durch Zeichen																											
Klartextalphabet		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheimtextalphabet		☪	♂	♂	♂	☺	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂	♂



Klassische Verfahren der Kryptographie: Substitutionsverfahren

Die polyalphabetische Substitution:

Vigenère-Verschlüsselung

$R = 3 \quad | \quad A/B = 2 \quad | \quad H/E = 1$

Klartext:	R	H	A	B	A	R	B	E	R
Schlüssel:	B	E	R	L	I	N	B	E	R
Geheimtext:	S	L	R	M	I	E	C	I	I

$I = 3 \quad | \quad S/L/R/M/E/C = 1$

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



Klassische Verfahren der Kryptographie: Substitutionsverfahren



Die ENIGMA



Die ENIGMA: polyalphabetisches Substitutionsverfahren

Die ENIGMA (griechisch αἴνιγμα ainigma "Rätsel") ist eine Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs des deutschen Militärs verwendet wurde.

Trotz vieler Verbesserungen der Verschlüsselungsqualität der Maschine vor und während des Krieges gelang es den Alliierten mit hohem personellem und maschinellem Aufwand, die deutschen Funksprüche nahezu kontinuierlich zu entziffern (Polnische Kryptographen knackten die frühe Enigma 1932. Alan Turing entwickelte in Bletchley Park Maschinen zur systematischen Entzifferung.).



Klassische Verfahren der Kryptographie: Spezialfall

Homophone Verschlüsselung:

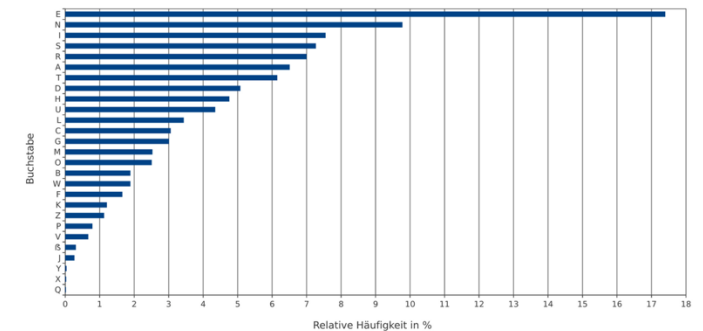
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	27	54	02	06	17	31	01	05	84	92	04	34	11	47	28	03	18	09	14	00	51	77	70	19	67
26	65	90	07	10	78	38	08	16			46	96	24	79			30	22	35	20					
36			41	12		64	13	21			87		29				45	32	43	57					
56			58	15			52	25					40				60	50	55	98					
82			88	33			62	44					49				68	66	75						
93				37				59					61				74	80	83						
				39				81					69				99	94							
				42				89					73												
				48									85												
				53									91												
				63																					
				71																					
				72																					
				76																					
				86																					
				95																					
				97																					

6	2	2	5	17	2	3	5	8	1	1	3	2	10	2	1	1	7	7	6	4	1	1	1	1	1
---	---	---	---	----	---	---	---	---	---	---	---	---	----	---	---	---	---	---	---	---	---	---	---	---	---

 = 100

Platz	Buchstabe	Relative Häufigkeit	Platz	Buchstabe	Relative Häufigkeit
1.	E	17,40 %	15.	O	2,51 %
2.	N	9,78 %	16.	B	1,89 %
3.	I	7,55 %	17.	W	1,89 %
4.	S	7,27 %	18.	F	1,66 %
5.	R	7,00 %	19.	K	1,21 %
6.	A	6,51 %	20.	Z	1,13 %
7.	T	6,15 %	21.	P	0,79 %
8.	D	5,08 %	22.	V	0,67 %
9.	H	4,76 %	23.	ß	0,31 %
10.	U	4,35 %	24.	J	0,27 %
11.	L	3,44 %	25.	Y	0,04 %
12.	C	3,06 %	26.	X	0,03 %
13.	G	3,01 %	27.	Q	0,02 %
14.	M	2,53 %			

Buchstabenhäufigkeiten in deutschsprachigen Texten





Blockchiffre:

Eine Blockchiffre ist ein symmetrisches Verschlüsselungsverfahren, das Daten in gleich großen Blöcken verarbeitet, typischerweise 64 oder 128 Bit. Jeder Klartextblock wird mit einem geheimen Schlüssel durch mehrere Runden mathematisch transformiert. Dabei kommen Operationen wie XOR, Substitution und Permutation zum Einsatz, um Vertraulichkeit zu gewährleisten.

Der gleiche Schlüssel wird auch zur Entschlüsselung benötigt, was sie symmetrisch macht. Da echte Nachrichten selten genau blockweise passen, werden sie oft mit Padding ergänzt. Blockchiffren wie AES gelten als sehr sicher und sind die Grundlage vieler moderner Sicherheitsprotokolle (z. B. TLS, VPN, Festplattenverschlüsselung).



Aufteilung in Blöcke:

Der Klartext wird in gleich große Blöcke zerlegt (z. B. 128 Bit bei AES). Falls der letzte Block zu kurz ist, wird er durch Padding (Auffüllen) ergänzt.

Verschlüsselung jedes Blocks:

Jeder Block wird mit dem gleichen geheimen Schlüssel durch eine mathematische Funktion in einen Chiffreblock umgewandelt.

Chiffretext entsteht:

Die verschlüsselten Blöcke werden zusammengesetzt und ergeben den Chiffretext.



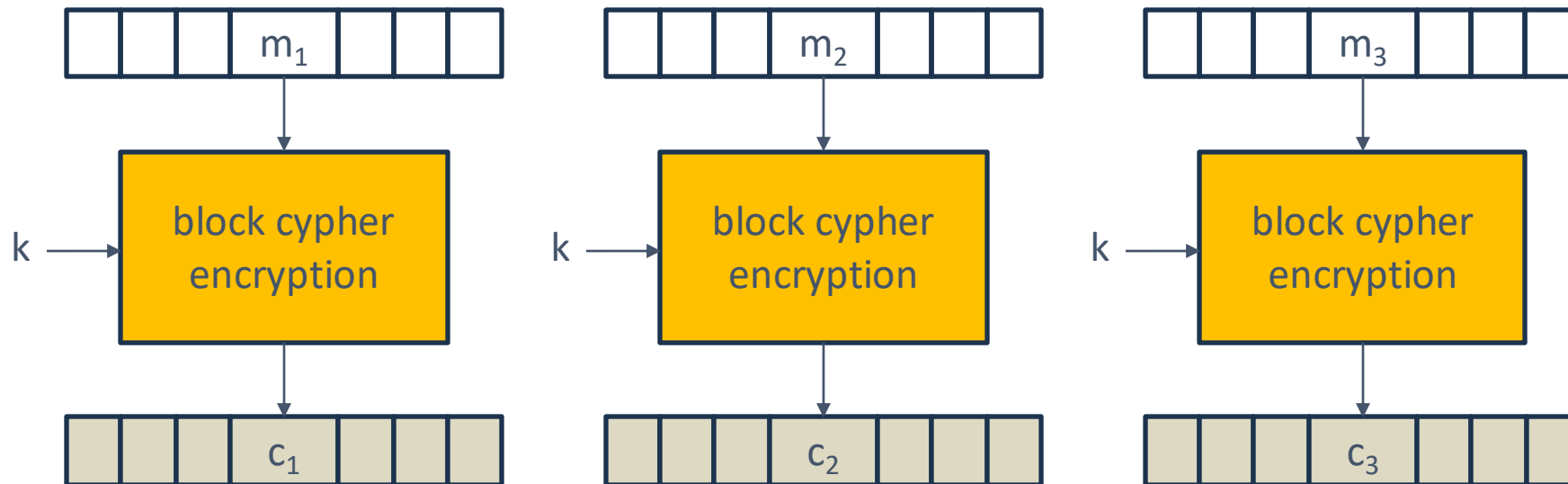
Moderne Verfahren der Kryptographie - Betriebsmodi

Die gleich großen Blöcke des Blockchiffreverfahren können auf unterschiedliche Art und Weise arbeiten. Dies sind die sogenannten Betriebsmodi. Sie bestimmen, wie diese Blöcke verarbeitet werden. Die Wichtigsten Betriebsmodi sind:

Modus	Kurzbeschreibung
ECB (Electronic Codebook)	Jeder Block separat verschlüsselt (unsicher bei gleichen Klartextblöcken).
CBC (Cipher Block Chaining)	Jeder Klartextblock wird mit dem vorherigen Chiffreblock verknüpft.
CFB (Cipher Feedback Mode)	Cypherblock als Initialisierungsvektor IV.
OFB (Output Feedback Mode)	Keystreamblock als Initialisierungsvektor IV.
CTR (Counter Mode)	Nonce + Counter als Initialisierungsvektor IV.



Electronic Codebook Mode (ECB):



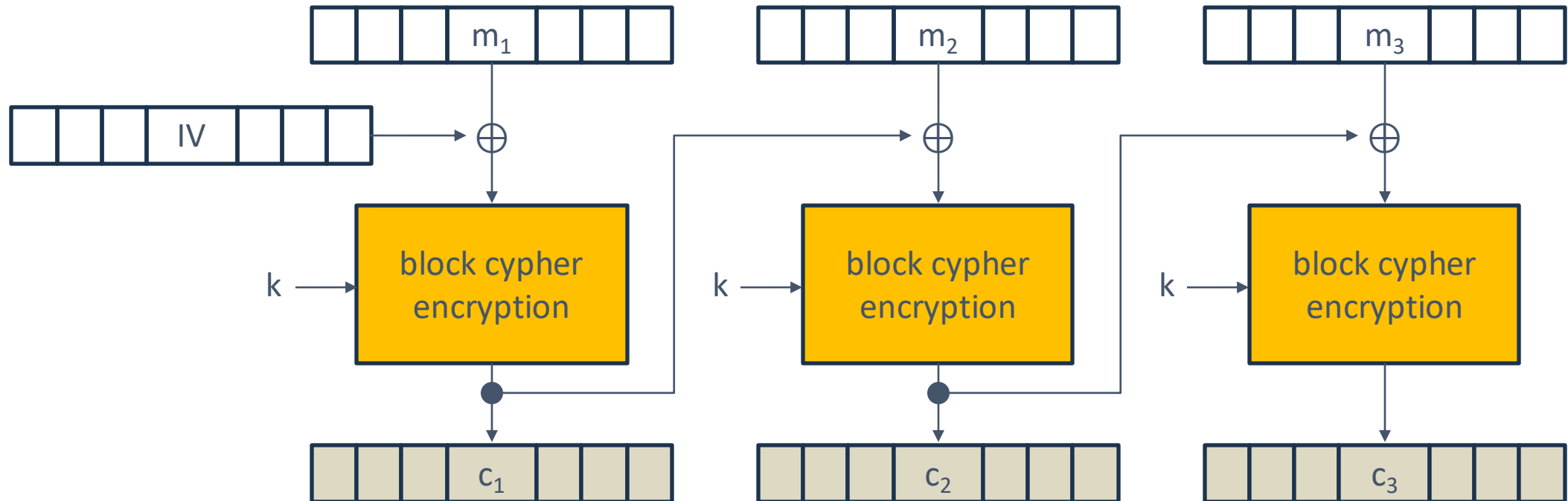
k = key | m = message (plain text) | c = cypher text



A = 11001010
B = 10110100
A \oplus B = 01111110

XOR: 1 wenn ungleich

Cypher Block Chaining (CBC) - encryption:



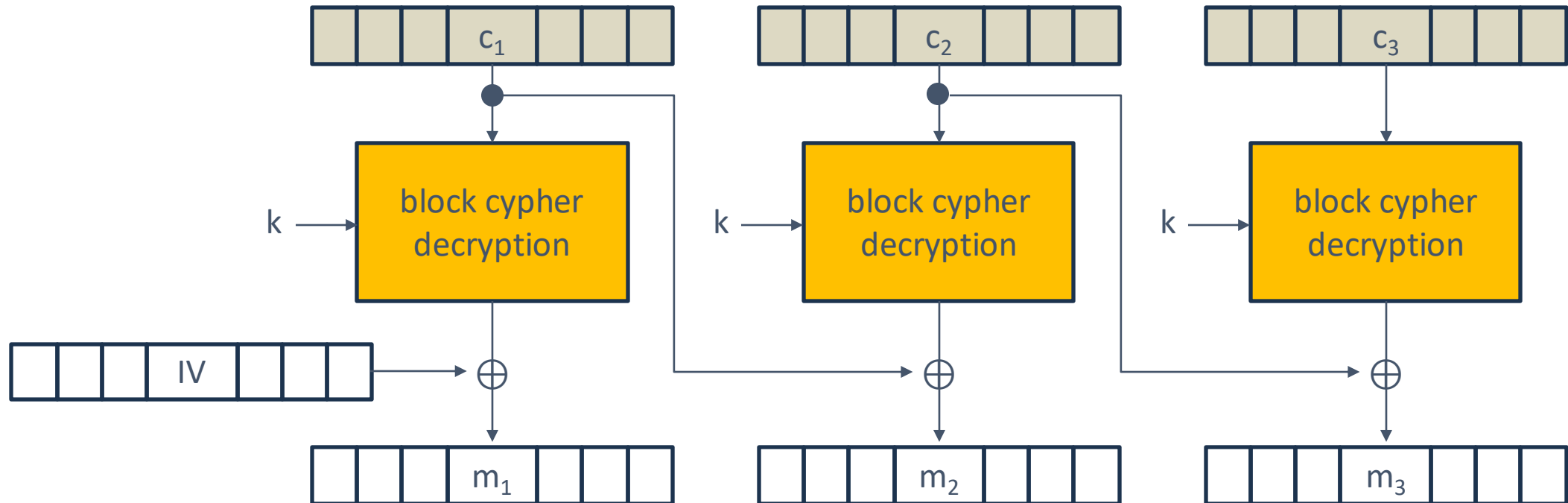
IV = Initialisierungs Vektor | k = key | m = message (plain text) | c = cypher text



A = 11001010
B = 10110100
A \oplus B = 01111110

XOR: 1 wenn ungleich

Cypher Block Chaining (CBC) - decryption:



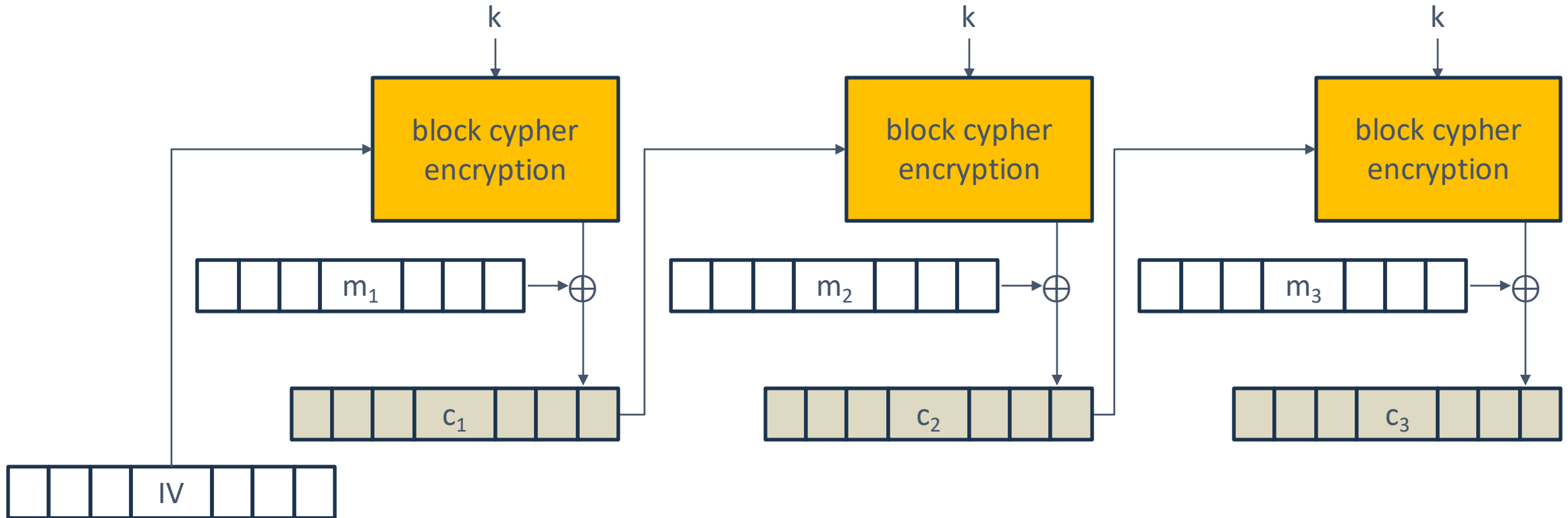
IV = Initialisierungs Vektor | k = key | m = message (plain text) | c = cypher text



A = 11001010
B = 10110100
A \oplus B = 01111110

XOR: 1 wenn ungleich

Cypher Feedback Mode (CFB):



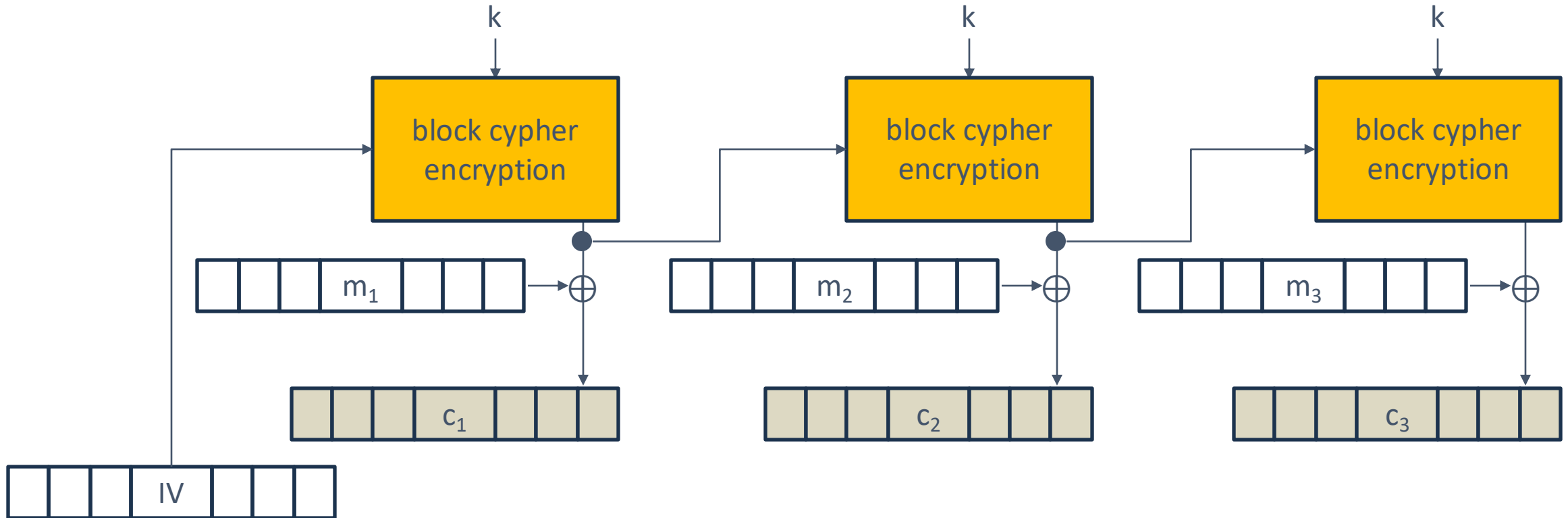
IV = Initialisierungs Vektor | k = key | m = message (plain text) | c = cypher text



A = 11001010
B = 10110100
 $A \oplus B = 01111110$

XOR: 1 wenn ungleich

Output Feedback Mode (OFB):



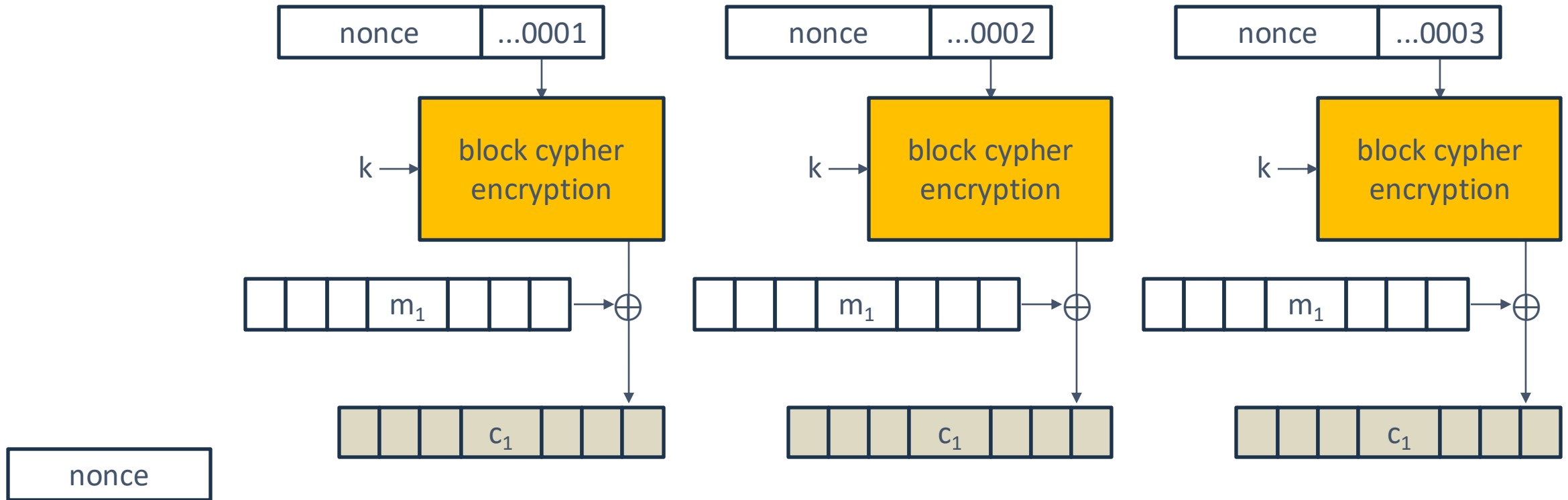
IV = Initialisierungs Vektor | k = key | m = message (plain text) | c = cypher text



A = 11001010
B = 10110100
 $A \oplus B = 01111110$

XOR: 1 wenn ungleich

Counter Mode (CTR):



nonce = Einmalwert | k = key | m = message (plain text) | c = cypher text

Lokale Dateien verschlüsseln



Verschlüsselung einzelner Dateien mit zum Beispiel:

- ZIP (7-Zip)
- GnuPGP (gpg)
- Conpal LAN Crypt 2Go (<https://conpal.de/2Go>)
- Hat.sh - auch nur im Browser (<https://hat.sh>)

Nur einzelne Dateien werden verschlüsselt. Außer bei GPG ist ein Schlüsselaustausch für den Austausch mit Anderen notwendig. Keine Installation bei Crypt 2Go und Hat.sh erforderlich.



Verschlüsselung von Emails und Dateien mit zum Beispiel:

- Alle zur Dateiverschlüsselung geeigneten Tools (als Anhang)
- OpenPGP
- S/MIME

Wenn nur der Anhang verschlüsselt werden soll, reichen die Tools aus der vorherigen Kategorie (Dateiverschlüsselung) aus. Ansonsten kommt es drauf an, was der Mail-Client (MUA) unterstützt. Thunderbird zum Beispiel unterstützt OpenPGP und S/MIME. Im Firmen und Behördenumfeld wird eher S/MIME eingesetzt, im privaten Umfeld eher OpenPGP.



Verschlüsselung eines Containers mit zum Beispiel:

- VeraCrypt
- Cryptomator
- BitLocker
- LUKS (nur Linux)

Ein Container ist eine Datei, die sich als Laufwerk oder Verzeichnis darstellt. Alle Dateien, die in diesen Container kopiert oder verschoben werden, werden automatisch verschlüsselt. Microsofts Virtual Hard Disk (VHD/VHDX) und Mac OS Images (.dmg) sind nur Container, die aber mit anderen Tools verschlüsselt werden können, zum Beispiel BitLocker (bei VHD/VHDX). Bei den Mac OS Images kann beim erstellen optional eine Verschlüsselung auswählen.



Verschlüsselung einer Partition oder Festplatte mit zum Beispiel:

- Bitlocker
- Mac OS FileVault
- LUKS (nur Linux)
- VeraCrypt

Um ganze Partitionen oder Festplatten zu verschlüsseln, bringen viele Betriebssystemvarianten bereits die entsprechenden Tools mit, Windows allerdings nur in den Pro und Enterprise Versionen. Alternativ können Tools von Drittanbietern verwendet werden, wie zum Beispiel das kostenlose VeraCrypt. Zur Erhöhung der Sicherheit sollte in der Pre-Boot Authentication Phase (PBA) ein Passwort oder eine PIN abgefragt werden.

Anmerkungen oder Fragen?